

THE STATE OF DIGITAL RIGHTS AND SAFETY IN NEPAL 2025

Digital Rights Nepal

December 2025

TABLE OF CONTENT

Executive Summary	01
1. Introduction	02
2. Key Development	02
A. Priority to ICT and digitalization	02
B. Internet Access and Digital Public Infrastructure: Promising Digital Expansion	03
C. Policy Landscape: increased control-oriented Regulation	03
D. Social Media Regulation: From Accountability to Overreach	04
E. Freedom of Expression and Press Freedom Under Growing Pressure	05
F. Misinformation, Disinformation, and the Erosion of Trust	06
G. Privacy and Data Protection: Emerging Challenges in Nepal	06
H. Mismanagement and Corruption in Nepal's Digital Governance	07
I. Escalating Cybersecurity Crisis in Nepal	08
J. Rising Cybercrime and Digital Fraud	08
3. Major findings	09
4. Recommendations	10
5. Major intervention by DRN	11
A. Policy Advocacy and Research	11
Social Media (Operation, Use and Regulation) Bill	11
AI Policy	12
Personal Data Protection Policy	12
E-Governance Blueprint	12
Joint Civil Society Report for the Universal Periodic Review (UPR)	12
National Intelligence Bill 2082	13
IT and Cybersecurity Bill	13
Digital Rights Weekly	13
Advocacy Materials	13
Annual Report on State of Digital Rights and Safety in Nepal 2025	13
B. Capacity Building Initiatives	13
Digital Rights School	13
Digital Rights Advocates Network	14
Workshop on Institutional Digital Policy Development	15
Capacity Building for Legal and Civil Society Actors	15
Defending Digital Freedom and Press Freedom	15
Regional initiative in AI informed Journalism	16
C. Collaboration and Partnerships	16
Women in Data	16
'Digital Rights Sub-Group' under EU HRD Working Group	17
Partnership with CSOs, Youth Organizations and Networks	17
Digital Rights Action Group	18
Regional and Global Collaboration	18
6. Conclusion	19

EXECUTIVE SUMMARY

The year 2025 marked a critical juncture for digital governance in Nepal. Digital infrastructure, online public services, and emerging technologies expanded rapidly, embedding digital systems deeply into governance, the economy, and everyday life. At the same time, this expansion was accompanied by increasingly restrictive regulatory frameworks, surveillance-oriented policies, and growing pressures on freedom of expression, privacy, and civic space.

This report finds that Nepal's digital transformation in 2025 was characterized by a widening gap between technological growth and rights protection. While the government advanced e-governance, digital identity systems, AI policy, and platform regulation, these initiatives were often pursued without adequate consultation, transparency, or human rights safeguards. Proposed and enacted laws on social media, cybersecurity, intelligence, and media regulation tilted toward control rather than accountability, leading to censorship, chilling effects on speech, and public resistance.

Social media regulation became the most visible flashpoint. The proposed Social Media Bill and enforcement of platform registration requirements culminated in nationwide platform bans, mass content removals, legal actions, and widespread protests. These measures disrupted communication, economic activity, and civic engagement, and raised serious concerns about proportionality, due process, and constitutional rights.

Freedom of expression and press freedom faced increasing constraints through a combination of legal action, platform moderation, judicial interventions, and informal pressures. Journalists, creators, and activists experienced takedowns, arrests, and intimidation, contributing to a chilling effect on dissent and public debate. Although courts provided some corrective rulings, judicial safeguards alone proved insufficient to counterbalance expanding executive power.

Misinformation, disinformation, and synthetic media emerged as major threats to social trust and stability, particularly during periods of political unrest. Weak state communication, low media literacy, and opaque platform moderation allowed false narratives and deepfakes to spread rapidly, amplifying polarization and undermining public confidence.

Privacy and data protection gained increased attention through court rulings and parliamentary debate, yet the absence of a comprehensive data protection law left citizens vulnerable to misuse of personal and biometric data, especially as digital identity systems and interoperability initiatives expanded.

Cybersecurity threats and cybercrime escalated sharply, exposing weak institutional preparedness, limited transparency in breach response, and growing risks to both public systems and individual users. Particularly alarming was the rise of transnational cybercrime and the trafficking of Nepali workers into forced online scam operations abroad.

Finally, audit reports and corruption cases revealed that Nepal's digital crisis is rooted less in technological capacity than in governance failures including mismanagement, politicization of regulators, weak oversight, and lack of accountability.

Despite these challenges, 2025 also demonstrated strong civic resistance and engagement. Journalists, civil society, youth movements, and digital rights defenders mobilized to contest restrictive policies and demand more transparent, rights-based digital governance. Courts, though limited, played an important corrective role, and negotiated outcomes such as the December 2025 agreement on digital rights reflect the continuing contestation over Nepal's digital future.

The report concludes that Nepal stands at a digital crossroads. Without a shift toward participatory lawmaking, strong data protection, independent oversight, and rights-centered governance, digital transformation risks deepening control, inequality, and mistrust. With the right reforms, however, it can become a foundation for inclusion, accountability, and democratic resilience.

1. INTRODUCTION

The year 2025 marked a pivotal moment for digital governance in Nepal, characterized by an unprecedented acceleration of legislative, policy, and regulatory initiatives in the digital space. The Government of Nepal introduced or advanced multiple legal and policy instruments governing social media, artificial intelligence, cybersecurity, data protection, surveillance, and e-governance. While these initiatives reflect a growing recognition of the importance of digital transformation, many of the proposed frameworks raise significant concerns regarding freedom of expression, privacy, data protection, proportionality of state power, and civic space.

Against this backdrop, digital rights in Nepal have become an increasingly contested terrain. Expanding state regulation, vague and overbroad legal provisions, limited transparency in policy-making, and weak institutional safeguards risk undermining constitutionally protected rights and Nepal's international human rights commitments. At the same time, civil society actors, journalists, technologists, youth, and legal professionals are playing a growing role in shaping digital policy discourse, promoting accountability, and advancing rights-respecting digital governance.

This report documents key digital policy and regulatory developments in Nepal in 2025, analyzes their implications for human rights and democratic governance, and highlights the role of civil society particularly Digital Rights Nepal (DRN) in engaging with, responding to, and influencing these processes.

The report seeks to contribute to informed public debate, strengthen evidence-based advocacy, and support the development of digital governance frameworks that are aligned with constitutional values, international human rights standards, and the needs of Nepal's diverse communities.

2. KEY DEVELOPMENT

A. PRIORITY TO ICT AND DIGITALIZATION

In 2025, Nepal renewed policy and fiscal emphasis on ICT and digitalization as central pillars of governance reform and economic transformation. The Government's policies and programs for FY 2082/83 prioritized the expansion of digital public services through the Nagarik App, the introduction of faceless services, and the integration of the national identity card as the backbone of service delivery.¹ Sectoral digitalization advanced across taxation, banking, agriculture, land administration, education, and health, alongside commitments to expand telecommunications, strengthen public broadcasting, and modernize postal services.² The Digital Nepal Framework is set to be revised, with parallel plans to establish ethical and institutional foundations for artificial intelligence, enhance cybersecurity for critical infrastructure, regulate social media platforms, and deploy advanced technologies in crime control and public administration.³

These policy commitments were bolstered by the federal budget for FY 2082/83, which allocated NPR 7.72 billion to the Ministry of Communication and Information Technology, a modest increase from NPR 7.25 billion the previous year.⁴ The budget included substantial investments in digital infrastructure, data centers, cloud systems, national connectivity enhancements, and preparations for launching Nepal's own satellite. It advanced digital inclusion through infrastructure expansion, digital literacy programs, and incentives for IT startups and service exports, while also introducing tax benefits, incubation support, and Industry 4.0 incentives to promote innovation and youth employment. Cybersecurity, AI research, digital health, e-governance, and data integration particularly through mandatory linkage with the national ID system featured prominently in the budget, signaling the state's intent to deepen digital governance across sectors.⁵

At the sub-national level, provinces and local governments aligned their programs with this digital push. Karnali Province announced a Digital Karnali Framework and AI-driven service delivery in agriculture.⁶ Madesh Province prioritized innovation through a School of AI and Robotics, citizen engagement via the "Hello CM" platform, and the establishment of a Space and Communication Center and a Startup and Incubation Center under the "Science and Technology Innovation Clusters" initiative.⁸ Bagmati Province committed to digitizing transport systems through smart, cashless, and green mobility solutions,⁹ while Kathmandu Metropolitan City advanced its smart city agenda through technology-enabled service delivery, transparency tools, and innovation programs.¹⁰ Complementing these developments, the Economic Reform Implementation Action Plan 2082 mandated stronger state control over public data, greater reliance on domestic IT firms, and updates to national IT policies to accommodate emerging technologies.

