

ORIGINAL

Digital Governance and Personal Data Protection: Proposals for an Ethical Public Transformation through the Privacy-by-Design Approach

Gobernanza Digital y Protección de Datos Personales: Propuestas para una Transformación Pública Ética desde el Enfoque Privacy-by-Design

Roxana Martínez¹  

¹Siglo 21 University, Research Secretariat. Córdoba, Argentina.

Cite as: Martínez R. Digital Governance and Personal Data Protection: Proposals for an Ethical Public Transformation through the Privacy-by-Design Approach. Salud, Ciencia y Tecnología - Serie de Conferencias. 2025; 4:1782. <https://doi.org/10.56294/sctconf20251782>

Submitted: 23-11-2024

Revised: 05-03-2025

Aceptado: 11-07-2025

Publicado: 12-07-2025

Editor: Dr. William Castillo-González 

Corresponding Author: Roxana Martínez 

ABSTRACT

Introduction: this research examined the relationship between digital innovation in public administration and personal data protection, employing a Privacy-by-Design (PbD) approach. It assessed the extent to which government platforms incorporate ethical and legal aspects that guarantee data privacy and security.

Method: a qualitative study of Argentine public initiatives was conducted, combining three strategies: (i) visual exploration of the platforms from the user experience; (ii) manual and automated analysis of metadata on published datasets; and (iii) development of a prototype in Python to validate technical aspects linked to PbD principles, such as security settings, transparency, and basic privacy control mechanisms.

Results: progress was observed in access to open public data and tools aimed at citizen transparency. However, the full incorporation of data protection principles remains a challenge, as evidenced by both manual analysis and automated testing of the prototype. Metadata analysis and technical evaluation revealed weaknesses in the design, particularly in privacy and the implementation of user-accessible control mechanisms.

Conclusions: the results underscore the importance of integrating Privacy-by-Design into smart governance, thereby strengthening citizen trust in digital services and promoting more responsible and sustainable forms of governance. Design recommendations are presented that foster a paradigm shift in application development and regulatory standards for digital public innovation.

Keywords: Privacy by Design; Smart Governance; Public Sector Innovation; Open Government Data; Personal Data Protection.

RESUMEN

Introducción: esta investigación analizó cómo la innovación digital en la administración pública se relaciona con la protección de datos personales, desde un enfoque centrado en el principio Privacy-by-Design (PbD). Se evaluó en qué medida las plataformas gubernamentales incorporan aspectos éticos y legales que garantizan la privacidad y seguridad de los datos.

Método: se realizó un estudio cualitativo sobre iniciativas públicas argentinas, combinando tres estrategias: (i) exploración visual de las plataformas desde la experiencia de usuario; (ii) análisis manual y automatizado de metadatos sobre conjuntos de datos publicados; y (iii) desarrollo de un prototipo en Python para validar aspectos técnicos vinculados a principios de PbD, como configuraciones de seguridad, transparencia y mecanismos básicos de control de privacidad.

Resultados: se observaron avances en el acceso a datos abiertos públicos y en herramientas orientadas a la transparencia ciudadana. Sin embargo, la incorporación completa de los principios de protección de datos

sigue siendo un desafío, evidenciado tanto en el análisis manual como en las pruebas automatizadas con el prototipo. El análisis de metadatos y la evaluación técnica revelaron debilidades en el diseño, especialmente en privacidad y en la implementación de mecanismos de control accesibles para usuarios.

Conclusiones: los resultados enfocan la importancia de integrar Privacy-by-Design en la gobernanza inteligente, fortaleciendo la confianza ciudadana en los servicios digitales y promoviendo formas de gobernanza más responsables y sostenibles. Se presentan recomendaciones de diseño que fomentan un cambio de paradigma en el desarrollo de aplicaciones y en estándares normativos para la innovación pública digital.

Palabras clave: Privacy-by-Design; Gobernanza Inteligente; Innovación en el Sector Público; Datos Gubernamentales Abiertos; Protección de Datos Personales.

INTRODUCTION

The concept of digital transformation is currently on the rise and is being used by various governments that implement technological innovation approaches.

Currently, in several countries around the world, it has become a strategic axis for the modernization of the Governmental State. Regarding the latter, digital transformation refers to the integration of digital technologies in all areas of public institutions and is implemented with the aim of improving the efficiency, transparency, and quality of services offered to citizens.⁽¹⁾

The growing demand for and use of large volumes of data (Big Data) leads to the use of platforms that enable the automation of various public services offered to citizens. This allows public administration to design public policies that efficiently respond to the real needs of society; it will also facilitate decision-making through predictive behaviour analysis.⁽²⁾ This paradigm shift, in terms of efficiency and transparency, has raised significant concerns about data exposure and the protection of personal data,⁽³⁾ as well as the management of information security in the government's use of emerging technologies.

In Latin America, and particularly in Argentina, several public policies have worked on the development and use of open data portals,^(4,5) civic applications to promote public accountability and strengthen citizen participation,⁽⁶⁾ and on budget visualization systems as mechanisms to promote this approach. However, these initiatives have evolved and become increasingly accessible to citizens,⁽⁷⁾ but in some aspects, they have not always considered technical design concepts in ethical and legal matters that ensure effective protection of the privacy of personal data.^(8,9) In this context, a problem is analyzed in aspects between digital innovation and the protection of citizens' rights.⁽¹⁰⁾ Therefore, as data becomes a valuable resource for public decision-making, the risks associated with its collection, management, and reuse increase in parallel.

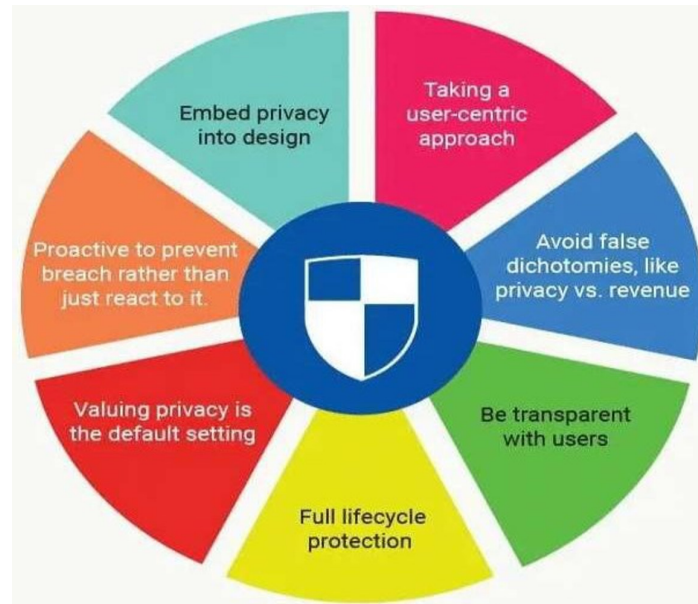
Given the above, it is necessary to analyze the technical aspects that define the design in the development and implementation of public technologies for the processing of personal data. The Privacy-by-Design (PbD) approach⁽¹¹⁾ is an emerging concept that offers a conceptual and technical framework aimed at incorporating privacy as an added value in the development of systems design.⁽¹²⁾

Originally proposed by Ann Cavoukian in the 1990s, this approach establishes seven fundamental principles,⁽¹³⁾ including proactivity, privacy by default, and design visibility. The seven criteria, with their corresponding descriptions, are shown in table 1.

