

NEPAL JOINT REPORT OF NON-GOVERNMENTAL ORGANIZATION ON UNIVERSAL PERIODIC REVIEW (UPR)

51ST SESSION (FOURTH CYCLE)

SUBMITTED BY
DIGITAL RIGHTS NEPAL IN COORDINATION
WITH DIGITAL RIGHTS ACTION GROUP (DRAG)

SUBMITTED TO
UNITED NATIONS HUMAN RIGHTS COUNCIL

16 JULY 2025

DRAG Secretariat

Digital Rights Nepal (DRN)

KMC-2, Neel Saraswati Marg, Kathmandu Nepal

E-mail- info@digitalrightsnepal.org

Website: www.digitalrightsnepal.org

DRAG Members



Organizations in solidarity with this report

Asia Pacific Internet Governance Academy Nepal Chapter, Body & Data, Center for Media Research – Nepal, Digital Media Foundation, DCA Nepal, Diyopost.com, Media Advocacy Group, National Policy Forum, Sancharika Samuha, Techpana, Technology Khabar.com, The Story Kitchen, Youth Innovation Lab

NEPAL

A Joint Submission by Digital Rights Nepal in Coordination with Digital Rights Action Group (DRAG) to the United Nations Universal Periodic Review 51st Session (Fourth Cycle) of the UPR Working Group of the Human Rights Council Concerning Digital Rights as Human Rights in Nepal

July 2025

INTRODUCTION

1. This joint submission has been prepared by Digital Rights Nepal, in coordination with Digital Rights Action Group (DRAG), comprised of Digital Rights Nepal, Women Leaders in Technology, Dignity Initiative, and Open Internet Nepal, a consortium of civil society organizations working for digital rights in Nepal. The secretariat of the DRAG is operated by Digital Rights Nepal, a not-for-profit initiative dedicated to the protection and promotion of digital rights in Nepal since 2020. It focuses on digital rights issues such as the right to online freedom of expression and association, online privacy, access to information, internet governance, cyber laws, policies, and cybersecurity. This submission highlights the issues of digital rights, including online freedom of expression and association, online privacy and data protection, and access to information.

METHODOLOGY

2. This report is the result of stakeholder consultations, media monitoring, and a desk review conducted between 2021 and June 2025. A national stakeholder consultation was held before finalizing the report. In total, 24 thematic experts were consulted during its preparation.

IMPLEMENTATION STATUS OF THE THIRD UPR REVIEW RECOMMENDATIONS (2021) ON DIGITAL RIGHTS

3. In Nepal's third cycle of UPR, 14 recommendations were related to freedom of opinion, and the right to expression.¹ Though there was no direct quote of the term digital rights, 14 recommendations were related to online freedom of expression and association, protection of privacy, data protection, cybersecurity, media, and information technology.²
4. A recommendation specifically referred to the Electronic Transactions Act, suggesting its reform to eliminate the criminalization of speech,³ but Nepal noted this recommendation. Many other recommendations suggested reforming media and IT laws or pointed to the need for new legislation regulating information technology and cybersecurity and the protection of freedom speech in online spaces.⁴ Despite supporting many of these recommendations, implementation remains weak.⁵

GENERAL LEGAL MEASURES AND HUMAN RIGHTS FRAMEWORK CONCERNING DIGITAL RIGHTS

a. Scope of International Obligations

5. Nepal ratified the International Convention on Civil and Political Rights (ICCPR) on 14 May 1991, which recognizes the right to privacy in Article 17, freedom of expression in Article 19, and the right to peaceful assembly in Article 21. Every treaty in force is binding upon the parties to it and must be performed by them in good faith.⁶ As a state party, Nepal has an international obligation to respect, protect, and fulfill all human rights enunciated in the ICCPR.

