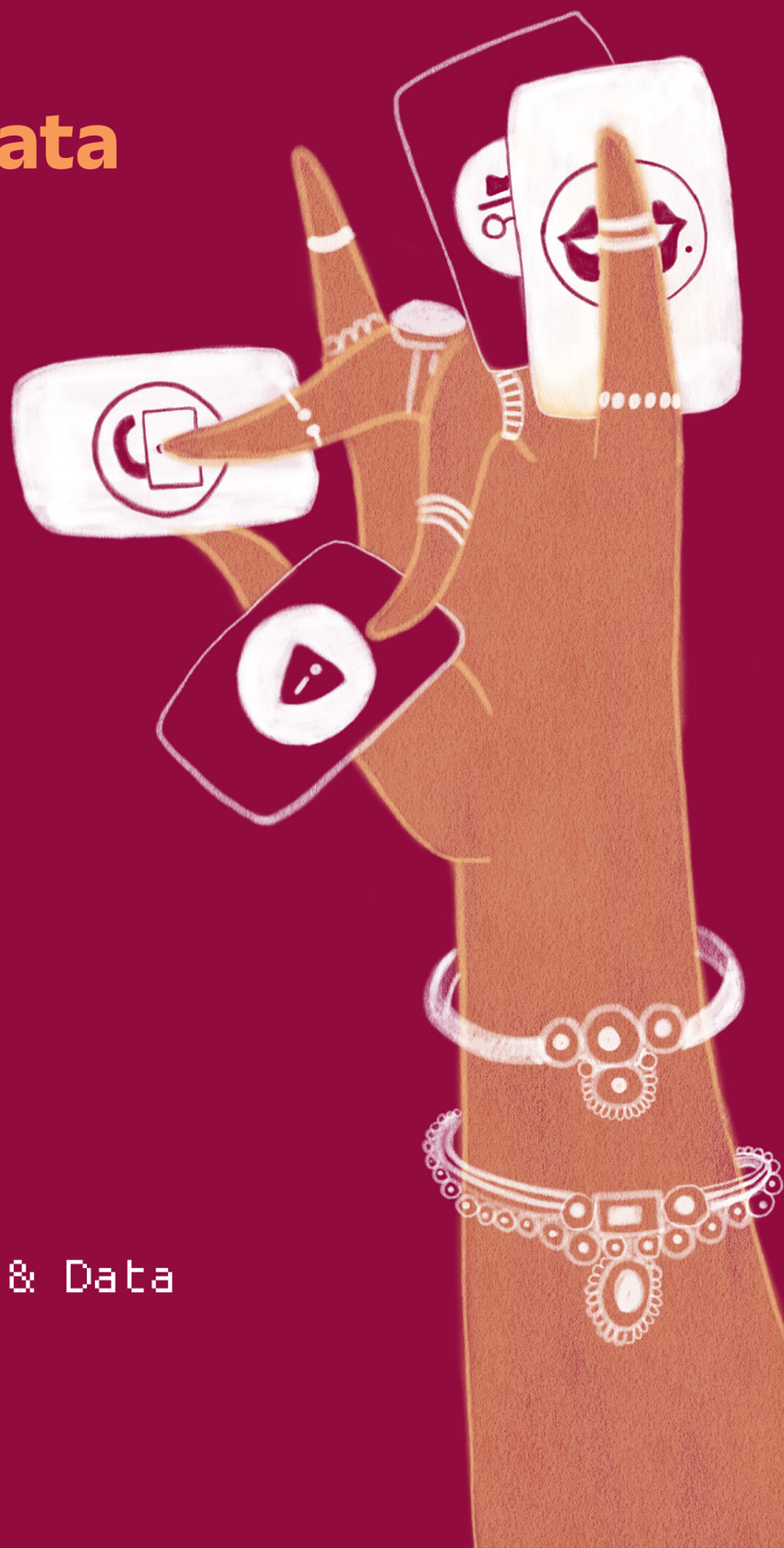
Annual Report Media Monitoring 2025

Body & Data



Body & Data

Table of Content

1

Review of the Status of Digital Rights in Nepali Media

Body & Data began an annual review report of Media Monitoring in 2021 to analyse and initiate discourse on what kinds of content, incidents, and trends regarding digital rights were prioritised in Nepali media throughout the year. The initiative was also to understand how our digital rights are connected with human rights that appear in the context of technology and the internet. Media monitoring is crucial to understanding the state of inclusion in digital rights and digital space, especially for individuals marginalized in society based on gender, sexuality, and community identity.

In 2025, we observed a significant rise in activities in the digital space of Nepal compared to the past years. This year, Nepal witnessed the emergence of new and unfamiliar digital threats, marking a shift in the nature and scale of online harm. The year also saw extensive government interventions in the digital sphere, often marked by confusion between regulation, protection, and control. At the same time, numerous incidents unfolded showing how marginalised communities remained particularly vulnerable in digital spaces. Although both the government and the private sector introduced various initiatives related to digital technology and services, these efforts frequently lacked inclusion, transparency, and accountability. Consequently, incidents of privacy violations, data breaches, identity theft, online scams, unethical use of AI, hacking, technology-facilitated violence, and cybercrime continued to rise throughout the year.

In 2025, Nepal experienced huge tension between freedom of expression and expanding government surveillance efforts. The control measures led by the state, including the social media ban, repeated censorship attempts, and the proposed Social Network Bill, triggered intensified public debate on digital rights and freedom of expression. The social media ban in Nepal further fuelled the Gen-Z movement against corruption and governance failures, transforming digital rights into a political and civic issue. The year marked a significant moment for digital rights advocacy, as online expression, access to information, and state accountability came under sustained pressure. Furthermore, the spread of misinformation and disinformation

during the sensitive period by both national and international media outlets raised serious ethical concerns within the media landscape.

Similarly, the year witnessed a rise in cases of non-consensual intimate image abuse targeting women and incidents involving the blackmail of minors through the weaponization of intimate images taken by establishing deceptive romantic relationships. Marginalised communities faced increasing digital threats on social media platforms, while women who asserted their voices online were met with hostility, harassment, and cyber attacks, resulting in widespread discrimination and significant psychological distress.

Media reports throughout the year also documented numerous cases of job scams, phishing, and financial fraud carried out through platforms such as WhatsApp and Facebook. The scams were mainly carried out through impersonation of public figures and they highly targeted systemically minoritized individuals facing unemployment and a lack of digital literacy. These events showed the growing scale and sophistication of online scams in Nepal.

Media coverage further cited repeated cyberattacks on government websites and systems. The series of episodes of data breaches and unauthorised access in government websites exposed inefficiency and incapability of the government to safeguard institutions and citizens.

Our annual monitoring and observation recorded a diverse range of events within digital rights and the digital space of Nepal. However, analyses from the perspectives of women, Dalits, indigenous nationalities, and sexual and gender minorities were found to be inadequate.