Table 1. Fundamental principles of Privacy-by-Design		
Number	Principle	Description
1	Proactive, not reactive; preventive, not corrective	Anticipates risks and seeks to prevent privacy violations before they occur.
2	Privacy by Default	The default settings should ensure the highest possible level of protection without requiring user intervention.
3	Privacy Built into the Design	Privacy is incorporated from the outset into system development, as an integral part of the technological and organizational architecture.
4	Full functionality - positive sum, not zero	Promotes solutions that integrate privacy with other legitimate interests, without sacrificing one for the other.
5	End-to-end security	Protects data throughout its entire lifecycle, from collection to secure disposal.
6	Visibility and Transparency	Processes must be open and auditable, ensuring both internal and external accountability.
7	Respect for user privacy	The user is prioritized, ensuring clear choices, control over their data, and individual-centered values.

Considering these criteria in the design of public platforms not only allows for compliance with current legal frameworks, such as the Personal Data Protection Law No. 25 326 in Argentina⁽¹⁴⁾ or the General Data Protection Regulation (GDPR) in Europe⁽¹⁵⁾ but also enables a deeper transformation in governance models. The decision to work with a proactive, privacy-focused approach promotes transparency, institutional trust, and citizen participation. This type of ethical approach to public innovation allows for individuals' rights to be the fundamental axis of government technological development.^(16,17) Therefore, the Privacy-by-Design criterion becomes a strategic pillar that guides the construction of digital services to become more legitimate.⁽¹⁸⁾

In today's context, where digital life is directly related to privacy, it can no longer be considered optional in software development.^(19,20) Integrating privacy by design is not only a good technical practice, but a fundamental condition for developing more secure and trustworthy digital environments.^(21,22) People are increasingly aware and concerned about how their data is handled, so it is necessary to incorporate data protection principles from the beginning of development.^(23,24) This framework is shown in figure 1.



Source: Yanamala et al.⁽¹⁶⁾

Figure 1. The Privacy by Design (PbD) Framework

The implementation of PbD in the Argentine governmental context, despite being a strategic central axis in data protection issues, has not yet been sufficiently documented or empirically evaluated. Based on this, the main objective of this research is to analyze aligned public government data platforms to understand the extent to which these platforms incorporate elements of the Privacy-by-Design approach in their functional, visual, and data management structures.

METHOD

Type of Study, Temporal and Spatial Framework

This study adopts an exploratory qualitative design with abductive reasoning to investigate the incorporation of Privacy-by-Design (PbD) principles in digital government platforms. The analysis focuses on Argentine public portals that publish open government data.

The study was conducted between August 2024 and March 2025, covering national, provincial, and municipal platforms across Argentina.

Case Selection: Population and Sample

The study focused on a purposive sample of 18 public platforms based on the following inclusion criteria:

- Access without authentication requirements.
- Active dataset publication within the last 12 months.
- Institutional purpose related to transparency or citizen participation.
- Functional mechanisms for information download or user interaction.

Platforms not meeting these criteria were excluded. The selection aimed to ensure a diversity of jurisdictions and administrative levels.

Methodological Strategies and Instruments

The methodological strategy combines three qualitative techniques; each associated with a specific instrument:

- Visual Exploration:
 1. Instrument: observation matrix based on the 7 PbD principles.
 2. Focus: navigation, privacy policies, user contact options.
- Metadata Analysis:
 1. Instrument: python scripts using pandas, requests, beautifulsoup.
 2. Focus: dataset metadata such as licenses, update dates, formats, authors.
- Technical Prototype:
 1. Instrument: Google Colab notebook developed by the research team.
 2. Focus: automatic validation of security settings, licenses, traceability, and user control mechanisms.

Additional instruments included a collaborative Google Sheet for cross-review and coding.

Figure 2 presents a summary of the three methodological strategies used in this qualitative study, and for each, the respective analytical objectives. This organization allows us to understand how the mixed analysis approach was articulated, combining visual exploration, metadata review, and prototype development, to comprehensively incorporate Privacy-by-Design principles into government digital platforms. The table shows the relationship between the techniques, aimed at both the detection of user-visible aspects and the automated technical validation of privacy-critical configurations.

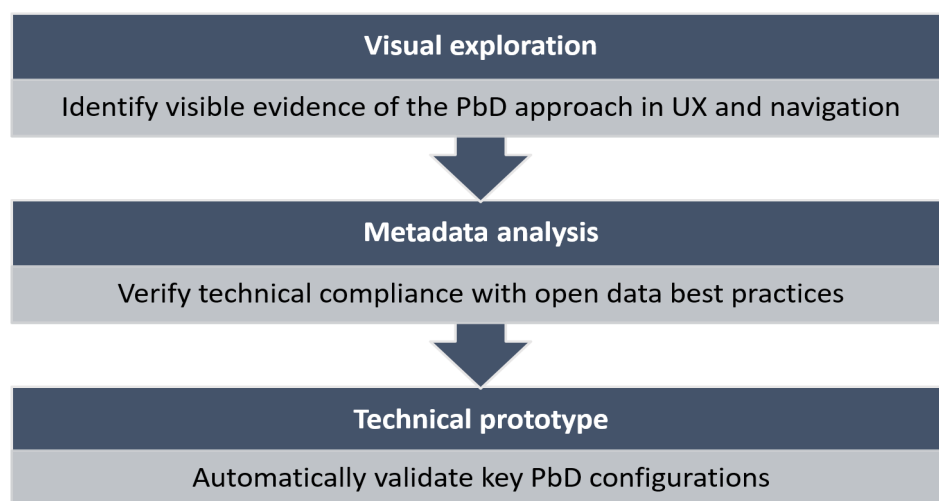


Figure 2. Methodological strategies and objectives of the study

Data Analysis and Coding Criteria

Each platform was analyzed against the PbD principles using a four-level scale: High - Medium - Low - None, which allowed us to identify:

- Common compliance patterns.
- Recurring gaps.
- Emerging best practices.

The findings were analyzed across all three strategies to ensure consistency and validation.

Validation and Ethical Criteria

A cross-validation process was implemented, comparing the outputs from:

- Manual visual inspection.
- Automated metadata extraction.
- Prototype-generated results.

Differences were discussed and resolved based on ethical and regulatory principles aligned with the PbD framework. Special attention was given to user autonomy, data minimization, and transparency indicators.

Table 2 presents the articulation between the seven Privacy-by-Design (PbD) principles and the three methodological strategies implemented in the study: visual exploration, metadata analysis, and prototype development.

The objective is to demonstrate how each strategy enabled the development of the different principles of the PbD approach, whether in functional, technical, or user experience aspects. This table identifies which principles were explicitly used in each stage of the analysis and which require further integration in future government platform design initiatives.