b. Constitutional and Legislative Framework

6. The Constitution of Nepal ensures the fundamental right to freedom within Article 17, which guarantees freedom of opinion and expression and freedom to assemble peacefully; Article 19 guarantees the right to communication without censorship of publication and broadcasting or dissemination of printing, audio, and audio-visual material, including electronic publication; Article 27 guarantees the right to demand and receive information on matters of public interest; and Article 28 guarantees the right to privacy, including their documents, data, and correspondence.
7. Despite progressive constitutional recognition and guarantees, the limitation clauses within each fundamental right hinder the exercise and full enjoyment of these rights. As a result, the legislation and policies enacted in line with the constitution provide similar or excessive restrictions to it. Therefore, professionals such as journalists, media personnel, public figures, celebrities, or people critical of the government or authorities in online spaces have increasingly experienced surveillance and censorship in their personal and professional lives.⁷
8. The Electronic Transaction Act, 2008, is used as a tool to regulate and curb cyberspace in Nepal. This legislation criminalizes certain unethical internet activities. However, section 47 of this act is increasingly being misused to limit Nepal's civic space by arbitrarily arresting and criminalizing online speech, citing immorality and threats to community harmony. Criminalizing immoral content leads to criminalizing broader forms of speech, as morality is contextual and does not have a definitive scale to measure. Such restrictive regulation has included the filing of cybercrime charges against a number of citizens, including the journalist Dil Bhusan Pathak,⁸ the arrest of Ramesh Bahadur Rawal who posted a Facebook status calling Prime Minister Oli as corrupt, and Man Bahadur Karki, whose Facebook post was deemed 'harmful to social harmony'⁹ and several youths for criticizing political leaders or posting controversial content online.¹⁰ These actions raised concerns about the chilling effect on free speech.
9. National Broadcasting (Eleventh Amendment) Regulation, 2021, raises serious concerns about free online space. The amendment to Rule 8 of the Regulation obliges online TV authorized to broadcast programs through the internet to obtain approval from the Ministry of Communication and Information Technology (MoCIT). The amendment to Rule 2 has expanded to define online television as "regularly produced audiovisual programs broadcasted through the internet." This loosely defined term extends wider licensing obligations to platforms such as YouTube channels, including regulation of all kinds of videos published in social media channels like Facebook and Instagram, among others. Similarly, other key terms like "OTT" and "video on demand" are poorly defined, creating confusion and the risk of misuse, especially in ways that could restrict digital expression and access to information. High licensing fees are also impractical. The government's failure to consult stakeholders before the amendment further undermines

transparency and accountability. Therefore, implementation should be halted until necessary revisions are made in consultation with stakeholders to align with constitutional rights and democratic values. Press Council Nepal (PCN) is a statutory body set up by the Government of Nepal to promote the standards of a free press in a democratic society and to advise the government on matters relating to the development of healthy and credible journalism in the country.¹¹ However, the PCN is trying to regulate social media, going beyond the jurisdiction provided by the Press Council Act, 1990.¹²

10. A recent Directive on Managing the Use of Social Networks 2023 came into force in November 2023 and outlines 21 prohibitions for social media users. Among those, one stipulates the mandatory requirement to sign up on social media with their verified real identity to access and engage with social media platforms and directly attacks the right to anonymity.¹³ Section 27(2) of the directive imposes NPR 50,000 fine on those who do not disclose their personal details. Anonymity is crucial for democratic participation and fundamental to the right to freedom of expression, especially for groups like LGBTQ+, political activists, whistleblowers, *Dalits*, marginalized groups, and victims of domestic abuse. Without it, discussion about government misconduct or political discourse could be met with fear of undue scrutiny and retaliation.
11. The Directives mandate the social network entities to register in the Ministry of Communications and Information Technology. Consequently, TikTok faced a ban for nine months, from November 13, 2023, to August 22, 2024,¹⁴ announced in a cabinet meeting for allegedly disrupting social harmony. However, conditions for lifting the ban were not announced, raising concerns over transparency gaps. Additionally, the Supreme Court on September 26, 2024, directed the government to formulate a law regulating social media platforms when the ban was challenged via writ petition.¹⁵ In an environment where press violations against online media are increasing, the directive issued by the Supreme Court to regulate social media further exacerbates the administrative regulation on online speech and broadens transparency gaps.¹⁶

Recommendations:

- Amend Section 47 of the Electronic Transition Act to decriminalize the act of online speech, shifting it to civil penalties, aligning with the ICCPR Article 19.
- Revise the Directive on Managing the Use of Social Networks 2023 to remove mandatory real-identity registration and ensure restrictions meet the three-part tests (legality, necessity, and proportionality).
- Enact concrete legislation to regulate social media platforms without restrictive administrative regulation on online speech, abiding by the international legal frameworks and human rights frameworks.
- Limit Press Council Nepal's jurisdiction to traditional media and establish an independent authority to regulate online media transparently.
- Ensure transparent, participatory legislative processes for digital platform regulations, involving civil society and marginalized groups.

c. Human Rights Institutions, Infrastructure, and Policy Measures

12. The National Human Rights Commission is established as a constitutional human rights monitoring body established as per the Paris Principles on NHRIs.¹⁷ It is mandated to monitor

human rights violations, including all forms of digital rights; advocate for freedom of expression, online and offline; and ensure domestic legislation aligns with international human rights standards, such as the ICCPR.¹⁸ It has the authority to recommend reforms in legislation and policies that restrict online freedoms and fails to protect against harms, investigate complaints, and promote overall human rights-based approaches in digital rights policies and regulatory practices.¹⁹ However, the institutional priority of the commission in promoting digital rights is not sufficient.