¹https://www.opmcm.gov.np/en/download/1746202420wpdm_only-english-translation-all-2082-pdf/

²Id.

³Id.

⁴<https://mo.gov.np/content/1523/budget-speech-2082-83/>

B. INTERNET ACCESS AND DIGITAL PUBLIC INFRASTRUCTURE: PROMISING DIGITAL EXPANSION

In 2025, Nepal experienced rapid but uneven expansion of internet access and digital public infrastructure. Mobile broadband subscriptions grew sharply, reaching nearly 26.8 million users,¹¹ driven largely by 4G adoption, while Nepal Telecom expanded 4G LTE coverage to over 744 local levels across all 77 districts and continued its nationwide FTTH rollout.¹² Fixed broadband users surpassed 3.1 million,¹³ and Nepal improved its global ranking in fixed broadband speeds, reflecting gradual infrastructure upgrades.¹⁴ Preparations for a long-delayed 5G auction advanced,¹⁵ signaling future capacity expansion, although high costs, low device penetration, and regulatory uncertainty remain key constraints.

At the same time, structural fragilities in Nepal's internet ecosystem became increasingly visible. A nationwide internet disruption linked to unpaid international bandwidth dues, heavy taxation, and foreign exchange approval delays exposed Nepal's dependence on imported bandwidth and weak policy coordination.¹⁶ Stakeholders warned of a looming telecom sector crisis, compounded by infrastructure damage during protests,¹⁷ inconsistent mobile internet performance leading to Nepal's removal from global mobile speed rankings¹⁸ and periodic failures of core digital platforms such as the Hello Sarkar grievance portal¹⁹ and voter registration systems.²⁰ These incidents underscored gaps in redundancy, cybersecurity preparedness, and institutional capacity to manage critical digital infrastructure.

Digital public infrastructure expanded in scope, particularly through the Nagarik App, which was legally entrenched and opened to private-sector services, positioning it as a central gateway for public and quasi-public digital services.²¹ Online voter registration linked to the national ID system saw unprecedented uptake,²² demonstrating strong public demand for digital services but also raising concerns around server capacity, data protection, and cybersecurity resilience. Sector-wide digitalization efforts, including paperless government systems,²³ free public Wi-Fi zones in Kathmandu,²⁴ and expanded digital banking and mobile payments,²⁵ highlighted steady progress toward e-governance. For FY 2024/25, the ICT sector is projected to contribute 1.94% to GDP, with a value-added growth rate of 4.81%, driven by increased activity in programming, information services, internet transactions, and wireless communications.²⁶

However, persistent digital inequality remains a major concern. Women's participation in the ICT sector stayed critically low: 58% of men use digital payments compared to just 36% of women.²⁷ Barriers include lower phone and SIM ownership, digital illiteracy, and reliance on male family members; notably, 40% of women with phones cannot read Latin-script messages, compared to 20% of men.²⁸ In addition, the continued use of SIM cards not registered in the user's own name²⁹ estimated at 40% undermines accountability, privacy, and consumer protection.

C. POLICY LANDSCAPE: INCREASED CONTROL-ORIENTED REGULATION

Throughout 2025, Nepal witnessed an unprecedented surge in policy and legislative activity shaping its digital, media, and governance landscape. While many initiatives reflect growing recognition of technology as a driver of development and service delivery, they also raise serious concerns regarding rights protection, institutional independence, and democratic accountability.

A significant share of policy momentum focused on regulating social media and the ICT sector. The registration of the Social Media Bill in the National Assembly³⁰ and the Information Technology and Cybersecurity Bill in the House of Representatives³¹ reflects the state's intent to regulate digital platforms and the broader ICT ecosystem. While both bills aim to modernize Nepal's digital legal framework, they have raised alarms over potentially regressive provisions affecting freedom of expression, privacy, and innovation. Supreme Court decisions upholding Section 47³² of the Electronic Transactions Act and mandating registration of all social media platforms further reinforced this regulatory trajectory³³.

Similarly, the passage of the Media Council Bill, 2080 by the National Assembly,³⁴ alongside debates surrounding the Mass Communication Bill, signals the government's intent to reform media oversight frameworks. Though these initiatives are framed as measures to enhance professionalism, dignity, and accountability in journalism,

¹¹Id.

¹²<https://www.techpana.com/2025/151256/digital-karnail-framework>

¹³<https://www.technologykhabar.com/2025/06/10/204399/>

¹⁴<https://techpana.com/2025/151214>

¹⁵<https://www.techpana.com/2025/151379/embossed-number-plates-mandatory-for-all-vehicles-in-bagmati-gps>

¹⁶<https://www.technologykhabar.com/2025/07/13/207837/>

¹⁷<https://www.technologykhabar.com/2025/12/09/>

¹⁸<https://www.techpana.com/2025/149460/nepal-telecom-to-shut-down-2g-service-on-1800-mhz>

¹⁹<https://www.techpana.com/2025/150798/ixed-internet-growth-in-nepal-which-isps-gained-most-users>

²⁰<https://www.techpana.com/2025/152166/nepal-fixed-broadband-speed-improves-average-download-upload>

²¹<https://kathmandupost.com/money/2025/11/25/nepal-closer-to-5g-auction-as-regulator-seeks-ministry-nod>

they have attracted criticism for provisions that may undermine press freedom and enable excessive executive influence over regulatory bodies.

In parallel, amendments to the Printing Press and Publication Act that formally recognize online media represent a significant step toward the legal acknowledgment of digital journalism. For some time, the registration of online media was temporarily suspended due to amendments to the Act.³⁵ Subsequently, the registration and renewal of online media were required to be conducted through the Department of Information and Broadcasting following the approval of the Printing and Publication (Second Amendment) Regulations, 2082.³⁶

Nepal also made notable advances in AI and emerging technology governance. The approval of the National AI Policy, 2025,³⁷ the establishment of a National AI Centre,³⁸ and draft sector-specific AI guidelines issued by Nepal Rastra Bank collectively indicate a strategic push toward AI-driven governance, finance, and innovation.³⁹ Yet, repeated concerns remain over short consultation timelines, weak safeguards, and the absence of a binding data protection law, especially as AI is increasingly linked with surveillance, financial monitoring, and law enforcement.

On data governance and digital identity, the expansion of the National Identity Card (NID) across banking,⁴⁰ voter registration,⁴¹ taxation,⁴² integration of NID in Nagarik app⁴³ and public services marks a transformative shift toward integrated digital systems.⁴⁴ The government's subsequent approval to extend the use of NID data across sectors, including highly sensitive areas such as foreign employment services, court case management, local-level registration, citizenship, social security, relief and disaster management, immigration services, and prisoner identification, and verification, further reinforces this digital shift.⁴⁵ Further use of Supreme Court rulings have cleared legal obstacles for NID implementation, it has also underscored the need for robust data security, public awareness, and accountability mechanisms.⁴⁶ While draft Personal Data Protection Policy 2082⁴⁷ was released for consultation, the lack of enforceable law leaves large-scale data reuse vulnerable to abuse.

Economic and service-delivery reforms further reinforced digitalization as a governance priority. The enactment and implementation of the E-Commerce Act,⁴⁸ Cloud and Data Center Guidelines,⁴⁹ digital payment⁵⁰ and cybersecurity directives⁵¹ strengthened the regulatory framework supporting online transactions, digital infrastructure, and secure digital services. The government restructured the E-governance commission to E-governance Board by amending the Electronic Good Governance Commission (Formation and Operation) Order, 2079 BS.⁵² The E-Governance Board published a draft E-Governance Blueprint aimed at enhancing the effectiveness of public service delivery through the use of ICT and fostering a transparent and accountable governance system through digital transformation.⁵³ Although the draft was released for public consultation at the beginning of 2025, no further information on its progress has been made available, raising concerns about the efficiency and follow-through of the E-Governance Board itself.