Table 2. Privacy-by-Design criteria applied in each methodological strategy

PbD Principles	Visual Exploration of Platforms	Metadata Analysis	Prototype Development
1. Proactive, not Reactive; Preventive, not Corrective	Identifies absence of warnings or anticipatory mechanisms.	Detects missing fields that could prevent privacy risks.	Prototype includes early-stage security validations.
2. Privacy by Default	Observes whether limited data is shared by default.	Evaluates anonymization settings or exposure by default.	Simulates environments where privacy is preconfigured.
3. Privacy Embedded into Design	Assesses whether UI/UX design includes privacy from the start.	Checks whether data structures avoid unnecessary exposure.	Architecture incorporates privacy as a baseline.
4. Full Functionality - Positive-Sum, not Zero-Sum	Evaluates how transparency and privacy coexist without functional trade-off.	Considers ethical boundaries without losing data utility.	Prototype balances utility with privacy safeguards.
5. End-to-End Security	Reviews encryption, authentication, or secure linking.	Identifies insecure formats or access control weaknesses.	Integrates security measures throughout data lifecycle.
6. Visibility and Transparency	Examines how data use and privacy policies are communicated.	Checks whether metadata declares sources, licenses, and purposes.	Prototype documents processes and enables traceability.
7. Respect for User Privacy	Identifies user control options or consent preferences.	Analyzes fields enabling user data governance.	Includes modules for user configuration and consent.

The table also visualizes the transversality of the PbD approach and its potential to guide both evaluation processes and design and development phases in digital public innovation contexts.

RESULTS

Application of the PbD-Evaluator Prototype

As part of this study, a technical tool named PbD-Evaluator was developed to assess the implementation of Privacy-by-Design (PbD) principles in Argentine government platforms. The prototype, implemented in Python and executed in a cloud-based environment (Google Colab), enabled automated validation of key privacy-related configurations, contributing directly to the empirical analysis.

The tool was designed around three core PbD principles:

- End-to-end security.
- Visibility and transparency.
- Respect for user privacy.

Based on these principles, the prototype evaluated the following criteria:

- Use of HTTPS and the presence of valid SSL certificates.
- Configuration of HTTP security headers (e.g., Strict-Transport-Security, Content-Security-Policy).
- Detection of third-party cookies and trackers.
- Availability and accessibility of privacy policies.
- Presence of user controls, such as cookie consent banners or personal data management forms.

The prototype operates through automated scripts using libraries such as requests, httpx, ssl, BeautifulSoup, and tldextract. It generates structured outputs in .csv format for further visualization and comparative analysis.

Table 3 summarizes the indicators implemented in the prototype and their mapping to the corresponding PbD principles:

The tool's modular architecture allows for dynamic URL input, minimal configuration, and reproducible results. This functionality made it possible to perform scalable privacy audits across multiple platforms efficiently and consistently.

Table 3. Summary of the evaluation criteria implemented in the prototype

Prototype Strategy	Indicator evaluated	Associated PbD Principle
HTTP Security Header Analysis	Presence of HSTS, CSP, X-Frame-Options, etc.	End-to-end security
Cookie and Tracker Scanning	Third-party cookies, persistence, identification	Respect for user privacy
Accessible Privacy Policy Verification	Functional link, readability, minimum required content	Visibility and transparency
Contact or Management Form Identification	Existence of personal data management mechanisms	User control and privacy by default

The PbD-Evaluator was applied to a curated sample of 18 Argentine public platforms. It enabled the identification of both common shortcomings, such as the lack of cookie consent tools or missing privacy policies, and promising practices, such as the presence of valid security certificates or secure HTTP configurations.

Figures 3 to 7 provide selected screenshots of the prototype's execution, using a test case from Argentina. gob.ar⁽⁴⁾, illustrating the technical procedures for analyzing secure connections, detecting trackers, verifying the visibility of privacy policies, and identifying the presence of user-facing data control mechanisms. These visual outputs exemplify how automated privacy diagnostics can enhance the evaluation of digital public services.

```
[ ] !pip install beautifulsoup4 requests tldextract httpx
import requests
from bs4 import BeautifulSoup
import re
import httpx
import ssl
import tldextract

Requirement already satisfied: beautifulsoup4 in /usr/local/lib/python3.11/dist-packages (4.13.4)
Requirement already satisfied: requests in /usr/local/lib/python3.11/dist-packages (2.32.3)
Collecting tldextract
  Downloading tldextract-5.3.0-py3-none-any.whl.metadata (11 kB)
Requirement already satisfied: httpx in /usr/local/lib/python3.11/dist-packages (0.28.1)
Requirement already satisfied: soupsieve>1.2 in /usr/local/lib/python3.11/dist-packages (from beautifulsoup4) (2.7)
Requirement already satisfied: typing-extensions>=4.0.0 in /usr/local/lib/python3.11/dist-packages (from beautifulsoup4) (4.14.0)
Requirement already satisfied: charset-normalizer<4,>=2 in /usr/local/lib/python3.11/dist-packages (from requests) (3.4.2)
Requirement already satisfied: idna<4,>=2.5 in /usr/local/lib/python3.11/dist-packages (from requests) (3.10)
Requirement already satisfied: urllib3<3,>=1.21.1 in /usr/local/lib/python3.11/dist-packages (from requests) (2.4.0)
Requirement already satisfied: certifi>=2017.4.17 in /usr/local/lib/python3.11/dist-packages (from requests) (2025.4.26)
Collecting requests-file>=1.4 (from tldextract)
  Downloading requests_file-2.1.0-py2.py3-none-any.whl.metadata (1.7 kB)
Requirement already satisfied: filelock>=3.0.8 in /usr/local/lib/python3.11/dist-packages (from requests-file) (3.18.0)
Requirement already satisfied: anyio in /usr/local/lib/python3.11/dist-packages (from requests-file) (4.9.0)
Requirement already satisfied: httpcore==1.* in /usr/local/lib/python3.11/dist-packages (from requests-file) (1.0.9)
Requirement already satisfied: h11>=0.16 in /usr/local/lib/python3.11/dist-packages (from httpcore==1.*->requests-file) (0.16.0)
Requirement already satisfied: sniffio>=1.1 in /usr/local/lib/python3.11/dist-packages (from anyio->requests-file) (1.3.1)
Downloading tldextract-5.3.0-py3-none-any.whl (107 kB)
107.4/107.4 kB 2.4 MB/s eta 0:00:00
Downloading requests_file-2.1.0-py2.py3-none-any.whl (4.2 kB)
Installing collected packages: requests-file, tldextract
Successfully installed requests-file-2.1.0 tldextract-5.3.0
```

Figure 3. Initialization of the environment and libraries for the automated privacy analysis