Moreover, reporting on technology-based violence against women tends to follow a fixed “hard news” format, with a noticeable lack of analytical or investigative reporting that could provide a deeper understanding of the issues. Similarly, reporting on the government’s social media ban and broader platform regulation largely focused on questions of enforcement and legality. But it failed to provide a deeper social analysis of its implications for freedom of expression, digital labour, and the voices of marginalised communities.

2

Objectives

The objective of media monitoring is to analyse news, events, discussions, debates and trends to gain insights into the status of digital rights in Nepal. From a feminist perspective, media monitoring serves as a powerful tool for the critical study of news, discourse, and emerging trends.

This type of analysis is essential for understanding the narratives constructed by the media and how these narratives shape public perception and policy responses. Such a perspective is particularly important for identifying the unequal and often disproportionate impacts of digital rights issues on women, queer individuals, Dalits, Indigenous peoples, persons with disabilities, and other marginalized communities.

Moreover, understanding the existing processes of narrative construction is also crucial for developing counter-arguments and for deconstructing and re-imagining traditional approaches to digital rights. A critical analysis of the digital rights landscape promotes informed public dialogue, strengthens evidence-based policy advocacy, and encourages engagement beyond superficial or event-driven reporting. It further enables the identification of underlying power structures, systemic biases, and patterns of unequal representation that continue to shape media discourse and public understanding of digital rights.

The media monitoring further enables critical reflection on whose voices are amplified in media narratives, how issues are framed, and which perspectives remain marginalised or excluded. The findings of this report are intended to provide a strong evidence base for future media sensitisation efforts, digital rights advocacy, and the promotion of inclusive and equitable representation of diverse voices within Nepal's digital and media landscape.

3

Methodology

This report presents an analysis based on year-long monitoring of digital rights-related developments in Nepal during 2025. For this purpose, we systematically monitored, collected, reviewed, and analysed news reports, opinion pieces, and discussion articles published in major online media outlets, focusing on digital platforms, the internet, technology, digital rights, and technology-facilitated violence.

The sources for this study include verified media reports, policy documents, public statements, and official government websites. Incidents have been grouped thematically to reflect broader structural patterns rather than isolated events. In total, 553 news items and related materials were collected, which also served as the basis for previously published monthly monitoring reports.

This annual media monitoring report synthesises the key themes that emerged from these monitoring efforts and presents them under thematic headings. Within each section, incidents are organised in a logical order to ensure factual clarity and institutional accountability. The study aims to critically examine the state of digital rights in Nepali media, identify emerging trends, and highlight persistent gaps in inclusion and representation.

Body & Data began media monitoring in 2021. Since then, we have been regularly collecting, analysing, and documenting news, opinions, and debates related to digital rights and publishing monthly, quarterly, and annual reports.

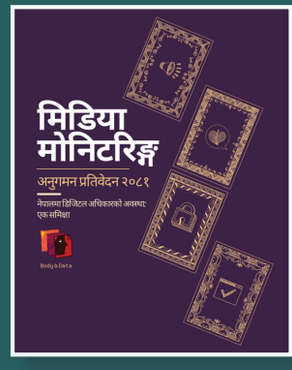
As part of our media monitoring methodology, we organise a “Media Monitoring Sharing Session (MM Sharing Session)” at the end of each month. In these sessions, we review and discuss the state of reporting on digital rights in Nepali media throughout the month.

These discussions involve deep analysis from a critical feminist and intersectional lens on issues such as digital violence, increasing surveillance on social media, privacy breaches, unequal access to technology, and legal and policy developments. This approach helps uncover the interrelation between factors such as caste, class, gender, sexuality, access, and geographic location.

the key themes that emerge from these discussions are compiled in our Monthly Media Monitoring Reports, which serve as essential references when preparing the annual report. The annual report analyses the data collected through monthly and quarterly monitoring, categorising it thematically.

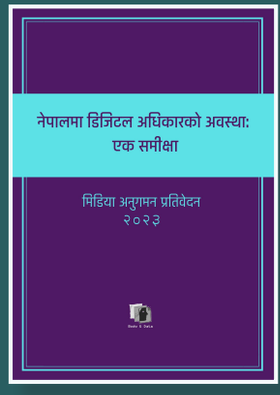
The goal of this annual report is to critically review the status of digital rights in Nepali media, identify visible trends, and highlight the lack of inclusivity. These reports serve as valuable resources for researchers, policymakers, lawmakers, journalists, activists and other stakeholders interested in understanding the evolution, trends, and challenges of digital rights discourse in Nepali media.

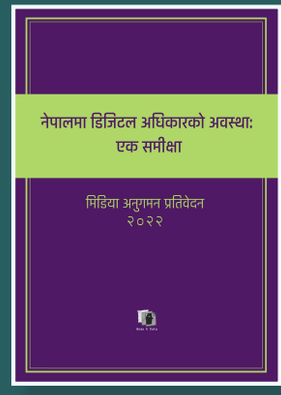
all our media monitoring reports are publicly



Note: This monitoring report has been prepared solely as an institutional initiative by Body & Data. While every effort has been made to ensure accuracy, we acknowledge the possibility of oversight or error and welcome your feedback or suggestions.

Please feel free to contact us at: communication@bodyanddata.org.