At the same time, security-oriented initiatives such as the draft National Intelligence Bill, 2082 seek to expand the mandate of the National Investigation Department (NID) under the Prime Minister's Office.⁵⁴ The Bill would grant the NID broad powers for surveillance, covert operations, counter-intelligence, and the use of advanced technologies to address threats including terrorism, organized crime, cybercrime, and smuggling. However, these expanded powers have raised serious concerns about risks to constitutional rights and democratic freedoms.⁵⁵ Together with stricter platform regulation, these developments point to a growing shift toward surveillance-heavy governance. While the state is rapidly constructing legal and institutional frameworks for digital governance, AI, and service delivery, many of these initiatives remain undermined by limited consultation, overlapping mandates, and insufficient human rights safeguards. For Nepal's digital future to be both innovative and democratic, policy development must move beyond control-driven regulation toward transparent lawmaking, independent oversight, strong data protection, and meaningful stakeholder engagement. Without this shift, the promise of digital transformation risks being overshadowed by the erosion of fundamental rights and public trust.

D. SOCIAL MEDIA REGULATION: FROM ACCOUNTABILITY TO OVERREACH

In 2025, Nepal's approach to social media governance marked a decisive shift toward restrictive regulation, raising serious concerns for digital rights and democratic freedoms. The government tabled a controversial Social Media Bill in January,⁵⁶ proposing heavy fines, imprisonment, and broad criminal liability for both platforms and users, based

³⁵<https://kathmandupost.com/money/2025/02/04/>

³⁶<https://www.nayapatrikadaily.com/news-details/>, <https://www.technologykhabar.com/2025/09/11/214848/>

³⁷<https://techpana.com/2025/151553/nepal-dropped-from-global-internet-speed-index-over-poor-mobile-data>

³⁸<https://techpana.com/2025/149884/hello-sarkar-website-problem>

³⁹<https://www.techpana.com/2025/154046/>

⁴⁰<https://mocit.gov.np/content/13037/citizen-app--officers-and-administration--references-2072/>

⁴¹<https://www.techpana.com/2025/154074/new-voter-registration-crosses-500k-225k-through-national-id>

⁴²<https://www.techpana.com/2025/154190/paperless-industry-ministry-online-process-nepal>

⁴³<https://www.technologykhabar.com/2025/11/05/219759/>

⁴⁴https://www.nrb.org.np/contents/uploads/2025/12/Kartik_2082_Publish.pdf

⁴⁵<https://www.techpana.com/2025/150613/it-sector-contributes-1-94-percent-to-nepal-gdp-in-fiscal-year-2081-82>

⁴⁶<https://www.worldbank.org/en/publication/globalindex>

⁴⁷Id.

⁴⁸<https://www.setopati.com/kinmel/information-technology/364365>

on vaguely defined offences such as harm to “national interests,” false information, pseudonymous use, and legitimate online expressions, such as comments, likes or hashtags. While the need to address online harms is legitimate, the bill was widely criticized by the political leaders, civil society, media and digital rights experts for its overbroad provisions, lack of stakeholder consultation, and disproportionate penalties that risk enabling censorship, silencing dissent, and chilling free expression.⁵⁷ Parallel to the bill, the government intensified enforcement of the 2023 Social Media Directives, repeatedly warning global platforms to register locally, appoint resident officers, and comply with content regulation requirements, culminating in sweeping bans on unregistered platforms and the nationwide shutdown of social media platforms.⁵⁸

Judicial and executive actions further reinforced this restrictive trajectory. A landmark Supreme Court ruling mandated compulsory registration and monitoring of all social media and digital platforms,⁵⁹ discouraging anonymous use and strengthening state oversight, while a number of contempt convictions against journalists sent a chilling signal to online media and independent voices.⁶⁰ The government’s eventual nationwide ban on major unregistered platforms,⁶¹ including Facebook, WhatsApp, YouTube, and X, severely disrupted communication, livelihoods, civic engagement, and access to information, prompting multiple writ petitions before the Supreme Court and Gen Z protest in early September 2025. Following protests in which 76 people were killed, the social media platform ban was withdrawn.⁶² Meanwhile, the removal of millions of Nepali videos from TikTok raised serious concerns about transparency, accountability, and due process in platform content moderation.⁶³

Sustainable and effective regulation must be grounded in transparency, proportionality, and meaningful public consultation, rather than blanket bans and punitive enforcement that erode trust and shrink civic space in Nepal’s digital public sphere.

E. FREEDOM OF EXPRESSION AND PRESS FREEDOM UNDER GROWING PRESSURE

In 2025, freedom of expression and press freedom in Nepal faced mounting pressure from an expanding mix of platform moderation, regulatory enforcement, judicial actions, and law enforcement interventions. Large-scale content moderation by platforms such as TikTok including the removal of millions of Nepali videos combined with closer coordination between TikTok and the government, raised serious transparency and due process concerns. Domestically, regulatory bodies and courts increasingly asserted authority over online expression: the Patan High Court upheld the Press Council Nepal’s jurisdiction over digital media;⁶⁴ the Supreme Court cautioned against “undignified” commentary on judicial matters;⁶⁵ and the Press Council took action against dozens of online platforms and media outlets for alleged ethical violations.⁶⁶

Journalists,⁶⁷ comedians,⁶⁸ content creators,⁶⁹ and apparel brands faced police complaints,⁷⁰ cybercrime charges, takedown orders, and informal pressures, contributing to a chilling effect on satire, criticism, and investigative reporting. High-profile cases involving journalists, contempt proceedings against media houses,⁷¹ and court-ordered content removals⁷² highlighted the growing use of defamation, cyber laws, and contempt powers to curb speech, often without clear public-interest assessments.

Public resistance to restrictive trends remained visible. A nationwide hashtag campaign⁷³ and strong opposition from the Federation of Nepali Journalists,⁷⁴ lawmakers,⁷⁵ civil society, and creators challenged the proposed Social Media Bill and broader regulatory overreach.⁷⁶ Courts also delivered some corrective rulings, including protections against arrest for journalists⁷⁷ and reversals of prior restraint orders, underscoring ongoing contestation over constitutional safeguards. However, the Gen Z-led protests, subsequent violence, attacks on media houses, temporary social media shutdowns, and Nepal’s classification as “obstructed” by CIVICUS reflected a shrinking civic space.⁷⁸

On a positive note, after more than three months of negotiations, Gen Z leaders and the interim government signed an agreement on 10 December 2025 to institutionalize the outcomes of the protest.⁷⁹ The agreement contains ten provisions, including a specific focus on freedom of expression and digital rights. Point 8 commits the government to preventing arbitrary regulation and censorship of online expression and to strengthening safeguards against illegal surveillance and misuse of digital data. The inclusion of these commitments reflects the growing centrality of digital spaces in Nepal and marks a meaningful step toward stronger protection of digital rights and freedoms. Taken together, developments in 2025 reveal a fragile environment for free expression in Nepal, where expanding digital governance and enforcement mechanisms have increasingly collided with constitutional guarantees of press freedom, artistic expression, and the public’s right to information.

⁵⁷<https://na.parliament.gov.np/bills/JCCTZJz>

⁵⁸<https://www.fiscalnepal.com/2025/06/15/>

⁵⁹https://supremecourt.gov.np/court/public/media/2025_02/a35af3d088a8c56bf1ef97cd35dffe6.pdf

⁶⁰<https://kathmandupost.com/national/2025/08/17/top-court-says-all-social-media-online-sites-must-register>

⁶¹<https://annapurnapost.com/story/473244/>

⁶²<https://www.technologykhabar.com/2025/08/05/210448/>

⁶³<https://www.technologykhabar.com/2025/10/31/219467/>

F. MISINFORMATION, DISINFORMATION, AND THE EROSION OF TRUST

In 2025, information integrity emerged as a critical fault line in Nepal's digital ecosystem, particularly amid heightened political tensions. The pro-monarchy protest on 28 March 2025 and Gen Z protest on 8- 9 September 2025, starkly exposed how quickly misinformation and disinformation can amplify violence and deepen social divisions. In the immediate aftermath, the absence of clear, timely, and authoritative communication from state institutions, coupled with fragmented and sometimes speculative media reporting, created an information vacuum. This vacuum was rapidly filled by misleading narratives circulating across social media platforms⁸⁰, ranging from exaggerated casualty figures and conspiracy theories to distorted portrayals of events on the ground.

The unchecked spread of false and misleading information not only blurred the line between fact and fiction but also eroded public trust in institutions, inflamed emotions, and heightened the risk of further unrest. In politically fragile contexts such as Nepal's, misinformation does not merely misinform, it actively destabilizes. When citizens are unable to distinguish verified facts from manipulated content, democratic debate is weakened and public order is placed at risk.

