DigitalRightsFoundation
"KNOW YOUR RIGHTS"

The Cost of Going Digital: Evaluating Rights Risks in Pakistan's Digital Governance

Policy Brief

CONTEXT

Across the world, states are increasingly adopting "digital nation" models to modernize governance, streamline service delivery, and enhance interaction between states and citizens. Pakistan now stands at a similar crossroads, seeking to build an integrated digital state through legal and institutional reforms.

With increasing internet penetration and expanding digital infrastructure, Pakistan has the potential to develop a robust and inclusive digital economy. To harness this potential, the government has launched initiatives under the Digital Pakistan Vision, such as the Digital Economy Enhancement Project (DEEP)[1], reflecting a national commitment to harnessing technology for governance and development. Complementary frameworks, including the National Artificial Intelligence (AI) Policy, further demonstrate Pakistan's broader shift toward data-driven governance.

A key milestone in this shift is the Digital Nation Act 2025 (DNA 2025)[2], originally introduced as the Digital Nation Pakistan Bill. The DNA 2025 envisions a unified digital ecosystem that integrates state institutions and citizens through a centralized framework of digital identities and data repositories. Its stated objectives include improving public service delivery, administrative efficiency, and promoting innovation. The Act establishes three central institutions: National Digital Commission (NDC) to provide strategic direction, Pakistan Digital Authority (PDA) to implement and oversee the National Digital Masterplan, and Strategic Oversight Committee (SOC) to monitor and ensure accountability of digital initiatives.

While these bodies are intended to strengthen coordination and efficiency, the centralisation of citizen data raises profound privacy and human rights concerns. The Act's extensive powers, limited public consultation, and lack of clear

1 https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099030524162525956
2 https://pakistancode.gov.pk/pdffiles/administrator2c2fd2fe7da1a657c40589a0705b3e20.pdf

safeguards pose a risk to citizens' rights to privacy, autonomy, and equality before the law, rights protected under Articles 4, 9, 14, and 25 of the Constitution of Pakistan.

Parallel to this, the Personal Data Protection Bill (PDPB)[3], which is still pending consultation, aims to provide the necessary legal foundation for data privacy in Pakistan. It proposes the establishment of a National Commission for Personal Data Protection (NCPDP) and introduces principles of consent, purpose limitation, and accountability. However, in its current form, the draft falls short of international human rights and data protection best practices, as outlined in the European Union General Data Protection Regulations (GDPR)[4]. It remains below GDPR standards, due to weak governance, vague definitions, diluted data subject rights, and expansive exemptions. Until the PDPB is enacted, Pakistan lacks a comprehensive framework to regulate the collection, storage, and sharing of personal data by state or private entities. This gap exposes citizens to unchecked data use, surveillance, and discriminatory profiling, raising critical concerns about how digitalization affects the protection and realization of human rights, particularly for marginalized communities

When Digital Progress Threatens Human Rights

Pakistan's digital transformation, though aimed at innovation, has already exposed significant human rights challenges.

1. Unregulated Data Collection and Use

The DNA 2025 centralizes citizen data across government departments, linking digital identity systems, social protection programs, and economic records. While designed to streamline governance, this integration significantly expands the state's capacity to collect, store, and process personal data. Without proper data protection safeguards, such centralization directly puts citizens' privacy and security at risk. Moreover, this centralized data hub risks re-categorizing citizens' information into higher-risk tiers related to highly sensitive Personal Identifiable Information (PII), whose sensitivity directly dictates the protective measures and compliance standards that should be applied[5].

3 https://moitt.gov.pk/SiteImage/Misc/files/Final%20Draft%20Personal%20Data%20Protection%20Bill%20May%202023.pdf

4 https://digitalrightsfoundation.pk/wp-content/uploads/2023/07/Legal-Analysis-Statement-on-PDPB-July-2023.pdf

5 https://www.deasylabs.com/blog/pii-classification-levels-understanding-the-hierarchy-of-personal-data-protection

At the core of this digital framework lies the National Database and Registration Authority (NADRA), the foundation of Pakistan's identity system and the primary custodian of citizens' personal data. Introduced without any human rights due diligence or impact assessment[6] NADRA's system has already demonstrated the inherent risks of unchecked digital centralization. It has a documented record of excluding gender-diverse individuals[7], arbitrary and discriminatory cancellation of identity cards on ethnic[8] and religious grounds, and repeated data breaches exposing sensitive personal information. Administrative errors within its databases have also led to wrongful denials of access to essential services, including healthcare, education, and social protection.