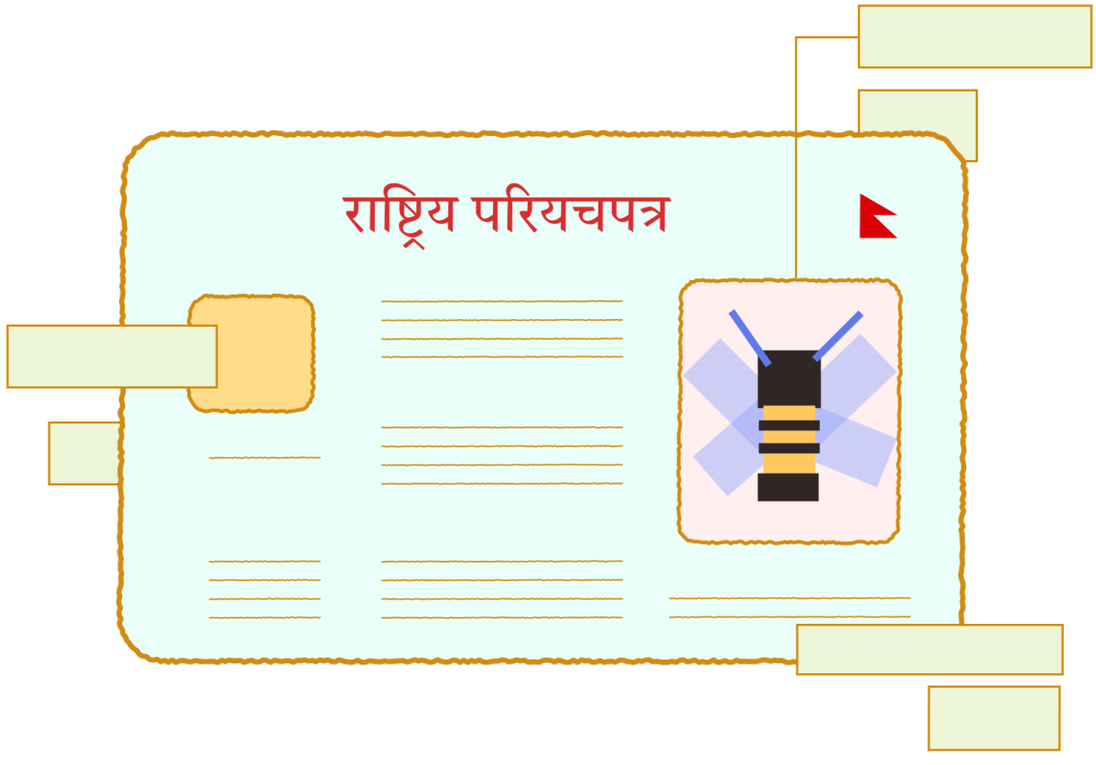
4

Thematic Observations

4.1.

Identity Theft, Privacy Breach, and

In 2025, Nepal witnessed a range of emerging digital safety threats, such as identity theft, impersonation, data misuse, and privacy breaches. A series of incidents has exposed the vulnerability of the country's data protection systems during the phase of digital transition. Similarly, the country observed a significant rise in hacking and phishing activities, which demand urgent attention and effective countermeasures.



4.1.1.

National Identity Card and Data Privacy Risk

In 2025, the expansion of digital governance in Nepal raised concerns about identity theft, privacy breaches, and the abuse of personal data. In January, the government integrated the National Identity Card (NID) system with platforms such as the Nagarik App to streamline access to public services and enhance administrative efficiency. However, this centralisation increased the risks of cyberattacks, data misuse, and unauthorised surveillance. Further, proposals to make the NID mandatory for access to public services came with the danger of deepening exclusion, especially for marginalized communities with structural barriers to obtaining the card. As digital ID is a "gatekeeper" to citizenship for marginalised groups like transgender community, which makes the NID not just a privacy risk but also a tool of erasure.

image source: ICT Samachaar

image source: TechPana.com

3,77,000+

new voters registered using NID

In November, the Election Commission integrated the online voter registration system with the National ID (NID) database to make voter registration more accessible, particularly for those who are geographically displaced from their voting districts. More than 3,77,000 new voters registered using this method, which shows the need. However, it is also important to note that this synchronisation further consolidated sensitive personal data into a monolithic state architecture. This integration also concentrated large volumes of sensitive personal data within interconnected systems. Given the NID's history of excessive data harvesting and its potential as a tool for state surveillance, this move risks transforming a mechanism of democratic participation into one of digital policing.

Furthermore, we saw technical weaknesses, including server failures and system vulnerabilities, in the website of Election Commission. Although authorities assured the public about data safety, recurring rumours of data breaches continued to erode trust. When there are such failures in the government websites, it is always the public data that is highly compromised. Without proper data protection and independent oversight, such centralization threatens the privacy and political safety of systemically minoritised populations.

Apart from this, Nepal's digital ecosystem faced broader security challenges with digital vulnerabilities. Even the official website of the Nepal Police was not safe. Also, the WhatsApp account of the Sunsari District Police Chief was hacked, with messages and money requests sent to the public. Scammers, in a similar manner, impersonated police officers, claiming that they would refund the money that was lost in online scams, and they used fake Facebook pages and images of former IGP Sarbendra Khanal. The very authorities meant to ensure public safety were mimicked to exploit victims. By this exploitation, victims got scammed twice: first by the impostors and then by a system that fails to protect them.

image source: DISCORD

image source: NTC

image source: TechPana.com

Moreover, the Gen-Z protests on September 8 and 9 exposed weaknesses in Nepal's digital infrastructure. Hackers exploited Malika Rural Municipality's SMS gateway, sending violent alerts under MALIKA_ALRT. Though the ID was suspended, Nepal Telecom made a claim of no responsibility. Furthermore, Discord, which was widely used by protesters, suffered a ransom-driven breach. This affected over 70,000 users, including personal and financial data via a third-party provider. Though Discord revoked access and notified affected users, the incident pointed to the risk of relying on external platforms for critical communication during political events. In addition, a hacking group called Midnight Ops Nepal defaced the Department of Hydrology and Meteorology's website, which affected public trust. This year, hacker and hacktivist groups such as KAZU, DIKU, and GenZ Rising Nepal exposed serious weaknesses in cybersecurity infrastructure and data protection by targeting government systems, political parties, and public platforms. While their actions were framed as a political protest, the theft of personal data from the Public Service Commission raises the question, "Who is harmed?" It is hundreds of thousands of everyday, unrelated users whose data is now looted.

4.2.

Financial Fraud, Online Scams, and Illicit Digital Activities

The exploitation of digital platforms in Nepal has grown into organised and increasingly sophisticated forms of fraud that combine technology with psychological manipulation. These crimes are causing serious financial and emotional harm. The alarming rise of financial fraud and online scams in 2025 has raised concerns about broader threats to public trust and digital safety.

Image source: Lokaantar.com

4.2.1. Organised Online Scam and Financial Fraud

Like the previous year, fraudulent activities continued to be carried out through digital media targeting the systemically minoritized. Within this, the authorities uncovered organised fraud networks operating both domestically and across borders. The 52 individuals, including six Chinese nationals, were arrested as they were carrying out scams through fake dating apps and illicit call centres. Similarly, in the case of Safaraj Khadka, forged government and bank documents were shared through WhatsApp and Viber. The media monitoring also recorded scams involving fake identities, such as Kusheshwar Mehta pretending to be a Thai bank manager, to cheat people. Together, these incidents revealed how everyday digital tools were misused for serious crimes.

This year, financial scams also constituted a significant portion of cybercrime. The fake investment apps and fraudulent schemes, such as the Nepse AI app, caused losses worth millions of rupees for citizens. This indicated gaps in enforcement and oversight rather than flaws in the technology itself. Also, fraudulent activities were carried out not only by larger networks but also by a few individuals. In individual cases, Milan, a person with a disability, and Madan, a civil service aspirant, both were scammed online, and they lost substantial amounts of money. These incidents exposed how systemically minoritized individuals were often left financially and emotionally devastated.