Figure 3 shows the initial setup of the work environment in Google Colab, where the libraries necessary for the PbD-Evaluator prototype to work are installed and imported. These include beautifulsoup and requests for browsing and analyzing HTML content on platforms, tldextract for decomposing web domains, and httpx along with SSL for performing security inspections on data transmission.

```
[ ] url = input("https://datos.gob.ar/").strip()
print(f"URL ingresada: {url}")

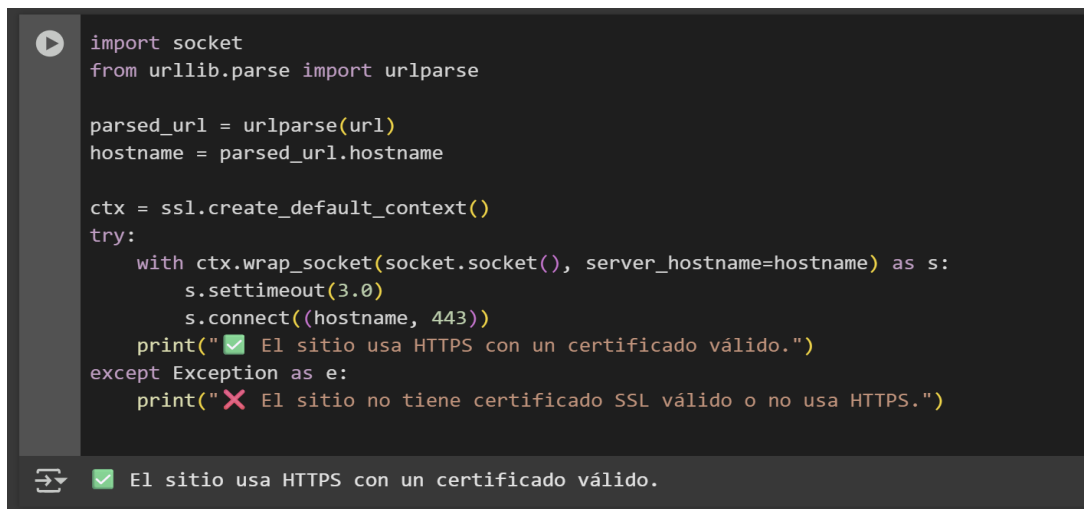
https://datos.gob.ar/https://datos.gob.ar/dataset/mineria-indice-produccion-minero-ipim
URL ingresada: https://datos.gob.ar/dataset/mineria-indice-produccion-minero-ipim
```

Figure 4. Dynamic URL Entry for Custom Assessment

Figure 4 shows the data entry module of the PbD-Evaluator prototype, where the user can enter the URL of a public platform for further analysis. In this example, the URL of the Argentine government's open data portal⁽⁴⁾ is used. This functionality allows for on-demand audits, adapting the prototype to different institutional or governmental environments. It also ensures flexibility in the assessment, facilitating the exploration of multiple sites without modifying the codebase.

Figure 5 shows the functionality for checking whether the platform being tested uses a secure communication protocol. Using libraries such as `ssl`, `socket`, and `urllib`, the script analyzes whether the website has a valid certificate and whether it operates under HTTPS. This validation is key to the “end-to-end security” principle of the Privacy-by-Design approach, as it guarantees the confidentiality of data during transmission. The test result is returned as a clear and straightforward message, indicating whether the platform meets this fundamental security requirement.

Figure 6 shows the functions required to audit the visibility of the privacy policy and the existence of tracking tools on public platforms. Using `requests` and `BeautifulSoup`, the script accesses the site's HTML content, checks for visible links to privacy policies, and detects the inclusion of scripts associated with common trackers such as Google Analytics, Facebook, or DoubleClick. This verification is aligned with the visibility and transparency principles of the Privacy-by-Design approach, as it allows users to identify whether they have access to clear information about the use of their data and whether tracking mechanisms exist that they have not been explicitly informed about.



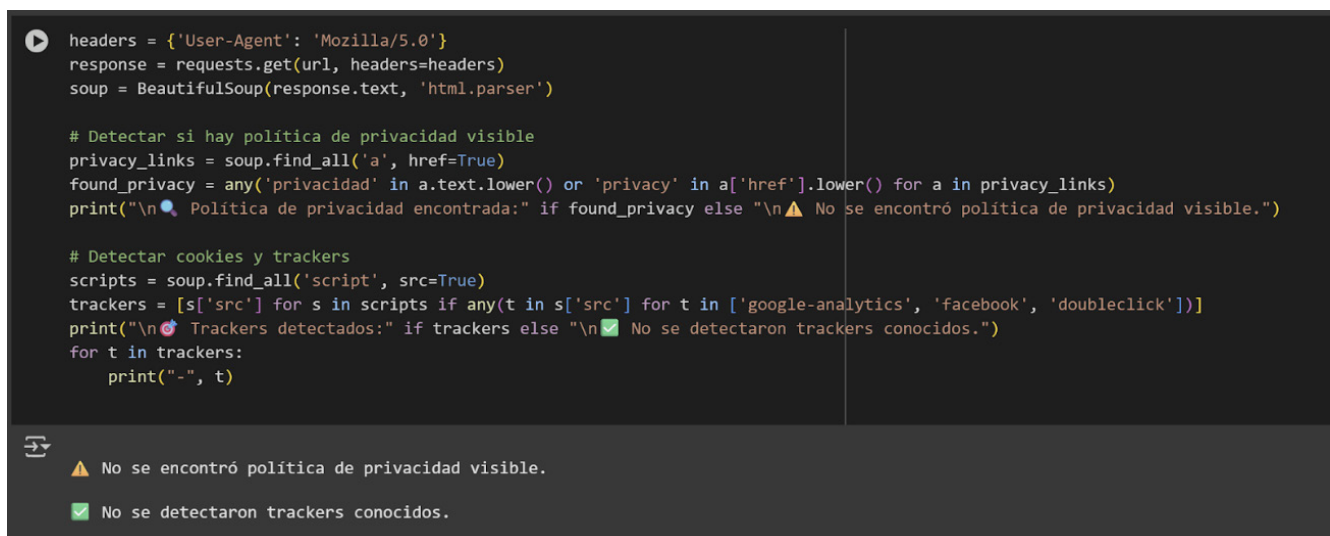
```
import socket
from urllib.parse import urlparse

parsed_url = urlparse(url)
hostname = parsed_url.hostname

ctx = ssl.create_default_context()
try:
    with ctx.wrap_socket(socket.socket(), server_hostname=hostname) as s:
        s.settimeout(3.0)
        s.connect((hostname, 443))
        print("✅ El sitio usa HTTPS con un certificado válido.")
except Exception as e:
    print("❌ El sitio no tiene certificado SSL válido o no usa HTTPS.")
```

✅ El sitio usa HTTPS con un certificado válido.

Figure 5. Automatic HTTPS and SSL Certificate Verification



```
headers = {'User-Agent': 'Mozilla/5.0'}
response = requests.get(url, headers=headers)
soup = BeautifulSoup(response.text, 'html.parser')

# Detectar si hay política de privacidad visible
privacy_links = soup.find_all('a', href=True)
found_privacy = any('privacidad' in a.text.lower() or 'privacy' in a['href'].lower() for a in privacy_links)
print("\n🔗 Política de privacidad encontrada:" if found_privacy else "\n⚠️ No se encontró política de privacidad visible.")

# Detectar cookies y trackers
scripts = soup.find_all('script', src=True)
trackers = [s['src'] for s in scripts if any(t in s['src'] for t in ['google-analytics', 'facebook', 'doubleclick'])]
print("\n🔍 Trackers detectados:" if trackers else "\n✅ No se detectaron trackers conocidos.")
for t in trackers:
    print("-", t)
```

⚠️ No se encontró política de privacidad visible.

✅ No se detectaron trackers conocidos.