This challenge has been further compounded by a noticeable surge in deepfakes and cheapfakes. In 2025 alone, manipulated videos and images targeting prominent political leaders, public officials, and cultural figures circulated widely on platforms such as Facebook, Instagram, and X.⁸¹ Fabricated visuals depicting arrests, humiliation, or scandal, often created using easily accessible editing tools and AI-enabled applications, have been weaponized to defame individuals, provoke outrage, and manipulate public opinion. With low levels of digital and media literacy, many users are ill-equipped to identify such content, allowing falsehoods to spread faster than corrections.

As Nepal navigates an increasingly volatile digital and political environment, safeguarding information integrity has become a shared democratic responsibility.

G. PRIVACY AND DATA PROTECTION: EMERGING CHALLENGES IN NEPAL

2025 reflects an increasing, though still fragmented, recognition of privacy and data protection as core constitutional and democratic concerns. Judicial interventions, parliamentary debates, and public controversies throughout 2025 have collectively underscored both the urgency of safeguarding personal data and the systemic weaknesses that continue to expose citizens to risk.

A landmark development was the Supreme Court's order directing Nepal Telecom to safeguard personal information. The Court held that any unauthorized access to customer data, particularly through outsourced billing systems, would constitute a violation of the constitutional rights to privacy, personal freedom, and dignity.⁸²

Importantly, the Court linked data protection not only to individual rights but also to national security, setting a strong constitutional precedent at a time when public institutions increasingly rely on private vendors and digital infrastructure. This ruling reinforces the principle that technological modernization cannot come at the cost of fundamental rights.⁸³

Despite existing legal practices, Privacy concerns have intensified with the expansion of state-led digital platforms. The study on interoperability between Nepal's Nagarik App and India's Aadhaar system highlights both the promise of cross-border digital integration and the risks it poses to data sovereignty, consent, and cross-border data sharing, particularly in the absence of a comprehensive data protection law.⁸⁴ Without clear legal frameworks and accountability mechanisms, such initiatives risk normalizing large-scale data exchange without adequate safeguards.

⁸⁰https://giwmcdnone.gov.np/media/pdf_upload/National%20AI%20Policy-Final_uxc%vq.pdf

⁸¹<https://www.technologykhabar.com/2025/11/10/220335/>

⁸²<https://www.nrb.org.np/contents/uploads/2025/12/AI-Guidelines.pdf>

⁸³<https://www.nrb.org.np/contents/uploads/2025/12/AI-Guidelines.pdf>

⁸⁴<https://election.gov.np/admin/public/storage/HOR%202082/Press%20Release%20Today%201.pdf>

⁸⁵<https://techpana.com/2025/154086>

⁸⁶<https://techpana.com/2025/149710/nagarik-app-update-now-account-creation-based-on-national-id-number>

⁸⁷<https://techpana.com/2025/153749/national-id-data-access-for-six-sectors>

⁸⁸<https://mokit.gov.np/content/13099/cabinet-decision--aci-policy--2082--/>

⁸⁹<https://myrepublica.nagariknetwork.com/news/sc-issues-three-point-directive-on-national-id-card-dispute-50-44.html>, <https://www.technologykhabar.com/2025/01/19/189850/>

⁹⁰<https://egc.gov.np/content/2501/fascinity-of-personal-data-protection-policy--2082/>

⁹¹<https://english.onlinekhabar.com/president-paudel-authenticates-4-bills.html>

⁹²<https://www.technologykhabar.com/2025/02/13/192281/>

⁹³<https://www.nrb.org.np/contents/uploads/2025/03/Payment-System-related-Unified-Directives-2081>

⁹⁴<https://nsc.gov.np/content/10881/cybersecurityadvisory01/>

These concerns have been echoed in Parliament. MPs have warned against institutionalizing the Nagarik App without robust data governance, raising unresolved issues around data storage, access controls, inter-agency coordination, and cybersecurity. Their calls for operational guidelines and oversight reflect growing concern that digital governance is advancing faster than legal and technical protections.⁸⁵

At the same time, rights-based approaches are beginning to shape law enforcement practices. The Nepal Police's decision to stop publicly releasing photographs of accused individuals marks a positive step toward protecting dignity, due process, and the presumption of innocence in the digital age.⁸⁶

The Central Investigation Bureau (CIB) of Nepal Police arrested two employees of the National Identity Card and Registration Department on charges of misusing the user ID and password assigned to a registration operator.⁸⁷ This incident underscores serious concerns regarding unauthorized access to government systems and the resulting threats to citizens' personally identifiable information (PII).

Taken together, these developments show a country in transition. While courts, lawmakers, and institutions are increasingly recognizing privacy as central to democratic governance, progress remains uneven. The absence of a comprehensive data protection law, weak institutional coordination, and limited digital literacy among decision-makers continue to expose citizens' data to risk.

H. MISMANAGEMENT AND CORRUPTION IN NEPAL'S DIGITAL GOVERNANCE

Audit reports, court rulings, and corruption cases reveal deep-rooted mismanagement in Nepal's digital and IT governance. The 62nd Auditor General's Report shows that the ambitious Digital Nepal Framework, launched in 2076 BS with a projected budget of over NPR 1 trillion, has largely stalled due to the absence of a clear implementing authority, weak coordination, and uncertain funding. Despite multiple digital tools being introduced, poor integration, limited capacity, and serious gaps in cybersecurity and data protection persist.⁸⁸

These systemic weaknesses are mirrored in major corruption cases involving digital infrastructure. The CIAA's cases on TERAMOCS,⁸⁹ the National Payment Gateway,⁹⁰ and MDMS⁹¹ expose irregular procurement, political influence, and misuse of public funds. Convictions of former NTA officials confirm that these were not isolated lapses but structural failures in oversight and accountability.⁹² As a result, the Nepal Telecommunications Authority has been left paralyzed, with stalled decision-making and declining institutional morale.

Operational failures at Nepal Telecom, including repeated nationwide outages caused by outdated billing systems and delayed procurement, show the real-world consequences of poor governance, financial losses, service disruption, and erosion of public trust.⁹³ Overall, Nepal's digital crisis is less about technology and more about institutions. Without transparent procurement, independent oversight, and accountable IT governance, digital transformation risks becoming another avenue for corruption rather than a driver of public good.

I. ESCALATING CYBERSECURITY CRISIS IN NEPAL

Nepal is facing a sharp rise in cyber threats targeting government systems, media houses, and citizens' personal data, exposing serious weaknesses in national cybersecurity preparedness. In response, the National Cyber Security Centre (NCSC) issued a 102-point advisory urging stronger protection of government websites, networks, and data, stressing that negligence and low awareness remain key risk factors.⁹⁴

Despite this, cyberattacks continue unabated. Major incidents include the hacking of Setopati's YouTube channel to promote illegal cryptocurrencies,⁹⁵ 13 large-scale attacks on government 21 subdomains,⁹⁶ the month-long shutdown of the Hello Sarkar portal,⁹⁷ and repeated claims by hacker groups such as KAZU,⁹⁸ DIKU,⁹⁹ and MidNight Ops Nepal¹⁰⁰ of breaching or defacing government websites.

Further, claims of compromised WiFi hotspots nationwide,¹⁰¹ fake bank websites,¹⁰² and wallet scams¹⁰³ highlight risks beyond state systems, affecting everyday users. Collectively, these incidents underscore an urgent need for robust cybersecurity governance, transparent breach response, institutional accountability, and widespread digital literacy. Without decisive action, Nepal's public digital infrastructure and citizens' data remain dangerously exposed.

⁸⁵<https://www.techpana.com/2025/169273/>

⁸⁶https://digitalrightsnepal.org/wp-content/uploads/2025/06/Blue-print.psb-English_compressed.pdf

⁸⁷<https://www.opmcm.gov.np/>

⁸⁸<https://digitalrightsnepal.org/report>

⁸⁹<https://na.parliament.gov.np/np/>

⁹⁰<https://kathmandupost.com/national/2025/01/30/>, <https://ekantipur.com/news/2025/01/29/>

⁹¹<https://mof.gov.np/content/13000/notice-from-the-ministry-of-communication-and/>, <https://technologykhabar.com/2025/03/20/195917/>

⁹²<https://kathmandupost.com/national/2025/08/17/top-court-says-all-social-media-online-sites-must-register>

⁹³<https://www.nayapatrikadaily.com/>

⁹⁴<https://kathmandupost.com/>

⁹⁵<https://www.aljazeera.com/news/2025/9/9>

⁹⁶<https://ekantipur.com/news/2025/06/26>

Further, claims of compromised WiFi hotspots nationwide,¹⁰¹ fake bank websites,¹⁰² and wallet scams¹⁰³ highlight risks beyond state systems, affecting everyday users. Collectively, these incidents underscore an urgent need for robust cybersecurity governance, transparent breach response, institutional accountability, and widespread digital literacy. Without decisive action, Nepal's public digital infrastructure and citizens' data remain dangerously exposed.