Moreover, the year also recorded such cases where innocent people got involved in online scams and faced legal consequences. For example, Miraj and Rajan were unknowingly involved in fraud through the bank accounts in their names. Similarly, Samjhana and Anu (names changed) were emotionally manipulated into online

scams. Later, all of them were held legally accountable. These episodes were the government's failure to protect citizens despite existing policies. In these kinds of online scams, most of the victims were youth, especially those facing unemployment. Scammers often targeted them through fake job offers or romantic relationships, leading to identity theft, emotional abuse, and even legal consequences.

Similarly, digital threats are also developing in a newer way to gain public trust for fraudulent activities. This year, celebrity impersonations using names like Sunita Dangol, Sadiksha Shrestha, and Swastima Khadka were repeatedly seen to exploit public trust and conduct online job scams. The scammers also ran fake lucky draws, QR-code fraud, and Scams promising easy incomes. These schemes targeted both everyday users and high-profile individuals, which have exposed gaps in financial consumer protection and regulatory oversight.

According to the Nepal Police and Nepal Rastra Bank, cyber scams dominated suspicious financial activities, with common tactics including OTP theft, fake jobs and investments, and unauthorised digital wallet transfers. Despite repeated public warnings from police and officials, scams continued to evolve faster than awareness efforts.

डेटिङ ऐप प्रयोग गरी नेपाली युवतीमार्फत अनलाइन ठगी गराउने चिनियाँ नागरिक पक्राउ

टेकपाना असार १८, २०८२ १७:४८

image source: techpana.com

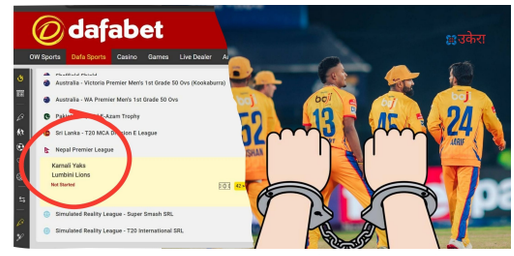


image source: ukeraa.com

4.2.2.

Illegal Online Gambling

Over the past year, the expansion of digital platforms has fueled illegal online gambling and other illicit digital activities in Nepal. The promotion of illegal online betting used popular content creators to manipulate audiences. The Content creators, including Rajkumar Thapa (Moto Vlogger), Vibid Jung Thapa (MRB Vlog), and Sandesh Tamang (2B Gamer), promoted banned online gambling platforms like Khalti 88, Jaibaji, and JW8. The advertisements were particularly made during the Dashain–Tihar period, luring users with promises of easy money and bonuses. In this context, both domestic and foreign actors promoted these acts, taking advantage of weak monitoring and limited cross-border enforcement.

On the other hand, deepfake technology was misused to gain public trust and carry out gambling activities. For example, public figures, including Shrinkhala Khatiwada and Balen Shah, were falsely portrayed as endorsing illegal gambling platforms.

Though gambling is prohibited under national law, online betting platforms continued to operate openly by exploiting regulatory loopholes and weak enforcement mechanisms. These platforms misused images of public figures, including well-known cricketers, such as Paras Khadka, and disguised advertisements as news content to gain legitimacy. Illegal online gambling during the year further illustrated the increasingly organised nature of digital crime. Betting platforms linked to events such as the Nepal Premier League continued to operate through surrogate advertising and cross-border networks. These incidents highlighted persistent weaknesses in digital governance, cybersecurity enforcement, and ethical oversight of online platforms in Nepal.

4.3.

Technology-Facilitated Gender Based

In 2025, technology continued to enable gender-based and identity-related violence online. Digital platforms and anonymous users perpetrated widespread misogynistic attacks, and celebrities who spoke out often faced public backlash on social media. Online harm frequently moved over into real-world violence as well. The cases of blackmail using non-consensual intimate images and the grooming of minors were also reported in multiple incidents. Also, marginalised groups tackled the threat of technology. These incidents exposed gaps in digital regulation, weak support for victims, and institutional indifference toward cybercrimes. Trolling, threats, abusive comments, and exploitation of private content further increased the vulnerability of marginalised communities.

4.3.1.

Online-Offline Continuum of Post-Separation Abuse

Incidents of exploitation of non-consensual intimate images and videos of women post-separation were observed throughout 2025. These incidents highlight the systemic expansion of coercive control in both online and offline spaces over women, where the perpetrators exploit the permanence of the internet to bypass physical boundaries, ensuring that the victim remains under surveillance and psychological duress long after the relationship ends. These incidents of post-separation abuse demonstrate how women's bodies are weaponised

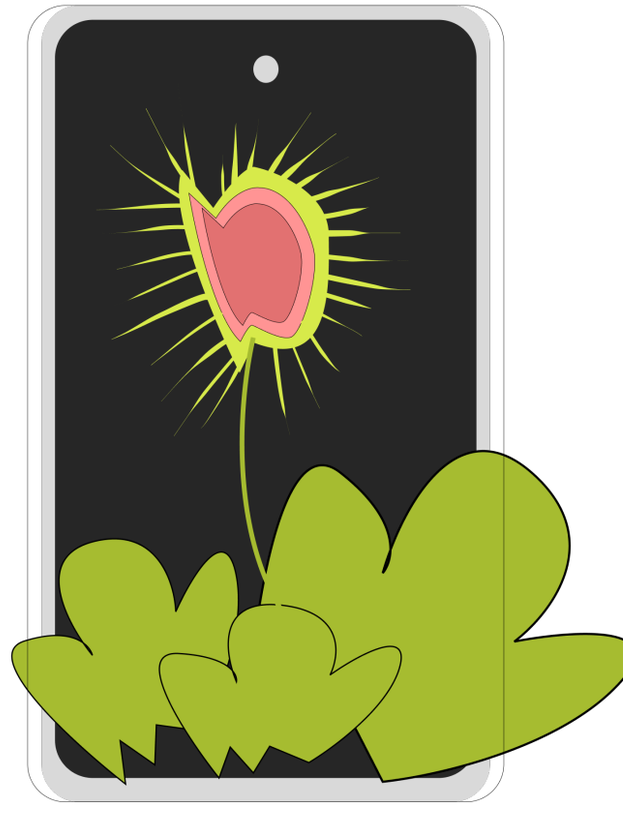


image source: .technologykhabar.com

as tools of control and retaliation even in online spaces. In a case of intergenerational harm, a man used intimate videos to blackmail his wife with recordings that even involved his own daughter. The suicide of Anjana Rizal this year exposed the impact of technology-facilitated violence, where the online violence amplified in the offline space.

of money. These incidents exposed how systemically minoritized individuals were often left financially and emotionally devastated.

Moreover, the year also recorded such cases where innocent people got involved in online scams and faced legal consequences. For example, Miraj and Rajan were unknowingly involved in fraud through the bank accounts in their names. Similarly, Samjhana and Anu (names changed) were emotionally manipulated into online scams. Later, all of them were held legally accountable.