2. Exclusion Through Data

Digital governance systems often assume that data is neutral; however, biases built into these systems can reinforce existing inequalities. Pakistan's experience with digital identity management has already shown how automation, inadequate training, and rigid verification protocols can disproportionately affect marginalized groups.

For this policy brief, DRF spoke to a transgender activist who shared their experience with obtaining a CNIC through NADRA's digital system. According to their account, applying for or updating a CNIC remains a deeply exclusionary process, shaped by both technological and procedural barriers that marginalize transgender individuals. Many applicants face delays due to staff confusion over the "X" gender marker and inconsistent digital record-keeping. The respondent also explained that changes linked to educational or employment records are not automatically updated across digital databases, resulting in multiple mismatches that hinder access to welfare programmes, SIM registration, and digital financial services.

Similarly, members of religious minorities, particularly those from Christian and Ahmadiyya communities, have encountered discriminatory practices in the digital identification process. In one notable case[9], a Christian citizen had to wage a protracted legal battle for 7 months merely to have his religious affiliation accurately reflected on his national ID card, after being wrongfully identified as Muslim in NADRA's records, and the correction was only achieved through judicial intervention.

---

6 https://digitalrightsfoundation.pk/wp-content/uploads/2025/06/Op-Ed-World-Bank-Digital-Public-Infrastructure-and-Human-Rights.pdf

7 https://www.dawn.com/news/1773898

8 https://www.aljazeera.com/features/2021/9/29/stateless-ethnic-bengalis-pakistan

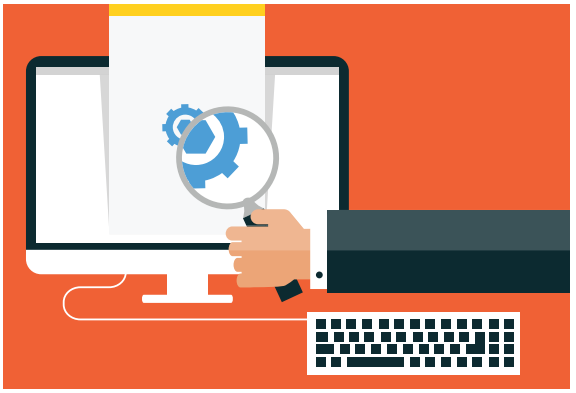
9 https://www.christiandaily.com/news/christian-in-pakistan-wins-faith-change-on-national-id-card

DRF spoke to a representative from the Christian community who pointed out a similar experience of persistent errors in NADRA's entry system, which can only be corrected through lengthy bureaucratic or judicial processes. He noted that when individuals return to their original faith after forced religious conversion, NADRA's digital registry often fails to update their records, leaving both them and their children misclassified. These errors cascade into voter registration and other digital systems, undermining political participation and access to essential services.

DRF also spoke to a woman from a marginalized community who attempted to apply for her ID card and visited the NADRA office on three separate occasions, yet encountered persistent gender-based discrimination. Despite informing officials that her husband resides in another city and that she has initiated legal proceedings for separation, the NADRA representative repeatedly refused to process her application without her husband's presence for a thumb impression.

These cases collectively demonstrate how exclusionary practices and systemic biases within digital identity systems can transform routine administrative processes into significant barriers, reinforcing the need for rights-based, inclusive, and accountable data governance mechanisms.

Surveillance Without Safeguards



The DNA 2025 grants broad powers to the Pakistan Digital Authority (PDA) to integrate and share citizen data across institutions. Without judicial authorization or independent oversight, this centralisation opens the door to near constant state surveillance under the guise of digital efficiency. Existing practices already illustrate these dangers - the telecom regulator's installation of a Lawful Intercept Management System (LIMS) allows state agencies to monitor users' calls, messages, and internet activity without transparent legal oversight[10], while the Peshawar Police's notorious "Hotel Eye" app, tracks hotel guests in real time under the pretext of enhancing security, exemplifies how technological interventions can outpace accountability mechanisms.[11] By merging identity, financial, and social data, the state gains unprecedented visibility into citizens' lives, with little regard for consent, purpose, or data retention.

10 https://www.dawn.com/news/1843299
11 https://www.arabnews.com/node/1438276/pakistan

This unchecked surveillance operating without transparent limits affects everyone but hits human rights defenders and journalists the hardest, fostering fear, intimidation, and self-censorship. The media faces censorship, websites and YouTube channels are blocked, and reporters are geo-tracked, further exacerbating their experience as front-line defenders. The 2025 World Press Freedom[12] ranking places Pakistan at 158th of 180 countries, underscoring the dangers that vulnerable groups face daily. Without a comprehensive data protection law, such initiatives normalize intrusion, erode public trust, and enable surveillance of dissent, journalists, and marginalized communities.