Figure 6. Detecting Privacy Policies and Third-Party Trackers

Figure 7 shows a prototype module designed to identify potential forms requesting sensitive personal information, such as ID or document numbers. Therefore, it is necessary to verify the presence of controls related to cookie management. Using HTML content analysis techniques and regular expressions, the script

searches for forms that include terms linked to personal data and locates text or buttons that allow users to accept, reject, or configure the use of cookies. This functionality is aligned with the principles of privacy by default and respect for user privacy, as it allows users to detect potential violations of the duty to clearly inform about data collection, as well as the absence of informed consent mechanisms.

```
[ ] forms = soup.find_all('form')
has_sensitive_forms = any('dni' in f.text.lower() or 'documento' in f.text.lower() for f in forms)

print("\n📄 Formularios con campos sensibles encontrados:" if has_sensitive_forms else "\n✅ No se detectaron formularios sensibles.")

cookies_info = soup.find_all(string=re.compile("cookies|aceptar|configurar", re.IGNORECASE))
print("\n🍪 Indicadores de gestión de cookies detectados:" if cookies_info else "\n⚠️ No se encontraron controles de cookies visibles.")
for ci in cookies_info[:5]:
    print("-", ci.strip())
```

✅ No se detectaron formularios sensibles.

⚠️ No se encontraron controles de cookies visibles.

Figure 7. Detection of forms with sensitive fields and cookie controls

Overview of Evaluated Platforms

The PbD-Evaluator prototype was applied to a purposive sample of 18 government websites selected for their institutional relevance, thematic diversity, and management of sensitive personal data. These platforms represent a wide spectrum of digital public services in Argentina, including areas such as healthcare, migration, justice, education, taxation, and budget transparency.

The selection criteria ensured the inclusion of platforms that met the following conditions: public accessibility without login requirements, active dataset publication within the last 12 months, an institutional purpose linked to transparency or citizen participation, and the presence of interaction or information download mechanisms. Furthermore, efforts were made to include platforms from various jurisdictional and administrative levels to ensure broader representativeness.

Table 4 lists the evaluated platforms alongside their institutional roles and the justification for their inclusion in the study.

Ref	Website	Main Focus / Justification
1	https://www.srt.gob.ar	Superintendence of Occupational Risks (occupational health procedures)
2	https://www.pami.org.ar	Health services and enrollment for older adults
3	https://www.argentina.gob.ar/interior/migraciones	National Directorate of Migration (immigration data)
4	https://www.sigen.gob.ar	State internal audit and oversight
5	https://www.cnrt.gob.ar	Supervision of road and railway transport
6	https://www.argentina.gob.ar/educacion	Educational policies and access to programs
7	https://www.jus.gob.ar	Ministry of Justice (access to judicial and institutional data)
8	https://www.argentina.gob.ar/produccion	Support programs for production, businesses, and SMEs
9	https://www.argentina.gob.ar/salud	Information and services from the Ministry of Health
10	https://www.datos.gob.ar	National open data portal
11	https://www.anses.gob.ar	Social security, procedures involving sensitive data
12	https://www.argentina.gob.ar	Centralized official State portal
13	https://presupuestoabierto.gob.ar	Budget transparency
14	https://tramitesadistancia.gob.ar	Electronic procedures management system
15	https://www.afip.gob.ar	Federal tax administration
16	https://www.ssalud.gob.ar	Superintendence of Health Services
17	https://www.argentina.gob.ar/jefatura/sintys	National Tax and Social Identification System; integrates databases for social programs
18	https://www.indec.gob.ar/	National Institute of Statistics and Censuses; large volume of statistical data with careful privacy handling

The selection of government websites analyzed using the PbD-Evaluator prototype was based on their institutional relevance, thematic diversity, and handling of sensitive personal data. These portals represent a broad range of digital public services, from healthcare, migration, and justice to budget transparency and tax management. The analysis aims to assess the incorporation of Privacy-by-Design principles in their configurations, privacy controls, and visible policies, providing a comprehensive view of the current state of data protection on digital platforms in the Argentine public sector.

Table 5 presents a summary of the results obtained using the PbD-Evaluator prototype in relation to three fundamental criteria of the Privacy-by-Design approach: the implementation of secure connections (HTTPS with a valid certificate), the visibility of privacy policies, and the presence of cookie management mechanisms. These aspects represent minimum conditions to guarantee a secure and transparent browsing environment for users. The verification was performed automatically on each government website included in the study.

Table 5. Basic Security and Privacy Aspects

Ref	HTTPS with valid certificate (✓/✗)	Visible privacy policy (✓/⚠/⊖)	Visible cookie management controls (✓/⚠)
1	✓ The site uses HTTPS with a valid certificate.	⚠ No visible privacy policy found.	⚠ No visible cookie controls found.
2	✗ The site does not use HTTPS or has no valid SSL certificate.	⊖ Not evaluated (ConnectTimeoutError)	⚠ No visible cookie controls found.
3	✓ The site uses HTTPS with a valid certificate.	⚠ No visible privacy policy found.	⚠ No visible cookie controls found.
4	✗ The site does not use HTTPS or has no valid SSL certificate.	⊖ Not evaluated (ConnectTimeoutError)	⚠ No visible cookie controls found.
5	✓ The site uses HTTPS with a valid certificate.	⚠ No visible privacy policy found.	⚠ No visible cookie controls found.
6	✓ The site uses HTTPS with a valid certificate.	⚠ No visible privacy policy found.	⚠ No visible cookie controls found.
7	✓ The site uses HTTPS with a valid certificate.	⚠ No visible privacy policy found.	⚠ No visible cookie controls found.
8	✓ The site uses HTTPS with a valid certificate.	⚠ No visible privacy policy found.	⚠ No visible cookie controls found.
9	✓ The site uses HTTPS with a valid certificate.	⚠ No visible privacy policy found.	⚠ No visible cookie controls found.
10	✓ The site uses HTTPS with a valid certificate.	⚠ No visible privacy policy found.	⚠ No visible cookie controls found.
11	✗ The site does not use HTTPS or has no valid SSL certificate.	⊖ Not evaluated (SSL CertVerification Error)	⚠ No visible cookie controls found.
12	✓ The site uses HTTPS with a valid certificate.	⚠ No visible privacy policy found.	⚠ No visible cookie controls found.
13	✗ The site does not use HTTPS or has no valid SSL certificate.	⊖ Not evaluated (SSL CertVerification Error)	⚠ No visible cookie controls found.
14	✗ The site does not use HTTPS or has no valid SSL certificate.	⊖ Not evaluated (ConnectTimeoutError)	⚠ No visible cookie controls found.
15	✗ The site does not use HTTPS or has no valid SSL certificate.	⚠ No visible privacy policy found.	⚠ No visible cookie controls found.
16	✓ The site uses HTTPS with a valid certificate.	⚠ No visible privacy policy found.	⚠ No visible cookie controls found.
17	✓ The site uses HTTPS with a valid certificate.	⚠ No visible privacy policy found.	⚠ No visible cookie controls found.
18	✓ The site uses HTTPS with a valid certificate.	⚠ No visible privacy policy found.	⚠ No visible cookie controls found.

Table 6 expands the analysis by highlighting key elements related to the exposure of personal data and the use of tracking technologies. It identifies whether the sites present forms with sensitive fields (such as ID or identifying information), as well as the detection of known trackers (e.g., Google Analytics or Facebook Pixel). In addition, relevant observations that emerged from the analysis are included, allowing for the identification of best practices or areas for improvement in terms of active privacy.