आफ्नै छोरीको अश्लील भिडिओ आमालाई पठाएर बुवाले गरे ब्ल्याकमेल

टेकपाना जेठ २०, २०८२ २२:३३

image source: techpana.com

फेसबुकमा साथी बनेका युवकले काठमाडौं घुमाउने बहानामा बोलाएर गरे १३ वर्षीया नाबालिका बलात्कार

टेकपाना पुस ९, २०८२ १७:३

image source: techpana.com

फेसबुकबाट चिनजान भएका व्यक्तिलाई भेट्न गएकी नाबालिकामाथि पटक-पटक बलात्कार

टेकपाना असार ६, २०८२ १५:५५

image source: techpana.com

4.3.2. Intersectional Identity and Online Violence

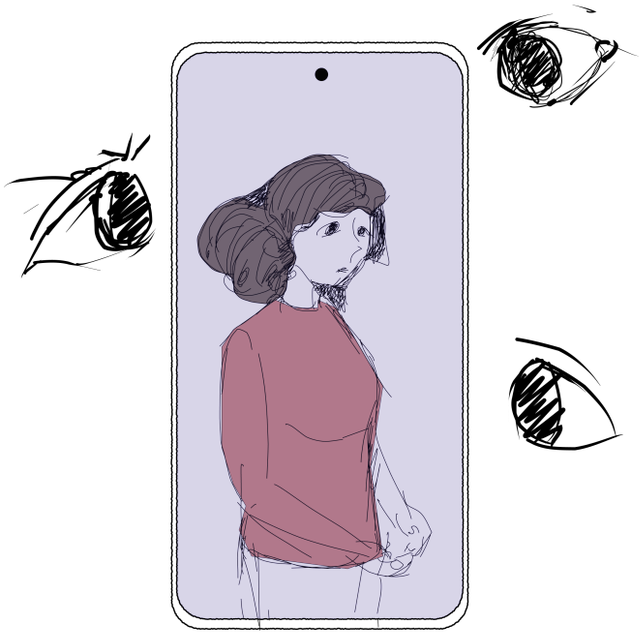
2025 showed that the nature of online violence disproportionately targets those at the intersections of multiple forms of marginalization. A minor with a disability was lured online, raped, and subsequently blackmailed, illustrating how perpetrators exploit both age and disability through digital grooming. Similarly, a 13-year-old girl was lured through Facebook and sexually abused, proving that “online” violence is often a precursor to physical trauma. Moreover, the arrest of Topendra Shahi for circulating abusive videos of young women from the Raute community highlighted a form of colonial digital violence. The exoticization and targeting of Indigenous bodies are not isolated incidents but are rooted in systemic discrimination and the historical marginalization of Indigenous communities.

4.3.3.

Misogynistic Intimidation, Institutional Betrayal and the Policing of Survivors

Even in 2025, we observed the state's failure to provide justice to survivors of TFGBV. Survivors like Smriti Paudel, who was stalked for a year by a politically connected individual, found themselves unheard both online and offline. The legal system's inadequacy was further highlighted in the case of 19-year-old Julie Jha, who was arrested following the death of a man who had allegedly groomed her since she was a minor. Rather than providing trauma-informed justice, police responses were widely criticized for pushing survivors toward informal settlements. This reinforces a toxic system where women are left unsupported and blamed for the violence they endure.

Besides individual violations, digital platforms were systematically exploited to suppress female voices in the public sphere. Public celebrities like Richa Sharma, Samikshya Adhikari and Eleena Chauhan were forced to publicly name their abusers due to slow legal support and responses. While this visibility builds solidarity, it also creates further legal and social risks for the victims.



अनि एलिना खराब कमेन्ट गर्नेहरूविरुद्ध लड्न थालिन्

'अब यहाँबाट पछि हटें भनें मपछिको पुस्ताले झन् धेरै सहनुपर्ने हुन्छ । कम्तीमा महिलाहरूलाई नेपालमा बाँझ्न सजिलो बनाइदेलान् कि ।'

असार २०, २०८२ | समर्पण श्री

महिला इन्फ्लुएन्सर विरुद्ध जथाभावी कमेन्ट गर्नेहरूलाई कारबाहीको दायरामा ल्याउने प्रहरीको चेतावनी

टेकपाना | कात्तिक ७, २०८२ १२:३८

The case of comedian Sajan Shrestha's sisters, who received rape threats in response to his content, illustrates how women's bodies are used as collateral for male-centric conflicts. Furthermore, the post of former Nepali cricket captain Sandeep Lamichhane accusing Paradigm TV of defamation triggered a wave of misogynistic attacks against female guests of the show. Influencers such as Dr Trishala Gurung, Nitu Malla Thakuri, Jasmin Maharjan, and Suruchi Budhathoki faced gender based harassment online that forced them to restrict comments. Thereafter, the Cyber Bureau warned that such actions violate the Electronic Transactions Act, 2063.

4.4.

Freedom of Expression in Crisis

Nepal's current legal and policy landscape indicates an increasingly restrictive environment for freedom of expression, particularly in the digital sphere. Authorities have relied heavily on Section 47 of the Electronic Transactions Act, 2063, a broadly worded provision that has been repeatedly used to suppress online criticism. Its vague scope has enabled action against journalists, lawyers, artists, and daily social media users, raising serious concerns about arbitrary enforcement and abuse of power.

4.4.1.

Social Media Control: An Oppressive and Undemocratic Move

In February, the Minister for Communication and Information Technology, Prithivi Subba Gurung, introduced the "Social Network Bill, 2081" in the National Assembly. The government stated that the bill aimed to regulate social media platforms and their users. According to the bill, social media companies would need to register with the government to operate in Nepal. It also called for stricter content moderation policies and aimed to address harmful online activities such as extortion, cyberbullying, phishing, scams, and other forms of digital crime. However, the proposed legislation faced strong criticism from journalists, civil society groups, and digital rights advocates. Critics argued that some provisions could negatively affect democratic values and digital freedoms. They expressed serious concerns about possible restrictions on online anonymity, the risk of controlling dissenting voices, and potential threats to independent journalism. The Federation of Nepali Journalists described the bill as an attack on press freedom and freedom of expression. Such an attempt by the government was widely viewed as a way to silence dissent and was considered dangerous for the protection of the public's freedom of expression.