Comparative Global Best Practices

To ensure that data protection in Pakistan reflects both global best practices and local realities, it is essential to learn from international models that prioritise the protection of vulnerable groups. The EU GDPR is widely regarded as the world's most comprehensive data protection framework, setting out principles and rights that place individuals, not institutions, at the centre of data governance. Article 5[13] mandates that data collection must be limited to what is strictly necessary for the stated purpose, while Article 35[14] mandates Data Protection Impact Assessments (DPIAs) for high-risk processing.

12 https://observerdiplomat.com/pakistan-ranked-158-of-180-in-the-world-press-freedom-index-2025/
13 https://gdpr-info.eu/art-5-gdpr/
14 https://gdpr-info.eu/art-35-gdpr/

South Africa's Protection of Personal Information Act (POPIA) prohibits processing sensitive data unless specific conditions are met, including explicit consent, legal obligations, protection of vital interests, or processing by religious, philosophical, or cultural organisations relating to their own members (Sections 27-33)[15]. In contrast, Pakistan's draft Personal Data Protection Bill (2023) does not include a narrowly defined set of lawful exceptions. The Bill should incorporate mandatory DPIAs for high-risk processing activities, particularly those undertaken by public bodies such as NADRA, welfare programmes, and health databases. Embedding these requirements would ensure that the handling of identity-linked data is transparent, necessary, and designed to prevent profiling, surveillance, and discrimination against minority communities.

The Estonian Personal Data Protection Act[16] (2018) sets out clear rules that personal data should only be collected for specific and lawful reasons and kept only as long as necessary (Section 14).[17] Alongside this, the X-Road Data Exchange Layer Framework[18] ensures that government institutions store data separately rather than in one central database, which helps prevent large-scale misuse or breaches. It also requires every instance of data access to be recorded, including who viewed the data and when (Section 51).[19] Citizens can access these records through an online portal, ensuring transparency and accountability. For Pakistan, especially in relation to religious and ethnic minorities, adopting similar measures, such as keeping data decentralised, logging all access, and giving citizens the right to see when their data is used, would make data handling more transparent and help prevent misuse or discrimination.

15 https://popia.co.za/protection-of-personal-information-act-popia/chapter-3-2/chapter-3-part-b/
16 https://www.riigiteataja.ee/en/eli/523012019001/consolide
17 https://www.riigiteataja.ee/en/eli/523012019001/consolide
18 https://eid.hsiaoa.tw/estonian-x-road/appendix-data-exchange-layer-act-english-version
19 https://www.riigiteataja.ee/akt/106082019006

RECOMMENDATIONS

Pakistan's digital transformation holds immense potential, but its success depends on embedding human rights, accountability, and inclusivity into every stage of implementation. Based on the findings of the policy brief and the evidence it presents, and to ensure that the DNA 2025 strengthens governance without undermining fundamental freedoms, the following measures are essential:

1 Strengthen Data Protection Laws Before Implementation

The full operationalisation of the DNA should be contingent upon the enactment of a robust Personal Data Protection Law that reflects global best practices. This framework must define clear standards for consent, data minimization, purpose limitation, and secure storage of personal information, incorporate mandatory DPIAs for high-risk processing (as in the EU GDPR), and ensure decentralised data storage with access logs and citizen oversight (as in Estonia's X-Road system). Adopting these measures would enhance transparency, accountability, and protection for vulnerable and minority communities.

2 Establish Independent Oversight and Redress Mechanisms

Create an autonomous Data Protection Authority with investigative and enforcement powers to oversee compliance by both public and private actors, imposing heavy fines on offenders. Alongside, establish accessible grievance mechanisms to provide individuals with timely remedies in cases of data misuse or discrimination.

3 Mandate Transparency and Public Accountability

Require all government agencies operating under the DNA 2025 to publish annual transparency reports, detailing data-sharing practices, breaches, and algorithmic decision-making processes. Regular public audits should ensure adherence to privacy and human rights standards.

4 Adopt Privacy-by-Design and Human Rights Impact Assessments

Pakistan's data protection law should follow POPIA's approach, and other relevant best practices, by restricting the processing of sensitive personal data such as religious beliefs, health, or race unless there is explicit consent, a legal obligation, or a clear public interest. Strong accountability and transparency measures, including access logging and purpose limitation, should be embedded. Mandatory Human Rights Impact Assessments should be conducted before launching major initiatives to evaluate risks to equality, autonomy, and access.