The alleged cybersecurity breaches and data leaks mentioned above, involving the personal data of millions of citizens, including police, public Wifi, and public service records, have raised serious privacy and data protection concerns, often met with official denials and ongoing investigations.

J. RISING CYBERCRIME AND DIGITAL FRAUD

Nepal is witnessing a sharp surge in cybercrime, ranging from digital arrest scams, phishing, fake apps, and WhatsApp hijacking to large-scale online gambling, cryptocurrency fraud, and cyber-kidnapping. Police have arrested dozens for online gambling and online betting operations worth billions of rupees, often involving crypto transactions and cross-border networks.¹⁰⁴

Kathmandu police have reported Nepal's first cyber-kidnapping case, where scammers used a WhatsApp video call to extort money by falsely claiming a 16-year-old boy was involved in a rape case.¹⁰⁵ Disturbingly, Nepali workers are being trafficked to countries such as Myanmar, Cambodia, and Oman under false promises of IT jobs and forced to run online scams, including cryptocurrency fraud.¹⁰⁶ Victims have their passports seized and are held under coercive conditions, recognized by the UN as a form of modern slavery.¹⁰⁷ 14 Nepalis were rescued from a scam center in Myanmar,¹⁰⁸ and Nepal Police arrested a trafficker who sent a Nepali youth to Cambodia for cyber fraud.¹⁰⁹

Nepal Police have begun deploying AI-based intelligence tools to strengthen investigations, while the NRB reports a 24% rise in suspicious financial transactions, largely linked to cyber fraud and illegal gambling.¹¹⁰ In FY 2081/82, a total of 18,928¹¹¹ Cybercrime cases were reported, most of them carried out through social media platforms such as Facebook, Messenger, and TikTok, with girls and women comprising the majority of victims. Together, these cases underline an urgent need for stronger digital governance, cross-border cooperation, public awareness, and

¹⁰¹<https://www.technologykhabar.com/2025/05/14/201284/>

¹⁰²<https://www.techpana.com/2025/1509>

¹⁰³<https://www.presscouncilnepal.gov.np/np/2025/11/26/11267/>, <https://www.presscouncilnepal.gov.np/np/2025/10/30/11181/>

¹⁰⁴<https://ekantipur.com/news/the-high-court-continued-the-short-term-interim-order-issued-against-the-journalist>

¹⁰⁵<https://techpana.com/2025/149616/nepali-comedy-scene-faces-legal-challenge-after-mocking-allegations>

¹⁰⁶<https://techpana.com/2025/151538/ker-a-ganatantra-t-shirt-sale-halted-after-cyber-bureau-request>

¹⁰⁷id.

¹⁰⁸<https://www.nayopatrikadaily.com/news-details/171342/2025-06-26>

¹⁰⁹<https://kathmandupost.com/national/2025/06/11/kathmandu-court-orders-two-news-websites-to-remove-articles>

¹¹⁰<https://www.techpana.com/2025/149495/social-media-bill-protest-hashtag-campaign-boina-de-sarkar>

¹¹¹<https://fnjnepal.org/en/press/758>

¹¹²<https://www.onlinekhabar.com/there-are-problems-with-the-social-media-bill-they-need-to-be-corrected>

¹¹³<https://www.onlinekhabar.com/the-aim-appears-to-be-to-criminalize-criticism-and-discourage-open-debate>

¹¹⁴<https://ekantipur.com/news/the-high-court-continued-the-short-term-interim-order-issued-against-the-journalist>

¹¹⁵<https://monitor.civicus.org/explore/nepal-anti-corruption-protests-force-political-change-despite-violent->

¹¹⁶<http://rajpatra.dop.gov.np/welcome/boak/?ref=26156>

¹¹⁷<https://www.techpana.com/2025/153051/facebook-group-renamed-31-times-now-gen-z-nepal>

¹¹⁸<https://www.technologykhabar.com/2025/04/15/198531/>

¹¹⁹<https://www.technologykhabar.com/2025/01/06/188440/>

¹²⁰id.

¹²¹<https://techpana.com/2025/149516/nepal-india-study-interoperability-of-nagarik-app-and-aadhaar-card>

¹²²<https://www.technologykhabar.com/2025/03/17/195607/>, <https://www.technologykhabar.com/2025/03/17/195614/>

¹²³<https://www.setopati.com/social/364910>

¹²⁴<https://ekantipur.com/news/2025/12/14/.html>

¹²⁵https://oag.gov.np/site_uploads/mahalkhaparakashakaka--1853199838.pdf

¹²⁶<https://kathmandupost.com/national/2025/05/15/corruption-case-filed-against-16>

¹²⁷<https://www.technologykhabar.com/2025/05/09/200844/>

¹²⁸<https://techpana.com/2025/149818/mdms-case-former-nta-presidents-found-guilty>

¹²⁹id.

¹³⁰<https://www.techpana.com/2025/154332/ntc-bypasses-billing-after-data-outage-causing-5m-loss>

¹³¹<https://ncsc.gov.np/content/10881/cybersecurityadvisory01>

¹³²<https://www.techpana.com/2025/149353/setopati-youtube-channel-hacked>

¹³³<https://techpana.com/2025/149623/riwash-neupane-article-on-cyber-security>

¹³⁴<https://www.techpana.com/2025/150214/hello-sarkar-website-back-online-after-one-month>

¹³⁵<https://techpana.com/2025/150481/>, <https://techpana.com/2025/150651/>

¹³⁶<https://techpana.com/2025/151998>

¹³⁷<https://www.techpana.com/2025/151350/midnightops-defaces-nepal-government-site>

¹³⁸<https://www.techpana.com/2025/153607/nepal->

¹³⁹<https://techpana.com/2025/153722/beware-of-fake-bank-websites-cyber-bureau-alerts->

¹⁴⁰<https://techpana.com/2025/153738>

3. MAJOR FINDINGS

i. Digital expansion outpaced rights and governance safeguards

Nepal made significant advances in digitalization, public service delivery, and ICT infrastructure in 2025. However, these developments consistently outpaced the establishment of robust legal, institutional, and human rights safeguards. This imbalance created systemic vulnerabilities, particularly in relation to privacy, accountability, data protection, and due process.

ii. A marked shift toward control-oriented digital governance

The year saw a clear shift toward surveillance-heavy and restrictive regulatory approaches, particularly through proposed social media, cybersecurity, intelligence, and media laws. These frameworks prioritized state control, monitoring, and enforcement over transparency, proportionality, independent oversight, and rights protection.

iii. Freedom of expression and press freedom came under increasing strain

Journalists, content creators, and online users faced rising legal action, content takedowns, contempt proceedings, platform restrictions, and informal political and institutional pressure. This produced a chilling effect on dissent, satire, and investigative reporting, despite constitutional guarantees of freedom of expression and media freedom.

iv. Social media regulation escalated into regulatory overreach

The Social Media Bill, mandatory platform registration requirements, content removal orders, and nationwide platform bans exemplified regulatory overreach. These measures led to widespread disruption of communication, economic activity, and civic space, contributing to public unrest, protests, and, in some instances, fatalities.

v. Digital public infrastructure expanded in the absence of adequate data protection

The rapid expansion of digital public infrastructure including the Nagarik App, national ID integration, and interoperability initiatives proceeded without a comprehensive and enforceable data protection law. This raised serious concerns regarding privacy, consent, data security, biometric misuse, and the long-term risks of centralized data systems.

vi. Persistent digital inequality and gender-based digital exclusion

Despite the growth of digital services, deep inequalities persisted, particularly affecting women, rural populations, persons with disabilities, and marginalized communities. These disparities were reflected in lower levels of device ownership, limited access to digital payments, digital illiteracy, and continued reliance on shared or unregistered SIM cards.

vii. Information integrity emerged as a critical democratic vulnerability

Misinformation, disinformation, and AI-generated deepfakes intensified during periods of political unrest, amplifying violence, distorting public discourse, and eroding trust in institutions. This exposed the absence of coordinated state communication strategies, platform accountability mechanisms, and sustained media and digital literacy frameworks.

viii. Escalating cybersecurity threats amid weak institutional preparedness

Repeated cyberattacks on government systems, media platforms, and public services revealed significant gaps in cybersecurity governance, incident response capacity, transparency, and institutional accountability, leaving critical public infrastructure and personal data highly exposed.