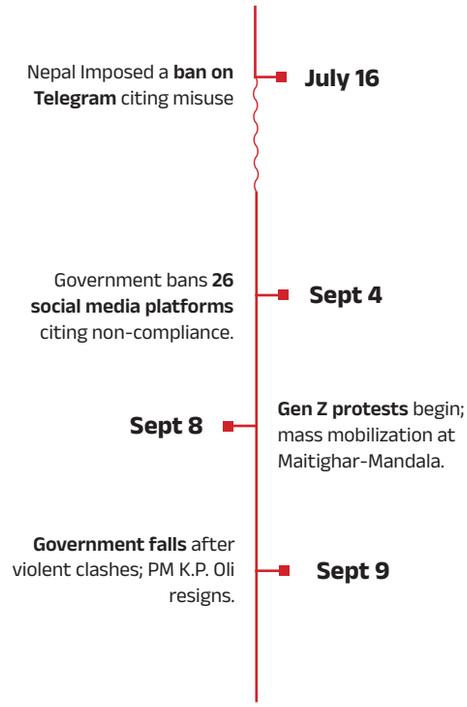
In July, Nepal imposed a ban on Telegram, citing its misuse in fraud, drug trafficking, and money laundering. However, legal experts argued that the blanket ban unfairly impacts millions of legitimate users and poses a

serious threat to free expression. A coalition of 27 Nepali digital rights groups then condemned the Telegram ban, warning of the negative effects on the digital economy, education, and marginalized communities who rely on Telegram for communication.

Throughout the year, the government of Nepal adopted an increasingly coercive approach to the regulation of global social media platforms. The government repeatedly set deadlines for platforms like Facebook, Instagram, and X to register locally or face potential blocking. Though some platforms, including TikTok, complied with registration requirements, major companies such as Meta did not. Following the expiration of the seven-day deadline on Bhadra 19, the Government of Nepal banned social media platforms that were not registered with the Ministry of Communication and Information Technology. The Internet Service Providers' Association of Nepal (ISPAN) strongly opposed the move and cautioned that such blocking would create significant technical challenges, encourage widespread VPN use, and damage Nepal's digital credibility.

Legal experts further criticised that the move contradicted the Supreme Court's directive, which called for regulation through law rather than administrative action. As criticism grew, IT Advisor Shaligram Parajuli

image source: 1. BBC News, 2. The Guardians



had disseminated misleading claims stating that Meta had initiated registration procedures, which were later denied by relevant officials. The then government faced further backlash when the offices of the Prime Minister and ministers continued to use banned platforms like Facebook and WhatsApp for official communication, drawing accusations of regulatory inconsistency and institutional hypocrisy.

Following nationwide Gen Z protests on September 8 and 9, the Council of Ministers decided to lift the social media ban and restore access to all social media platforms. Moreover, the Indian Supreme Court refused to impose a blanket ban on pornography websites, citing Nepal's protests that blanket restrictions produce more resistance than solutions. Effective governance of digital spaces requires laws that are transparent, proportionate, and aligned with constitutional protections aligned with international human rights standards and domestic realities. Without such reforms, administrative overreach risks weakening digital rights protections and affecting Nepal's broader democratic commitments.

.

4.4.2. Press and Creative Freedom at Crisis

In 2025, several media faced the increasing legal and institutional pressure that frequently threatened independent journalism and freedom of expression. This year, media monitoring recorded a series of court interventions, legislative proposals, and regulatory actions that hampered critical and free press reporting.

In June, the court issued interim orders directing the removal of investigative reports published by online media outlets such as Nepal Khabar and Bizmandu. It was particularly in relation to reporting on Santosh Narayan Shrestha, Chair of the Securities Board of Nepal. These orders were issued on defamation grounds without engaging the Press Council Nepal, the legally mandated media regulatory body. Similarly, journalist Dilbhusan Pathak faced an arrest warrant in the same month over a YouTube episode of his Tough Talk series. His video was about a controversial hotel transaction allegedly linked to a political family.

At the policy level, the Media Council Bill and amendments to the Printing and Publication Act, 2048, were proposed. These drew criticism for potentially expanding government influence over media regulation. Media professionals expressed concern that the proposed framework expanded state authority by centralising control over appointments and dismissals within the Media Council. A writ petition was filed at the Supreme Court challenging Section 7(b) of the bill and seeking restoration of an independent regulatory framework.

Similarly, the Film Bill was proposed with the provision of granting the Ministry authority to override the Film Development Board. The bill also introduced provisions such as mandatory script approvals and post-production bans. These measures threaten filmmakers' autonomy and risk silencing creative and dissenting expression. This could disproportionately affect marginalised communities that rely on media and art to amplify their voices.

All these suppressions and developments reflect a troubling trend toward increased legal, judicial, and administrative control over the media. Without the respect for independent regulatory mechanisms, press freedom is always targeted and attacked by power. It also weakens democratic accountability and promotes self-censorship within journalism and creative expression.

Media registration and renewal will no longer be from the Information Department

According to the provisions of the Printing House and Publication Act, 2048 made by the government through the amendment of some Nepal Acts, there is now an arrangement for online registration from the District Administration Office.

श्रावण २०, २०८२ | रासस

image source: Ekantipur.com

4.4.3.

Online Speech, Political Expression and Institutional Regulation

The series of incidents from 2025 disclosed the strict institutional control over expression that challenged authority. For example, authorities took disciplinary action against 166 armed police officers for posting in uniform on TikTok. Also, TikToker Rama Basnet was arrested under the ETA,2063, for political content. In the case of "Driver Resham," online comments led to his arrest and he faced severe legal consequences.

Furthermore, the authorities sought to control dissent by banning the satirical "Banana Republic" (केरा गणतंत्र) T-shirt design. In another case, a cybercrime complaint was filed against lawyer Sujit KC for a Facebook post in which he criticised the political family. All of these activities illustrated the state's increased policing of free speech. Such measures signalled a shrinking civic space, where cyber laws are increasingly used to censor criticism and political satire.

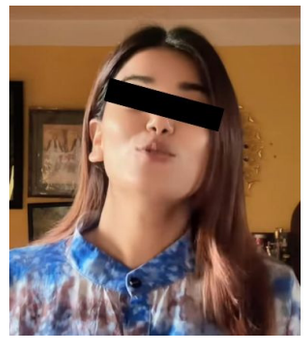


image source: TechPana

This year, creative expression also came under scrutiny. The viral songs and artistic content were reported for allegedly harming cultural values. A person was arrested for creating a rap video criticising the then Prime Minister. Civil society and rights groups warned that these practices undermine democratic participation by transforming laws intended to ensure online safety into instruments of intimidation.

अश्लील भएको भन्दै तीन लोकगीतविरुद्ध साइबर अपराध ब्युरोमा उजुरी

उकेरा संवाददाता ४४ हप्ता अघि

देउवा पुत्र जयबिरबारे फेसबुकमा लेख्दा अधिवक्ता केसीविरुद्ध साइबर अपराधको मुद्दा

उकेरा संवाददाता ४८ हप्ता अघि

Furthermore, individuals who expressed critical or dissenting views faced online harassment, threats, and coordinated backlash. Such intolerance turned social media into a hostile space for open expression. When an actress made a casual comment on the looks and potential of Hridendra Sha, she faced coordinated online abuse and boycott calls, as the opinion was taken as disrespectful by royalist groups. Similarly, choreographer Arjun Khadka faced assault for his satirical TikTok content critical of a political party. This illustrated how digital dissent provoked physical retaliation, affecting free expression and personal safety. The pattern of suppressing critics in 2025 highlighted the urgent need for strong safeguards for freedom of expression and institutional restraint.