5 Strengthen Cybersecurity and Data Governance Frameworks

Develop national cybersecurity protocols to protect sensitive databases against breaches and unauthorized access. Ensure that any data breach is promptly communicated to the public, accompanied by a transparent report detailing the cause and corrective measures taken. Implement data classification standards and clear procedures for cross-agency data sharing to prevent misuse and recurring violations.

6 Establish Independent Data Regulators and Ethical Standards

Lessons from global digital governance models highlight the importance of independent data regulators insulated from political influence. Their mandate should include ensuring compliance with privacy principles, promoting informed consent practices, and safeguarding against algorithmic discrimination.

ROUNDTABLE-BASED RECOMMENDATIONS

The following recommendations are informed by a multi-stakeholder roundtable convened by the Digital Rights Foundation to assess human rights risks within Pakistan's digital transformation framework.

1 Gender and Minority Impact Assessments in Digital Policy-Making

All proposed digital governance laws, rules, and regulatory frameworks should include gender and minority impact assessments prior to adoption. These assessments can help policymakers understand how laws may affect women, transgender persons, religious minorities, and young people in real-life contexts, including potential risks related to surveillance, exclusion, or misuse, allowing for more inclusive and balanced policy outcomes.

2 Platform Accountability Frameworks

Rather than relying on platform bans or broad restrictions, a focus on accountability-based regulation can better protect users while preserving digital access. Clear standards for content moderation, grievance redress, data protection, and cooperation with lawful oversight can encourage responsible platform behaviour without limiting freedom of expression or access to information.

3 Embed Privacy-by-Design and Safety-by-Design in Digital Services

Privacy and safety considerations should be integrated into digital services from the earliest stages of development. This is particularly important for applications handling sensitive data, such as location tracking, health information, dating preferences, or biometric identifiers, and can be supported through shared responsibility among developers, platform operators, and app stores.

4 Clear and Proportionate Data Retention Practices

Data retention rules should clearly define how long data may be stored, where it is kept, and who can access it. Transparent standards and proportionate enforcement mechanisms can help prevent misuse, reduce unnecessary data collection, and strengthen public trust in digital systems. In this context, the passage of the Personal Data Protection Bill into law is essential to establish a clear legal baseline for data protection, retention limits, and accountability.

5 Inclusive Digital Governance and Advisory Structures

Digital governance bodies and advisory committees should reflect diverse perspectives by including women, transgender persons, and members of marginalised communities with relevant legal, technical, or human rights expertise. These bodies should also consult grassroots organisations working closely with these communities to ensure that policy decisions are informed by lived realities. Transparent selection criteria can enhance policy quality, reduce blind spots, and strengthen confidence in digital decision-making processes.

6 Strengthen Capacity Within Existing Enforcement and Regulatory Institutions

Rather than establishing new institutions, priority should be given to building the capacity of existing enforcement and regulatory bodies. Targeted training on digital rights and online harm, along with inclusive recruitment practices that encourage participation from women and transgender professionals, can improve institutional responsiveness and effectiveness.

7 Digital Rights Awareness and Education Initiative

Digital rights awareness is most effective when approached as an ongoing public education effort. A coordinated initiative across schools, universities, media platforms, and public spaces can promote understanding of everyday digital risks, informed consent, online safety, and privacy, with consistent messaging sustained over time.

8 Access to Digital Rights Information through Local Languages

Providing information on privacy rights, data use, complaint mechanisms, and legal protections in local languages and clear formats can make digital rights more accessible. This approach is particularly important for communities with limited digital literacy and supports wider participation in digital spaces.

9 Regulatory Frameworks for AI and Emerging Technologies

As AI and new technologies continue to evolve, regulatory frameworks should be developed proactively and aligned with international standards on transparency, accountability, and human rights. Special consideration should be given to how user data is collected and used, ensuring innovation remains inclusive and rights-respecting. Clear requirements should also be introduced to label or tag AI-generated content, supporting transparency and informed user engagement.

10 Transparency and Accountability from Social Media Platforms

Social media platforms operating in Pakistan should be encouraged to share clear information about their data practices, content moderation processes, and cooperation with government requests. Regular transparency reporting can support public understanding, inform policy development, and promote responsible engagement between the state, platforms, and users.

DigitalRightsFoundation

"KNOW YOUR RIGHTS"


@DigitalRightsFoundation


@digitalrightsfoundation


@digitalrightsfoundation


@digitalrightsfoundation


Digital Rights Foundation


@digitalrightspk.bsky.social


@DigitalRightsPK


@DigitalRightsPK