Based on the survey presented in tables 5 and 6, the findings were analyzed using visual representations that allow a clearer understanding of the distribution of compliance with key aspects of the Privacy-by-Design approach. These visualizations show the results obtained by the prototype and offer a comparison of the minimum security and digital transparency conditions implemented by government websites. The first graph addresses the presence of valid certificates in HTTPS connections, considered an essential standard for ensuring the integrity and confidentiality of transmitted data.

Figure 8 shows the number of cases regarding verification of a secure connection using HTTPS with a valid certificate. Of the 18 websites analyzed, 12 meet this basic security requirement, representing 66,7 % of the total. However, six platforms still have flaws in the implementation of SSL certificates or do not use HTTPS, which weakens the protection of communications between the user and the server. This situation can expose

citizens to unnecessary risks when exchanging personal information, especially in government services that manage sensitive data.

Ref	Trackers Detected (list or "No")	Forms with Sensitive Fields (☑/✗)
1	☑ No known trackers detected.	☑ No sensitive forms detected.
2	⦿ Not evaluated (ConnectTimeoutError)	☑ No sensitive forms detected.
3	☑ No known trackers detected.	☑ No sensitive forms detected.
4	⦿ Not evaluated (ConnectTimeoutError)	☑ No sensitive forms detected.
5	☑ No known trackers detected.	☑ No sensitive forms detected.
6	☑ No known trackers detected.	☑ No sensitive forms detected.
7	☑ No known trackers detected.	☑ No sensitive forms detected.
8	☑ No known trackers detected.	☑ No sensitive forms detected.
9	☑ No known trackers detected.	☑ No sensitive forms detected.
10	☑ No known trackers detected.	☑ No sensitive forms detected.
11	⦿ Not evaluated (SSL CertVerification Error)	☑ No sensitive forms detected.
12	☑ No known trackers detected.	☑ No sensitive forms detected.
13	⦿ Not evaluated (SSL CertVerification Error)	☑ No sensitive forms detected.
14	⦿ Not evaluated (ConnectTimeoutError)	☑ No sensitive forms detected.
15	☑ No known trackers detected.	☑ No sensitive forms detected.
16	☑ No known trackers detected.	☑ No sensitive forms detected.
17	☑ No known trackers detected.	☑ No sensitive forms detected.
18	☑ No known trackers detected.	☑ No sensitive forms detected.

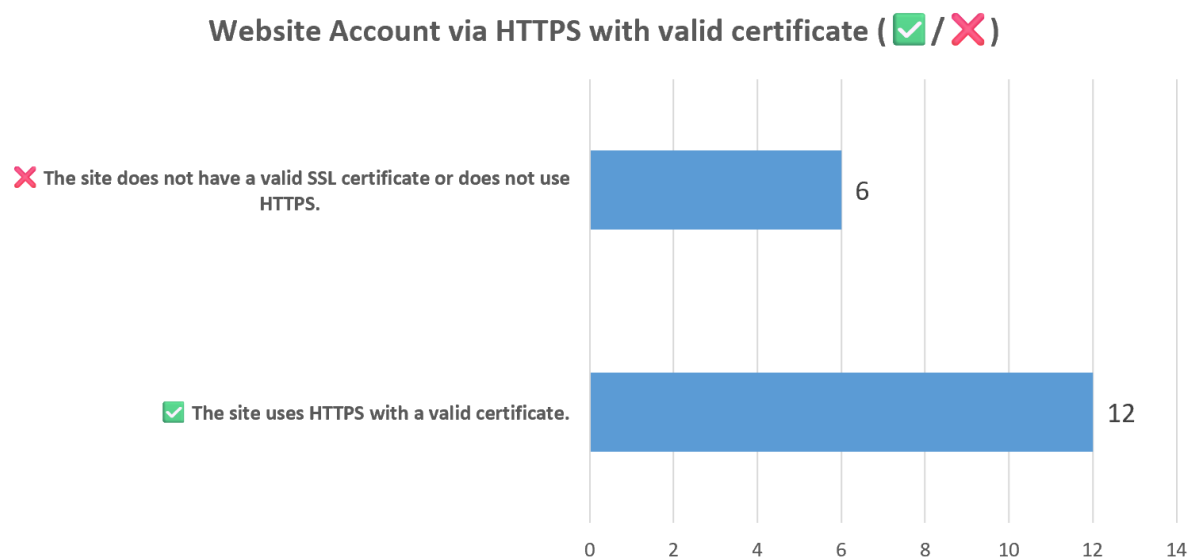


Figure 8. Distribution of government websites according to the use of HTTPS with a valid certificate

Figure 9 shows the results regarding the visibility of privacy policies on the analyzed sites. This aspect constitutes a fundamental pillar of the transparency principle within the Privacy-by-Design approach, as it allows users to understand how their personal information will be treated. Of the total platforms evaluated, 13 did not find a privacy policy posted in an accessible manner (\triangle), which represents a critical shortcoming in terms of institutional communication and informed consent. Furthermore, the evaluation was not possible in 5 sites due to technical errors: 3 due to connection errors (*ConnectTimeoutError*) and 2 due to SSL certificate verification failures. These results demonstrate the need to improve personal data protection practices on public sector portals.

Website Account by Visible privacy policy (🟢/⚠️)

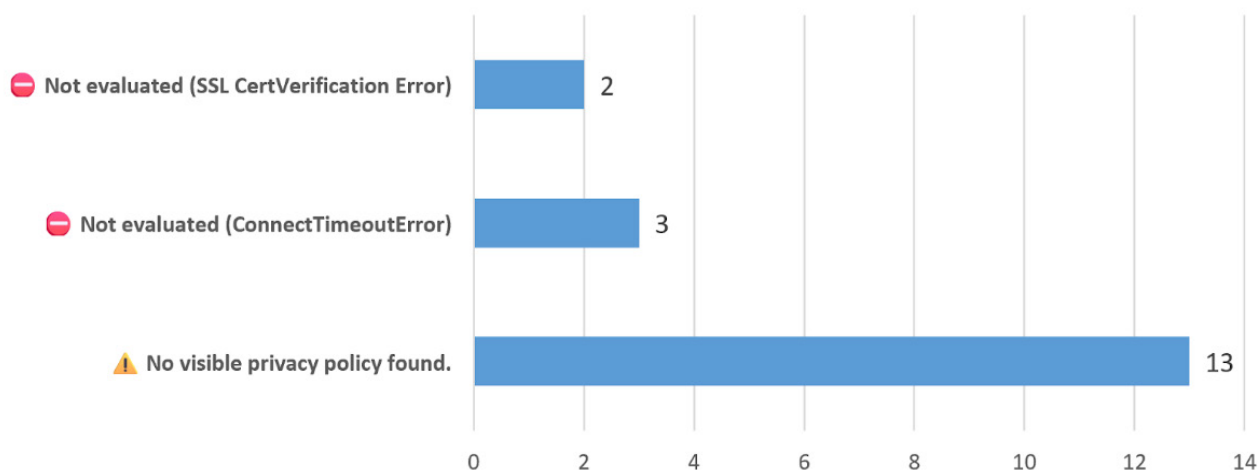


Figure 9. Distribution of government websites by privacy policy visibility

Furthermore, figure 10 provides an overview of the presence of tracking technologies on the evaluated sites, particularly well-known trackers such as Google Analytics, Facebook Pixel, and other similar tools. Detecting these elements is important from an active privacy perspective, as they involve the collection of browsing data, often without explicit consent. In this analysis, 13 sites did not show any trackers detectable by the tools used (🟢), which is a desirable practice in terms of data minimization and user respect. However, 5 sites could not be properly evaluated: 3 due to connection timeout errors (ConnectTimeoutError) and 2 due to SSL certificate verification errors. These results highlight the need to incorporate stricter third-party auditing practices and greater vigilance regarding invisible technologies that can compromise privacy in public digital environments.