ix. A surge in cybercrime and transnational digital exploitation

There was a sharp rise in cyber fraud, online gambling, and digital extortion. Emergence of new patterns of crime such as cyber-kidnapping, alongside the trafficking of Nepali workers into forced online scam operations abroad. These trends highlighted absence of and failures in cross-border cooperation, victim protection mechanisms, and law enforcement capacity in addressing transnational digital crimes.

x. Governance failures and corruption undermined trust in digital transformation

Auditor-General reports and corruption investigations revealed stalled flagship digital projects, irregular procurement practices, politicization of regulatory institutions, and administrative paralysis. These findings suggest that Nepal's digital crisis is rooted more in governance and institutional weaknesses than in technological limitations.

xi. The judiciary emerged as an important though uneven safeguard

Courts played a significant corrective role in cases related to privacy, media freedom, and due process. However, judicial interventions alone proved insufficient to counterbalance expansive executive authority, weak legislative safeguards, and structural governance deficits.

xii. Public resistance and civic contestation remained resilient

Despite a shrinking civic space, sustained opposition from journalists, civil society organizations, youth movements, and digital rights defenders demonstrated strong public demand for transparent, accountable, and rights-respecting digital governance in Nepal.

4. RECOMMENDATIONS

1. Participatory and Transparent Policy-Making

- ◉ Ensure that all draft laws, policies, and regulations affecting digital rights undergo meaningful public consultation with civil society, technical experts, journalists, youth, and marginalized communities.
- ◉ Establish formal mechanisms for stakeholder feedback to be incorporated into lawmaking and regulatory decisions.

2. Freedom of Expression and Press Freedom Safeguards

- ◉ Review and amend restrictive social media, cybersecurity, and media laws to align with constitutional guarantees and international human rights standards.
- ◉ Limit broad and punitive penalties for online expression; ensure proportionality, due process, and independent oversight.
- ◉ Encourage platforms to implement transparent content moderation mechanisms with avenues for appeal.

3. Privacy and Data Protection

- ◉ Enact a comprehensive Data Protection Law with clear principles on consent, data minimization, cross-border transfers, and independent enforcement.
- ◉ Strengthen institutional safeguards for government-managed digital services, including Nagarik App and biometric systems, to prevent unauthorized access and misuse.
- ◉ Promote public awareness campaigns on privacy rights and digital hygiene.

4. Cybersecurity and Digital Infrastructure

- ◉ Establish a coordinated national cybersecurity strategy with clear roles, responsibilities, and accountability mechanisms.
- ◉ Develop rapid and transparent breach-response protocols to protect citizens' data and maintain trust in public digital systems.
- ◉ Regularly assess the resilience of critical digital infrastructure, including e-governance platforms and public services.

5. Combatting Misinformation and Disinformation

- ◉ Invest in media and digital literacy programs to empower citizens to identify misinformation, disinformation, and AI-generated content.
- ◉ Strengthen independent fact-checking institutions and encourage platform accountability for rapid correction of false content.
- ◉ Develop public communication strategies that ensure timely, accurate, and authoritative information during emergencies or political unrest.

6. Gender, Inclusion, and Digital Equity

- ◉ Ensure equitable access to digital services, devices, and internet connectivity for women, rural communities, and marginalized groups.
- ◉ Design digital rights programs, training, and policies that account for gendered risks and inequalities in the online space.

7. Strengthen Institutional Governance and Accountability

- ◉ Enhance oversight of regulatory bodies, procurement processes, and digital public infrastructure to reduce corruption, mismanagement, and misuse of authority.
- ◉ Introduce independent monitoring mechanisms for law enforcement, judiciary, and digital platforms to ensure rights compliance.
- ◉ Encourage multi-stakeholder coalitions to monitor and advocate for ethical, transparent, and accountable digital governance.

5. MAJOR INTERVENTION BY DRN

Throughout 2025, Digital Rights Nepal (DRN) played a central role in monitoring, analyzing, and responding to developments affecting digital rights, safety, and governance in Nepal. Through policy advocacy, research, capacity building, and coalition work, DRN sought to promote rights-based digital governance and strengthen civic engagement in digital policy processes.

A.POLICY ADVOCACY AND RESEARCH

Social Media (Operation, Use and Regulation) Bill



The year 2025 marked a critical turning point in social media regulation in Nepal with the introduction of the Social Media (Operation, Use and Regulation) Bill. Digital Rights Nepal (DRN) engaged closely with the process from its earliest stages, conducting a detailed review of the draft Bill, submitting written feedback,¹¹² and facilitating public and expert consultations.

Following the Bill's registration in the National Assembly on 9 February 2025, several of DRN's recommendations were reflected in the revised version. DRN continued its advocacy through additional submissions¹¹³ on the registered Bill, the publication of policy briefs¹¹⁴ and analytical summaries,¹¹⁵ and ongoing engagement¹¹⁶ with lawmakers, regulators, media, and civil society actors.

As part of this effort, DRN co-organized a national dialogue on Digital Rights and the Social Media Bill with Martin Chautari¹¹⁷ on 5 August 2025. The dialogue examined the Bill's implications for freedom of expression, platform governance, intermediary liability, and civic space, and provided a platform for journalists, legal experts, policymakers, and civil society to debate rights-respecting approaches to social media regulation in Nepal.



Fig: National Dialogue on Digital Rights and the Social Media Bill with Martin Chautari on 5 August 2025

¹¹²<https://www.technologykhabar.com/2025/03/27/196637/>, <https://www.technologykhabar.com/2025/03/09/194896/>

¹¹³<https://english.onlinekhabar.com/kathmandu-sees-first-case-of-cyber-kidnapping>

¹¹⁴<https://techpana.com/2025/153863>,

¹¹⁵https://bangkok.ohchr.org/sites/default/files/wp_files/2023/08/ONLINE-SCAM-OPERATIONS-2582023.pdf

¹¹⁶<https://techpana.com/2025/153863>

¹¹⁷<https://techpana.com/2025/150484>

¹¹⁸<https://www.onlinekhabar.com/police-purchase-ai-based-intelligence-tools-hoping-to-facilitate-crime-investigation>

¹¹⁹<https://www.nepalpolice.gov.np/media/081-82-suicide-cyber-crime-ne-1.pdf>

AI Policy

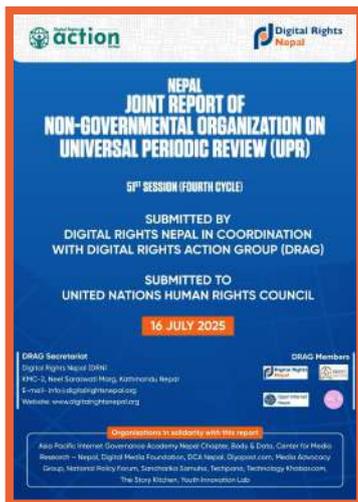
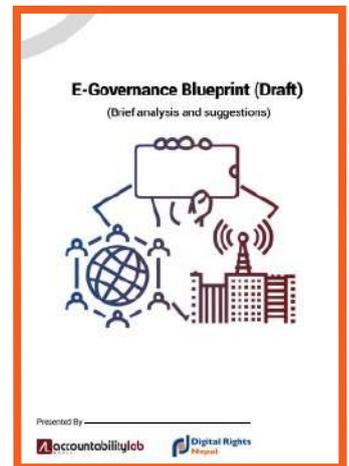
Nepal Government had published a draft of AI Policy seeking public recommendation and suggestions. DRN prepared and submitted a comprehensive analysis of the draft AI Policy, highlighting gaps in accountability, transparency, human rights safeguards, and risk governance. The paper was developed in collaboration with the AI Association Nepal (AIAN) through stakeholder consultations and expert review, contributing to a more grounded and inclusive policy debate on AI governance in Nepal.¹¹⁸

Personal Data Protection Policy

On July 15, Digital Rights Nepal (DRN), in collaboration with Digital Rights Action Group (DRAG), organized a Stakeholder Consultation on the draft Personal Data Protection Policy released by the E-Governance Board. The consultation facilitated feedback from civil society, legal experts, technologists, and media actors. DRN subsequently published an analysis paper emphasizing consent, purpose limitation, independent oversight, and remedies for rights violations.