4.5.

Digital Governance and Digital

In 2025, our annual observation saw some expansion of digital systems across government institutions, but without proper strategies. The authorities did not strengthen digital infrastructure, data protection mechanisms, and privacy safeguards at the same pace. The government authorities forwarded ambitious plans, but the goals were not backed by budget priorities. The weak digital infrastructures resulted in digital rights violations at the institutional level that directly affected citizens. They struggled to access effective remedies, while clear, accessible legal frameworks and support mechanisms remained underdeveloped.

4.5.1.

Policy Ambitions and Regulatory Gaps Seen in Digital Governance

In February, the Minister for Communication and In 2025, Nepal's digital governance landscape was defined by high-level policy ambition paired with failure in democratic execution. While the state proposed expansive frameworks, its primary focus remained on centralizing control rather than expanding digital rights or ensuring equitable access, resulting in the tools of protection being used for policing.

The government's repeated attempts to domesticate global platforms through the Social Media Operation Directive, 2080 and the subsequent Social Network Bill exposed a gap between legislative intent and enforcement capacity. These measures mandating local registration and representative appointments were met with resistance from civil society and global tech giants like Meta, X, and LinkedIn. Critics argued these provisions were less about safety and more about creating a mechanism for state surveillance and the suppression of dissent. The eventual pausing of these mandates revealed a state caught in a regulatory paradox of attempting to enforce authoritarian-style controls without the technical resources or the political will to align with international human rights standards.

A similar pattern of "rhetoric over results" emerged within the Digital Nepal Framework 2.0. Though there was an

expansive vision, progress was slow due to weak inter-agency coordination, outdated bureaucratic approaches, and insufficient public investment. Under the Economic Reform Action Plan 2082, the government introduced several market-oriented policies, including a Remote Work Policy, Digital Nomad Visas, and tax incentives for the IT sector. While these measures aim to position Nepal within the global digital economy, stakeholders remain sceptical. Without a foundation of legal clarity, transparent planning, and reliable data protection, these policies risk benefiting only a small, urban elite while the broader public remains vulnerable to system failures.

5,000

skilled professionals within five years

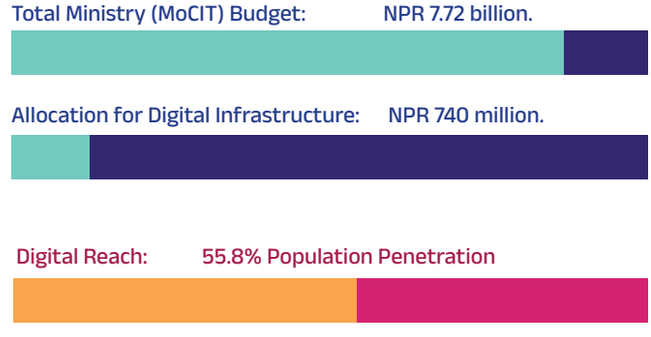
4.5.2. Low Budget Allocation for Digital Infrastructure

In 2025, the allocation of budget to digital sectors made the mismatch between digital ambition and financial commitment more evident. In FY 2082/83, of the NPR 7.72 billion allocated to the Ministry of Communication and Information Technology, only NPR 740 million was directed toward digital infrastructure. This limited investment raised serious concerns about the sustainability of flagship initiatives such as "Digital Nepal." For this, experts and the Office of the Auditor General repeatedly warned that without substantial investment in digital literacy, technical skills, and secure infrastructure, digitalisation efforts would remain fragile.

4.5.3. AI in Nepal: Opportunities and Risks

In August 2025, Nepal introduced the National AI Policy, 2082 (2025), which presents an ambitious vision to train 5,000 skilled professionals within five years. It also aimed to establish AI Excellence Centres in every province and create an AI Regulation Council to align with global standards. Experts view it as a promising step, but they also cautioned that the success will depend on adequate funding and the effective use of national data.

Also, the use of AI and technology has expanded in the criminal justice system. Nepal Police planned to adopt AI for crime analysis and offender identification, marking a shift toward data-driven policing. While this initiative has the potential to tackle technology-driven crimes, its effectiveness depends on proper training, ethical implementation, and rigorous evaluation of outcomes. Furthermore, algorithmic bias within the technology can make things difficult for systemically minoritised people.



4.6.

Misinformation, Disinformation, and

Over the past years, the rapid expansion of internet access and digital platforms has fundamentally reshaped how people receive and share information. While these technologies have empowered voices and strengthened public participation, they have also exposed a troubling reality. The same tools are increasingly being misused to spread misinformation, distort facts, and manipulate public perception. The harm becomes more visible during periods of political transition. As the country was in the phase of political transition, misinformation and disinformation were increasingly used to influence political intent and shape preferred narratives. Our media monitoring during the period recorded the growing use of artificial intelligence and digital tools to generate misleading content.

4.6.1. Rise of Misinformation and Disinformation after Gen-Z Protest

During the Gen Z protest in Nepal, several international outlets painted an incomplete and misleading picture of the movement. They largely portrayed the social media ban as the main reason behind the movement, ignoring the deeper frustrations that had been building for years, including corruption, inequality, and political failure. Some news reports even went as far as suggesting the protests supported the return of the monarchy or aimed to make Nepal a Hindu state, which completely distorted what the protesters were actually fighting for.

At the same time, false news and rumours spread rapidly from claims of army takeovers and assaults to exaggerated death tolls, creating unnecessary fear and confusion. Even trusted figures, including politicians and mayors, fueled confusion by sharing unverified information online. The then mayor of Dharan, Harka Sampang, reposted an old protest video. Similarly, CPN-UML leader Mahesh Basnet falsely claimed that Balen Shah's ancestral home had been vandalized; both posts later proved to be misleading. Similarly, some

of the news channels projected their own political narratives onto Nepal's situation. For example, the Indian media made sensational coverage, which added layers of tension. These episodes showed how fragile the information space becomes when truth and rumour collide.

However, young Nepalese use media like TikTok, Facebook, and Discord to tell their own stories and fact-check misleading claims. It showed how people can regain control over the narratives set by mainstream media.

> For an in-depth analysis of the Gen Z protest, please refer to the media monitoring report "Gen Z Protest in Nepal" by Body & Data.

After the Gen-Z movement and formation of an interim government, we witnessed multiple fake social media accounts in the names of Prime Minister Sushila Karki and several ministers. The fake profiles caused confusion and misinformation, and also misled the general public. Similarly, several fake pages of then Minister Kulman Ghising and Rameshwar Khanal were seen for many days. The issue of fake profiles of those in authority emphasised the weak digital governance and poor digital continuity during political transitions.