Website Account by Trackers detected (list or "No")

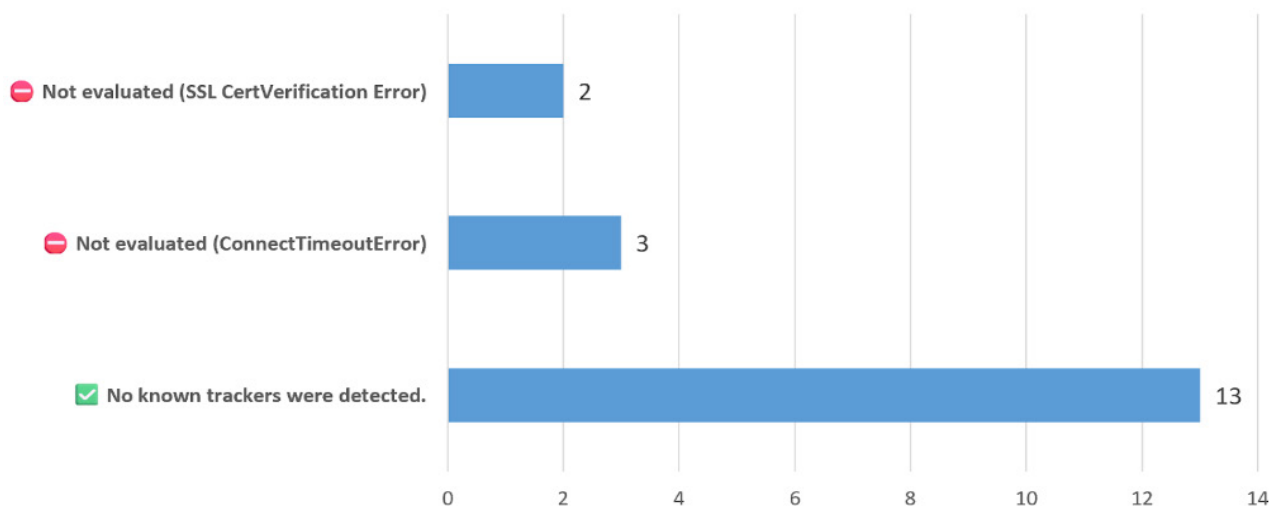


Figure 10. Distribution of government websites by tracker detection

Finally, regarding forms that could involve the collection of sensitive personal data, such as document numbers or other identifiers, the analysis did not identify any positive cases in any of the 18 sites evaluated. However, this finding should not be interpreted as a guarantee of privacy, as it could be due to the lack of automatic detection of embedded or dynamic forms. Furthermore, regarding visible mechanisms for cookie management, all the sites analyzed lacked accessible controls for the configuration or informed acceptance of cookies, which represents a critical weakness in terms of compliance with the principles of transparency and informed consent of the Privacy-by-Design approach. These results reinforce the need to move toward more comprehensive implementation of practices that guarantee privacy by design in public sector digital services.

These findings, presented through both tabular summaries and visualizations, provide a diagnostic snapshot

of how Privacy-by-Design principles are, or are not, being operationalized across a diverse sample of Argentine government platforms. While some basic standards, such as the use of HTTPS, are widely met, significant shortcomings remain in critical areas like transparency, cookie management, and proactive user control. The data collected through the PbD-Evaluator prototype reveal not only recurring gaps but also opportunities to strengthen public sector privacy practices through more systematic design and oversight. These patterns are examined in greater depth in the following section, which interprets the results from a strategic and ethical perspective.

DISCUSSION

The analysis conducted using the PbD-Evaluator prototype on 18 Argentine government websites revealed significant patterns in the implementation of privacy and personal data protection practices. First, it was verified that all sites use HTTPS, guaranteeing a secure connection that protects the confidentiality and integrity of the information transmitted. This aspect is a basic requirement for digital security and reflects a widespread commitment, as noted by various authors in the field of cybersecurity.^(25,26,27)

However, despite this secure infrastructure, cookie management presents a considerable challenge. For example, none of the analyzed sites displayed visible controls for user cookie management. The absence of clear mechanisms for consent and active cookie management can affect transparency and citizen trust,⁽²⁸⁾ which is in line with previous studies that emphasize the importance of user control in personal data management.⁽²⁹⁾

Regarding forms with sensitive fields, the results indicated that no forms were detected in the 18 sites that collect sensitive data, which could be interpreted as a precautionary measure to minimize risks. However, this finding invites us to reflect on the possible functional limitation that this may represent for the offer of digital public services, in relation to the work presented in which the importance of maintaining the balance between data minimization and functionality is presented.^(30,31)

The analysis of privacy policies showed that, although most sites have such policies, the accessibility of information varies considerably. Therefore, it is necessary to highlight the fact that some portals present documents with technical or legal language, making them difficult to understand for non-specialized users. This aspect is precisely reflected in some research that highlights the need for understandable policies to strengthen trust and regulatory compliance.^(32,33,34)

Furthermore, although a moderate presence of trackers and third-party tools was detected on the analyzed sites, their existence calls for reflection in the sense that potential risks in terms of privacy could be present. These elements can collect browsing information without the explicit knowledge of the user, which violates the principle of transparency. Some research warns about the impact of these practices, since data processing is beyond the direct control of public institutions.^(35,36) This finding reinforces the need for a proactive assessment of technological integrations in digital government environments, using a rights-centered approach.

Importantly, these findings highlight the importance of incorporating a more systematic Privacy-by-Design approach that not only ensures the technical protection of data but also improves transparency and user control over their information. This comprehensive approach is essential for moving toward digital governance aligned with international data protection principles.^(37,38,39)

This work seeks to provide empirical evidence and generate a list of best practices on strategic recommendations that contribute to the development of more sustainable digital public policies, achieving smart and people-centered governance. On the other hand, one of the limitations of this work is its focus on the technical analysis of 18 government websites, without addressing in-depth the degree of effective privacy policy compliance or considering users' perspectives on these practices. Furthermore, the PbD-Evaluator prototype was applied to only a few websites, so it would be interesting to expand its validation with more application cases on public government platforms.

CONCLUSIONS

This work identified progress and challenges in the implementation of privacy best practices on Argentine government websites. While the sample analyzed websites has secure connections and no forms with sensitive data were detected, there are significant opportunities for improvement in aspects such as cookie management, the clarity of privacy policies, and the incorporation of technologies.

Regarding the findings, it is noted that although basic protection measures are in place, further user-centered analysis is still needed. The Privacy-by-Design approach aims to address privacy from the outset and across the board, not just as a technical requirement, but as a value that permeates design, which should be considered when implementing decisions in the digital technology field.

As future lines of research for this project, it is necessary to continue developing accessible evaluation tools, such as the PbD-Evaluator prototype, that allow for simple monitoring of how privacy principles are applied on public platforms. It would also be desirable for these assessments to encourage concrete actions in regulatory reviews, as well as improvements to the user experience, which would provide greater transparency in use.