E-Governance Blueprint

Nepal Government, E-Governance Board had published a draft of E-Governance Blueprint requesting for suggestions from the stakeholders. Together with Accountability Lab Nepal, DRN prepared an analysis and recommendation paper¹¹⁹ on analyzing Nepal's E-Governance Blueprint, recommending improvements related to transparency, accessibility, grievance mechanisms, and public accountability and submitted it to the Nepal Government, E-Governance



Joint Civil Society Report for the Universal Periodic Review (UPR)

Digital Rights Nepal (DRN), in coordination with the Digital Rights Action Group (DRAG), submitted a joint civil society report on the state of digital rights in Nepal¹²⁰ for the Fourth Cycle of the Universal Periodic Review (UPR). The report was informed by a national consultation¹²¹ held on 20 June 2025, which brought together civil society actors to assess key trends, challenges, and priorities in Nepal's digital rights landscape.

To broaden participation and transparency, DRN also produced and disseminated two public campaign videos inviting feedback from a wider range of stakeholders on digital rights concerns in the country. These inputs helped ensure that the UPR submission reflected both expert analysis and grassroots perspectives on digital rights, freedom of expression, privacy, and digital governance in Nepal.



Fig. Digital Rights UPR Stakeholder Consultation Workshop on 20 June 2025

¹¹⁸https://digitalrightsnepal.org/wp-content/uploads/2024/10/19Sep24_final_1.pdf

¹¹⁹<https://digitalrightsnepal.org/report>

¹²⁰<https://digitalrightsnepal.org/report/four-page-brief-social-media-operation-usage-and-regulation-bill-2082/>

¹²¹<https://digitalrightsnepal.org/wp-content/uploads/2025/08/Summary-Analysis-paper-on-Social-Media-Bill>

¹²²<https://digitalrightsnepal.org/activity/interaction-program>

¹²³<https://digitalrightsnepal.org/activity/dialogue-on-digital-rights-and-the-social-media-bill-2081/>

¹²⁴<https://digitalrightsnepal.org/report/>

¹²⁵<https://digitalrightsnepal.org/report/analysis-and-recommendations-on-nepals-e-governance-blueprint/>

¹²⁶<https://digitalrightsnepal.org/report/nepal-joint-report-of-non-governmental-organization-on-universal-periodic-review-upr-for-51st-session/>

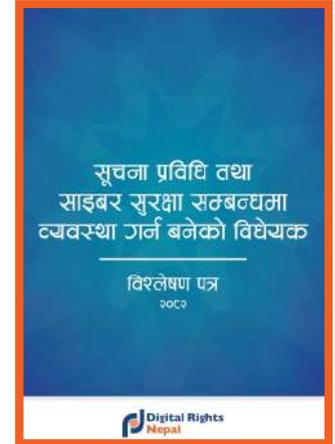
¹²⁷<https://digitalrightsnepal.org/activity/digital-rights-upr-stakeholder-consultation-workshop/>

National Intelligence Bill 2082

On 1 August 2025, the Government of Nepal published a draft of the National Intelligence Bill, 2082, for public consultation. Digital Rights Nepal (DRN) conducted a detailed legal and human rights analysis of the draft, focusing on its implications for privacy, surveillance, due process, and oversight. DRN submitted formal recommendations to the government and published an analysis paper highlighting key concerns and proposing safeguards to ensure the Bill's alignment with constitutional guarantees and international human rights standards.¹²²

IT and Cybersecurity Bill

The Information Technology and Cybersecurity Bill was registered in the House of Representatives on 10 June 2025. In response, Digital Rights Nepal prepared a policy analysis¹²³ following a stakeholder consultation held on 30 June 2025. The analysis critically examined the Bill's provisions on surveillance, content regulation, intermediary liability, cyber offences, and institutional powers. It also put forward concrete recommendations to ensure that the law is rights-respecting, proportionate, transparent, and consistent with Nepal's constitutional framework and international human rights obligations.



Digital Rights Weekly

In 2025, DRN published 52 weekly newsletters, continuing an effort that began in 2022. With this, Digital Rights Weekly reached its 186th edition. These newsletters highlighted key digital rights issues, laws, and policy developments, while also sharing ICT-related opportunities, DRN's engagements, and ongoing advocacy efforts.

Advocacy Materials

DRN produced advocacy materials, including infographics and videos, on issues such as content regulation laws, information integrity, cyber hygiene, digital divide and discrimination, technology-facilitated gender-based violence (TFGBV), and the Universal Periodic Review process. These materials served as concise, accessible tools for raising public awareness of critical digital issues.

Annual Report on State of Digital Rights and Safety in Nepal 2025

Offering an evidence-based analysis of Nepal's digital rights landscape throughout 2025, DRN is preparing for its Annual Report on Digital Rights and Safety in Nepal 2025. This report has examined key policy developments, legislative initiatives, judicial trends, and real-world challenges faced by journalists, activities, women, minorities, and youth throughout the year 2025. It is intended to serve as a resource for policymakers, researchers, civil society, and international partners, while also contributing to informed public discourse on digital governance in Nepal.

B. CAPACITY BUILDING INITIATIVES

In 2025, Digital Rights Nepal (DRN) prioritized strengthening the institutional and advocacy capacity of civil society organizations (CSOs), youth, educators, legal professionals, and grassroots actors to advance digital safety, digital literacy, and rights-based digital governance across Nepal. Through a combination of structured training programs, province-level networks, and thematic workshops, DRN expanded its geographic reach while deepening engagement at both institutional and community levels.

Digital Rights School

The Digital Rights School (DRS) is DRN's flagship two day capacity-building program, launched in 2022 to strengthen knowledge, skills, and advocacy capacity on digital rights among CSOs, journalists, lawyers, students, and activists. Following its nationwide implementation across all seven provinces in 2024, the third edition of the DRS was implemented in 2025 in Gandaki, Karnali, and Bagmati Provinces.

The 2025 edition placed particular emphasis on strengthening the institutional and advocacy capacity of CSOs through an inclusive and rights-based approach to digital governance. The curriculum covered emerging digital rights challenges, online safety, freedom of expression, privacy and data protection, cybersecurity, and the role of civil society in shaping digital policy, accountability mechanisms, and public discourse.

¹²²<https://digitalrightsnepal.org/report/>

¹²³<https://digitalrightsnepal.org/report/>

¹²⁴<https://digitalrightsnepal.org/activity/>

¹²⁵<https://digitalrightsnepal.org/activity/d>



Fig: Wrap up of Digital Rights School 2025 at Bagmati

Digital Rights Advocates Network

The Digital Rights Advocates Network (DRAN) functions as a province-based platform of alumni from DRN's Digital Rights Schools, established to sustain local-level advocacy on digital safety, responsible internet use, and digital rights awareness.

In 2025, DRAN members organized and supported several outreach activities. In Gandaki Province, DRAN collaborated with Eureka and with the support of DRN organized a seven-day Digital Rights and Safety School Awareness Campaign in Pokhara between December 2024 and January 2025.¹³⁴ In Lumbini Province, DRAN curated and delivered an Online Safety and Digital Hygiene program at Kashi Nobel Academy and the American Corner in Bhairahawa in December 2025,¹³⁵ reaching students and educators with practical tools on digital risk prevention.



Fig: Digital Rights Alumni at Digital Rights and Safety School Awareness Campaign in Pokhara



Fig: Digital Rights Alumni at Online Safety and Digital Hygiene program at Bhairahawa

Workshop on Institutional Digital Policy Development



Fig: Workshop on Institutional Digital Policy Development

Building on its focus on institutional capacity strengthening, DRN organized a workshop on Institutional Digital Policy Development.¹²⁶ Held on 22 August 2025, the workshop was designed to equip civil society organizations (CSOs) with practical knowledge and tools to develop, review, and strengthen their internal digital policies and strategies. It addressed critical areas including information access, website management, cyber safety, privacy, data protection, communications, and digital rights advocacy.

Capacity Building for Legal and Civil Society Actors

DRN conducted a Capacity-Building Workshop for Lawyers on 16 October 2025, focused on strengthening understanding of digital rights, online safety, privacy, data protection, and cybersecurity among legal practitioners and law students.¹²⁷



Fig: Capacity-Building Workshop for Lawyers on 16 October 2025



Fig: DRN organized a Capacity-Building Workshop for Civil Society Organizations on "Strengthening Organizational Digital Safety" on 17 October 2025

On 17 October 2025, DRN organized a capacity building workshop for civil society organizations on "Strengthening Organizational Digital Safety,"¹²⁸ equipping CSOs with practical knowledge, skills, and tools to safeguard organizational data, communications, and digital infrastructure.