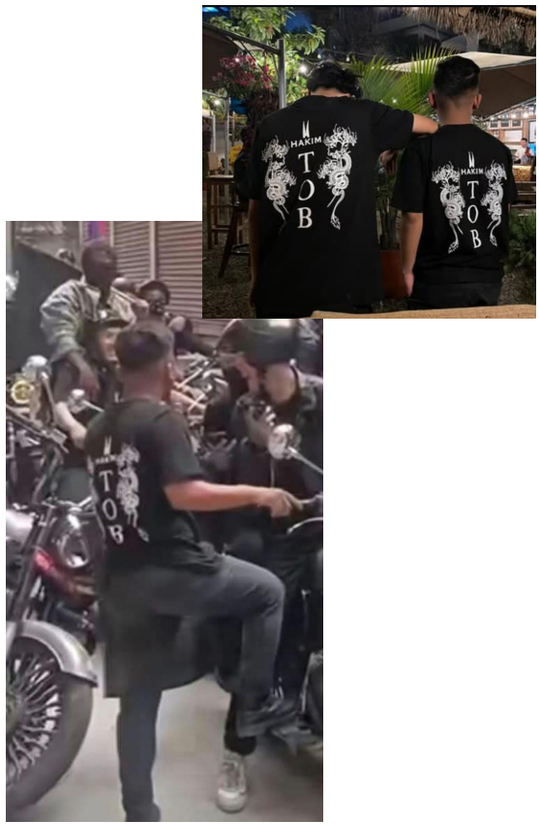


image source: The Kathmandu Post.

Simultaneously, misinformation fueled online tensions when a viral photo showed a man holding a gun in a TOB T-shirt. The acronym "TOB" was interpreted as Tibetan Original Blood, but in reality, it was "The Original Brothers," a Nepali motorcycle club. Also, the associated person was Tenzing Dawa in a 2-year-old music video with a prop gun. This way, misinformation and symbolic misinterpretation can escalate social tensions, especially when there is involvement of indigenous faces.

These incidents highlight a serious concern that misinformation is not only about wrong facts. It creates real-world harm when symbols, identities, and narratives are distorted. This risk increases even more in politically sensitive situations. For this reason, fact-checking by private institutions alone is not enough. There is a need for stronger digital critical literacy, greater accountability on platforms, and responsible

4.6.2.

Unethical Use of AI

In 2025, Nepal witnessed the unethical use and misuse of AI carried out to mislead the public and shape emotions. With the election scheduled for 5 March 2026, December 2025 saw a growing use of image-generative AI to mislead the public and manipulate emotions. For example, an AI-generated video falsely showed UML leader Pradeep Gyawali crying during the party's national convention. Similarly, a fake image depicted UML chair KP Sharma Oli kissing folk singer Jyoti Magar. Another deepfake video misused real audio from a speech by CPN-UML Secretary Mahesh Basnet but altered the visuals to defame him. These are some of Image-Based Sexual Abuse to achieve political ends. As AI-generated content became more realistic, it also became increasingly difficult to distinguish from authentic material. These developments suggest the need for heightened caution in the use of AI tools, particularly in sensitive and high-stakes areas such as law enforcement.

image source: Ekantipur.com

image source: TechPana

image source: TechPana

6

Recommendations

1. Nepal should enact a comprehensive and user-friendly data protection law that includes clear rules on data collection, processing, user consent, and safeguards against misuse.
2. Legislate against AI-generated harms (like non-consensual deepfake pornography) with a focus on restorative justice and immediate content removal, rather than just criminalizing the technology itself.
3. Explicitly protect the Freedom of Expression of activists, journalists, and marginalized communities, ensuring that "vague morality clauses" in the Electronic Transactions Act, 2063 (ETA) are not used to silence feminist dissent.
4. Prevent excessive government surveillance, as well as arbitrary control over content.
5. Establish an independent mechanism or body to address media-related and digital content.
6. Invest in modern cybersecurity infrastructure, build specialised cybercrime units and develop inter-agency coordination to regulate cybercrimes.
7. Establish secure data management systems and national data centres to protect sensitive information, avoiding foreign control on data.

8. Ensure fast track, victim-centric and user-friendly reporting and response mechanisms for cybercrime, harassment and online abuse.

9. Ensure meaningful participation of women, minorities, marginalised communities, civil society, and journalists in decision-making and policy-making related to digital rights.

10. Promote gender inclusive, feminist and intersectional approaches in cybersecurity, digital safety and digital governance policies.

11. Conduct nationwide critical digital literacy programs focusing on online safety, informed consent, misinformation detection and ethical online engagement.

12. Ensure cross-border cooperation to combat transnational cybercrimes and digital fraudulent activities.

13. Reform existing institutional frameworks to ensure efficient, accountable, transparent, inclusive and responsive digital governance.

6

Conclusion

In conclusion, this report outlines the key activities recorded in the domain of digital rights in 2025. The report identifies the evolution of digital rights issues, finds out the challenges surrounding them, explores how media have reported them, outlines the gaps and provides guidance on addressing them. Our objective is to ensure equality, integrity, privacy, and security in the digital space. The report has been prepared in alignment with guaranteeing equitable access and protection for all. It further seeks to point out the necessary

Media Coverage analyzed in this report has been sourced from the following outlets:

The Kathmandu Post, Techpana, Ratopati, Kantipur, Onlinekhabar, Nepal Press, Shilapatra, Gorkhapatra, BBC News, Desh Sanchar, Nagarik News, ICT Samachar, ICT Frame, Nepal Live, Himal Press, Setopati, Naya Patrika, Thahakhabar, BarhaKhari, The Rising Nepal, The Himalayan Times, Nepal Khabar, Bizness News, Ukeraa, Jus Nepal, Global Nagarik, Khabarhub, Online Patrika, Nagarik Dainik, The Farsight, Republica, Annapurna Post, Clickmandu, Nepal Fact Check, Technology Khabar, Rajdhani Daily, Kalakarmi, Nepal Live, Lokantaar

Researcher
Smriti Ranabhat

Co - Researcher
Nuva Rai

Cover and Layout Design
Rojan Ghimire

Cover Illustrations
Monisha Choudhary

Published by
Body & Data

With Support from
Vision for Change

Stay connected with us as we build a feminist ecosystem!
Facebook Instagram Bluesky X
@bodyanddata

Body & Data for an accessible, safe and just digital space for all.
communication@bodyanddata.org
bodyanddata.org

Annual Report of Media Monitoring, 2025

Body & Data

Body & Data

Body & Data for an accessible, safe and just digital space for all.

communication@bodyanddata.org
www. bodyanddata.org