Future research could expand the sample, incorporate qualitative methodologies, and analyze the relationship between institutional design, privacy, and citizen trust. Likewise, it would be important to develop more tools like the PbD-Evaluator in collaboration with public agencies, reinforcing a sustainable digital transformation for rights.

BIBLIOGRAPHIC REFERENCES

1. Valdiviezo GT, Alegre LR, Ayala DM, Padilla RD. Digital transformation in Latin America: a systematic review. *Rev Venez Gerenc.* 2022;27(100):1519-36.
2. Aucancela AM. The era of big data and open data in public administration. *Rev Eurolatinoam Derecho Adm.* 2021;8(1):61-76.
3. De Los Ríos Rueda MA, Galvis-Tovar JE. Colombia: Integration of Health Data Protection Regulations and the Case for International Health Data Transfers. In: *International Transfers of Health Data: A Global Perspective*. Singapore: Springer Nature Singapore; 2025. p. 239-59.
4. Argentina.gob.ar. Datos abiertos [Internet]. [cited 2025 Jul 6]. Available from: <https://www.argentina.gob.ar/datos-abiertos>
5. Buenos Aires Data. BA Data [Internet]. [cited 2025 Jul 6]. Available from: <https://data.buenosaires.gob.ar/>
6. Hossain MA, Dwivedi YK, Rana NP. State-of-the-art in open data research: Insights from existing literature and a research agenda. *J Organ Comput Electron Commer.* 2016;26(1-2):14-40.
7. Hondares YP, Almora RM, Véliz AP. La protección de datos personales. *Rev Científica Ecociencia.* 2021;8:126-61.
8. León-Arroba RC, López-Sevilla GM. A Security-by-Design Architecture Proposal for the Protection of Personal Data in Public Entities. *MQRInvestigar.* 2024;8(4):4192-218.
9. Meyers G, Van Oirsouw CC, Keymolen EL, Goossens J. After the announcement: an interdisciplinary analysis of blockchain development in governments. *Policy Des Pract.* 2023;6(4):505-19.
10. Wang X. The Problems and Optimization Paths of Digital Government Governance in Shandong Province. In: *Proc 2nd Int Conf Digit Econ Manag Sci (CDEMS)*. Atlantis Press; 2024. p. 504-10.
11. Shafik W. Shaping the Next Generation Smart City Ecosystem. In: *Smart Cities: Innovations, Challenges and Future Perspectives*. Cham: Springer Nature Switzerland; 2024. p. 3-52.
12. Andrade VC, Gomes RD, Reinehr S, Freitas CO, Malucelli A. Privacy by design and software engineering: a systematic literature review. In: *Proc XXI Braz Symp Softw Qual.* 2022. p. 1-10.
13. Cavoukian A. Privacy by design: The seven foundational principles. *IAPP Resour Cent.* 2021.
14. Porcelli AM. La protección de los datos personales en el entorno digital. *Quaestio iuris.* 2019;12(2).
15. European Union. Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR).
16. Yanamala AK, Suryadevara S. Navigating data protection challenges in the era of AI: A comprehensive review. *Rev Int Artif Med.* 2024;15(1):113-46.
17. Matheus R, Janssen M, Janowski T. Design principles for creating digital transparency in government. *Gov Inf Q.* 2021;38(1):101550.
18. Del-Real C, De Busser E, van den Berg B. A systematic literature review of security and privacy by design. *Int Rev Law Comput Technol.* 2025:1-32.
19. Jowarder RA, Jahan S. Quantum computing in cyber security. *World J Adv Eng Technol Sci.* 2024;13(1):330-9.

20. Quach S, Thaichon P, Martin KD, Weaven S, Palmatier RW. Digital technologies: tensions in privacy and data. *J Acad Mark Sci.* 2022;50(6):1299-323.
21. Eom SJ, Lee J. Digital government transformation in turbulent times. *Gov Inf Q.* 2022;39(2):101690.
22. George G, Merrill RK, Schillebeeckx SJ. Digital sustainability and entrepreneurship. *Entrep Theory Pract.* 2021;45(5):999-1027.
23. Feng S, Zhang R, Li G. Environmental decentralization, digital finance and green technology innovation. *Struct Change Econ Dyn.* 2022;61:70-83.
24. Castro C, Lopes C. Digital government and sustainable development. *J Knowl Econ.* 2022;13(2):880-903.
25. Yee CK, Zolkipli MF. Review on confidentiality, integrity and availability in information security. *J ICT Educ.* 2021;8(2):34-42.
26. Kim L. Cybersecurity. In: *Nursing Informatics.* Cham: Springer; 2022. p. 391-410.
27. Jha RK. Cybersecurity and confidentiality in smart grid. *Recent Res Rev J.* 2023;2(2):215-41.
28. Nouwens M, Liccardi I, Veale M, Karger D, Kagal L. Dark patterns after the GDPR. In: *Proc CHI Conf Hum Factors Comput Syst.* 2020. p. 1-13.
29. Borberg I, Hougaard R, Rafnsson W, Kulyk O. So I sold my soul: Effects of dark patterns. In: *USEC Symp.* 2022.
30. Georgiadis G, Poels G. Towards a privacy impact assessment methodology. *Comput Law Secur Rev.* 2022;44:105640.
31. Aljeraisy A, Barati M, Rana O, Perera C. Exploring relationships between privacy by design and privacy laws. *arXiv [Preprint].* 2022 Oct 6. Available from: <https://arxiv.org/abs/2210.03520>
32. Zaeem RN, Barber KS. Economics of Privacy: Privacy, a Machine Learning Perspective. In: *Encyclopedia of Cryptography, Security and Privacy.* Cham: Springer; 2025. p. 745-7.
33. Mohan N, KA Z. Assessing the impact of privacy policy motivations. *Int J Hum Comput Interact.* 2025;1-4.
34. Reeck C, Guo X, Dimoka A, Pavlou PA. Uncovering the neural processes of privacy. *Inf Syst Res.* 2024;35(2):727-46.
35. Adam S, Makhortykh M, Maier M, et al. Improving quality of web tracking: challenges and new solutions. *Soc Sci Comput Rev.* 2024 Oct 16.
36. Choi JR, Kim S. Predicting privacy protection and self-tracking behaviors in smart health. *Telemat Inform.* 2024;86:102069.
37. Andraško J, Mesarčik M. Data protection in EU electronic identification. *TalTech J Eur Stud.* 2021;11(2).
38. Politou E, Alepis E, Virvou M, Patsakis C. Privacy and data protection challenges in the distributed era. Cham: Springer; 2022.
39. Alic D. Data protection and cybersecurity regulations in AI governance. *CEU Thesis Repos.* 2021 Jun.

FINANCING

The author received no funding for this research.

CONFLICTS OF INTEREST

The author declares no conflicts of interest.

AUTHORSHIP CONTRIBUTION

Conceptualization: Roxana Martínez.

Data curation: Roxana Martínez.

Research: Roxana Martínez.

Methodology: Roxana Martínez.

Prototype: Roxana Martínez.

Validation: Roxana Martínez.

Drafting - original draft: Roxana Martínez.

Writing - proofreading and editing: Roxana Martínez.