Defending Digital Freedom and Press Freedom

As part of its overarching mandate, DRN remained firmly committed to protecting digital freedom and press freedom. Under this mandate, DRN actively engaged in policy dialogue on the Mass Communication Council Bill and the Mass Communication Bill. DRN published policy briefs and formal submissions on these bills and held consultations and dialogues with policymakers.

In parallel, DRN provided legal support to journalists and media houses facing legal action solely for carrying out their journalistic duties. In 2025, DRN supported 13 cases related to freedom of expression, offering assistance ranging from legal consultations to courtroom representation. These cases reflected a broad spectrum of instances in which journalists and media outlets were targeted for their reporting.

To further strengthen this work, DRN is currently developing a Handbook on Digital Rights and Security, Information Integrity, and Election Reporting in collaboration with the Federation of Nepali Journalists. Through these combined efforts, DRN continued to defend freedom of expression and uphold press freedom in Nepal.

¹²²<https://digitalrightsnepal.org/activity/d>

¹²³<https://digitalrightsnepal.org/activity/workshop>

¹²⁴<https://digitalrightsnepal.org/activity/>

¹²⁵<https://digitalrightsnepal.org/activity/capacity-building-workshop>

Regional initiative in AI informed Journalism

In 2025, Digital Rights Nepal (DRN), in collaboration with UNESCO and regional universities Kathmandu University (Nepal), North South University (Bangladesh), and Guru Gobind Singh Indraprastha University (India) undertook a series of activities to advance AI literacy, ethical awareness, and practical competencies among journalists in South Asia. These initiatives included webinars, expert consultations, and the development of a draft AI-informed journalism curriculum tailored for the region. DRN facilitated a Steering Committee meeting and an Expert Conference on AI in Journalism in Kathmandu,¹²⁹ bringing together academics, journalists, policy specialists, and industry leaders to validate the curriculum framework and provide guidance on localization, verification, ethics, and pedagogical design. Through these activities, DRN strengthened regional academic collaboration, promoted AI literacy in journalism, and laid the groundwork for the adoption of AI-informed educational programs across the partner universities and beyond, reinforcing its broader advocacy for responsible and rights-respecting AI use in media.



Fig: Welcome Remarks presented at Expert Conference on AI in Journalism by Mr. Nirman Mani Adhikary, Head of the Department of Languages and Mass Communication, Kathmandu University

C. COLLABORATION AND PARTNERSHIPS

Women in Data

In collaboration with the Women in Data (WID) Steering Committee, DRN co-organized a panel discussion on Women in Tech Policy and Governance – Shaping Nepal’s Digital Future on 7 February 2025,¹³⁰ alongside the launch of the Women in Data Platform. During the Women in Data Conference 2025¹³¹ organized on 25 February, DRN led a breakout session on Gendered Disinformation and showcased the newly developed WID Nepal website supporting women in data-related fields.



Fig: Panel discussion on Women in Tech Policy and Governance – Shaping Nepal’s Digital Future on 7 February 2025



Fig: Women in Data Conference 2025 on 25 February

'Digital Rights Sub-Group' under EU HRD Working Group

DRN serves as the coordinator for the Digital Rights Sub-Group under the EU Working Group on Human Rights Defenders. In this capacity, DRN facilitates regularly scheduled meetings to foster collaboration and strategic action among key stakeholders.¹³² These ongoing initiations serve as a platform for addressing the digital issues related to human rights defenders, including online freedom of expression, media freedom, disinformation, the right to information, cyberbullying, hate speech, and cybersecurity risks faced by human rights defenders.



Fig: Meeting of the Digital Rights Sub-Group under the EU Working Group on Human Rights Defenders on 13 February 2025

Partnership with CSOs, Youth Organizations and Networks

DRN collaborated with SpeakUp Nepal and Youth Initiative in February 2025 to host public webinars on the proposed Social Media Bill.¹³³ In partnership with Yuwalaya and with the support of Oxfam, DRN conducted a two-day Digital Rights and Safety Workshop for youth leaders.

DRN also collaborated with Rotaract and Leo Clubs to organize youth-focused awareness workshops, including You, Me, and the Internet (26 July 2025)¹³⁴ and Beyond the Screen: Protecting Young Minds in the Digital World (3 December 2025).¹³⁵

DRN served as the title sponsor of Optima Model United Nations 2025, collaborated with Break the Stigma 4.0 to organize a session on Countering Online GBV, supported the organization of Youth IGF Nepal 2025,¹³⁶ and partnered with the Digital Media Foundation to organize the National AI Summit 2025.



Fig: Session on Countering Online GBV in Nepal Law Campus along with Break the Stigma 4.0

Digital Rights Action Group

DRN formed the Digital Rights Action Group (DRAG) together with Dignity Initiative, Open Internet Nepal, and Women Leaders in Technology. The Group combines the strengths of its members to promote inclusive, coordinated, and impactful digital rights advocacy through joint campaigns, consultations, policy engagement, and public education.



DRAG STEERING COMMITTEE



Fig: Workshop on Community Contribution in Censorship Detection on 14 November 2025

Regional and Global Collaboration

As part of regional collaboration, DRN is a part of a regional coalition i.e. Digital Accountability Collective South Asia (DACSA), formed by Digitally Right (Bangladesh), Digital Rights Foundation (Pakistan), Digital Rights Nepal (Nepal), and Hashtag Generation (Sri Lanka).

DRN also continued its partnership with the Open Observatory of Network Interference (OONI) to monitor internet censorship, organizing a Workshop on Community Contribution in Censorship Detection on 14 November 2025 in collaboration with Netalitica.¹³⁷

¹³⁴<https://digitalrightsnepal.org/activity/drn-hosts-second-meeting-of-digital-rights->

¹³⁵<https://digitalrightsnepal.org/activity/-discuss-the-social-media-bill-2081/>

¹³⁶<https://yigf.org.np/youth-igf-nepal-2025/>

¹³⁷<https://digitalrightsnepal.org/activity/you-me-and-the-internet>

¹³⁸<https://digitalrightsnepal.org/activity/beyond-the-screen>

¹³⁹<https://digitalrightsnepal.org/activity/workshop-on-community-contribution-in-censorship-detection/>

6. CONCLUSION

The state of digital rights and safety in Nepal in 2025 reflects a society in transition, one where digital technologies have become deeply embedded in governance, markets, and everyday life, but where the institutions and safeguards needed to govern them democratically remain fragile and incomplete.

The year revealed a persistent pattern: digital expansion consistently outpaced rights protection. Public services were digitalized, platforms were regulated, and new technologies were introduced, but often without sufficient transparency, consultation, or accountability. As a result, digital governance increasingly took on a control-oriented character, privileging surveillance, restriction, and enforcement over participation, trust, and rights.

This imbalance has real consequences. It has narrowed civic space, weakened freedom of expression, exposed citizens' data to misuse, enabled misinformation to destabilize public debate, and left critical systems vulnerable to cyber threats and corruption. It has also eroded public trust, a resource as vital to democratic governance as any technology.

At the same time, 2025 demonstrated that Nepal's digital future is not predetermined. Civic resistance, legal challenges, youth mobilization, and civil society advocacy showed that digital spaces remain contested and politically alive. The demand for a rights-respecting, transparent, and accountable digital order is strong and growing.

The path forward is therefore clear. Nepal must move from control-driven digital governance to rights-respecting digital governance. This requires participatory lawmaking, independent and credible regulatory institutions, strong data protection and privacy laws, transparent platform governance, robust cybersecurity frameworks, and sustained investment in digital and media literacy. Above all, it requires recognizing that digital rights are not technical issues, but democratic ones.

Whether Nepal's digital transformation becomes a tool for empowerment or a mechanism of control will depend not on the technologies adopted, but on the values embedded in the laws, institutions, and practices that govern them.

About Us

Digital Rights Nepal

Digital Rights Nepal (DRN) is a non-profit organization established in 2020, dedicated to safeguarding digital rights and fostering a secure online environment in Nepal. With a diverse team of advocates and experts, DRN conducts research, advocates for policy reforms, and engages in capacity-building initiatives to promote online freedom of expression, privacy protection, access to information, and cybersecurity. Led by passionate changemakers in human rights and digital advocacy, DRN plays a pivotal role in shaping the digital landscape of Nepal, both locally and on the international stage.



Phone: +977-9767245100

Address: 47 - Neel Saraswoti Marga, Gairidhara - 2, Kathmandu

Email: info@digitalrightsnepal.org.np

Web: www.digitalrightsnepal.org