13. The Ministry of Communications and Information Technology is established to formulate and implement national ICT policies that include cybersecurity strategies and online content regulation. The ministry's areas of work include, but are not limited to, contributing to formulating and bringing ICT laws and directives on social media and online platforms. It also has a role for cross-ministry coordination for the implementation of safe internet practices and collaboration with stakeholders to build cyber resilience infrastructure. However, the IT and Cybersecurity Bill and Directive on Managing the Use of Social Networks 2023 developed by the ministry are met with severe and excessive limitations on online speech and overall press freedom.²⁰
14. The Cyber Bureau of Nepal Police is the main investigation body that investigates and forwards its investigation reports to the government prosecutors for the prosecution of cybercrimes under available cyber laws such as the Electronic Transaction Act, 2008. The Bureau is authorized to handle cases such as online harassment and threats, financial fraud, online defamation, unauthorized access to computers and computer systems, etc. It has provided cyber incident reporting mechanisms through email, SMS, phone, and their online portal.²¹ From mid-July 2023 to mid-July 2024, a total of 19,730 complaints were registered at the Cyber Bureau.²² The number of complaints registered at the Bureau is far beyond its investigation capacity. There is a need to build institutional capacity to effectively handle cybercrime complaints and investigations that are victim-centric and survivor-friendly.

Recommendations:

- Incorporate all rights related to “digital rights” in the mainstream protection and monitoring framework mechanism of the NHRC.
- NHRC should include digital rights-related violations, policy restrictions, and protection measures in its policy documents, reports, and publications to document cases and sensitize the stakeholders.
- Build the capacity of the NHRC authorities and staff to be adequately updated on digital human rights and ethical internet practices in the environment where technology is constantly evolving for the promotion and better protection of digital rights.
- Adhere to the international human rights commitments made by Nepal with regard to its obligations under the ICCPR and previous UPR recommendations.
- MOCIT should adhere to the constitutional rights to freedom of opinion and expression and safeguard privacy, promote freedom of expression, ensure data protection, and prevent censorship.

- Build capacity of the Cyber Bureau by providing adequate human, financial, and technological resources.

I. IMPLEMENTATION OF INTERNATIONAL HUMAN RIGHTS OBLIGATION CONCERNING DIGITAL RIGHTS AND FREEDOM

15. The latest state-party report under the ICCPR Nepal submitted was on 21 February 2012.²³ Nepal is due to submit its third periodic report, which was initially due in 2018 and revised due in April 2022.²⁴ The lists of issues prior to the submission of the third periodic report of Nepal under the ICCPR have called upon Nepal to provide information on the steps taken by the state party to promote and protect the right to freedom of opinion and expression, including online expression.²⁵ The lists of issues have also called upon Nepal to provide information on the reports indicating that entertainers and artists such as Pranesh Gautam and Samir Ghising have faced criminal charges for exercising their freedom of expression.²⁶ Likewise, in the Concluding Observations of the Human Rights Committee in 2014 in the second periodic report, Nepal received recommendations to guarantee, in law and in practice, the right to freedom of expression to all individuals.²⁷ Despite flagging respect and protection of these rights, the situation has not improved but is getting worse day by day.²⁸ There have been no policy reforms, no institutional setup, and no adequate measure taken to address the recommendations provided for the improvement of digital rights, such as, the amendment of ETA.

II. MAJOR AREAS OF CONCERN

a. Lack of definition of Technology-Facilitated Gender-Based Violence (TFGBV)

16. Nepal recognizes the concept of online violence perpetrated towards women²⁹; however, Nepali laws do not have an accepted definition of TFGBV. Due to this, complex forms of online violence, such as doxing, non-consensual sharing of intimate images, and AI-generated deepfake materials or abusive images targeting women, girls, and marginalized groups, are unaddressed.³⁰
17. The gap in criminalizing cybercrime perpetrated towards women in the form of TFGBV combined with misuse of ETA to target speeches rather than perpetrators undermines individuals' privacy, dignity, and equality guaranteed by Articles 17 and 26 of ICCPR and Article 5 of CEDAW.

Recommendations

- Include the definition of TFGBV in the draft IT and Cybersecurity Bill as “an act of violence or harassment perpetrated through digital platforms or technologies, disproportionately affecting individuals based on gender.”
- Include in the definition that online harassment, cyberstalking, doxing, non-consensual sharing of intimate images, and the creation or dissemination of AI-generated images or deepfakes intended to harm, degrade, or intimidate victims, particularly women, LGBTQ+ individuals, and marginalized communities, are TFGBV.
- Establish a dedicated task force under the Ministry of Women, Children, and Senior Citizens to develop TFGBV policies, with input from National Women Commission, civil society and tech companies.
- Mandate platforms to implement harmful content moderation, accessible and easy reporting mechanisms, and AI-specific safeguards to create age-appropriate, safe online spaces.

b. Inadequate Online Privacy and Data Protection

18. The absence of a comprehensive data protection law leaves citizens vulnerable to unauthorized data access and misuse, particularly in the National Identity (NID) system and proposed MDMS/TERAMOCS systems.³¹ Private sectors are not adequately regulated, making them comply with data protection of the users. Nepal has adopted a national identity system to access various public services, such as passport issuance, opening bank accounts, and receiving social security allowances. The government is considering using the software and biometric data from the National Identity Card and Registration Department to enable online applications and streamline public services.³² While the initiative aims to simplify processes and reduce redundant data collection, it faces substantial legal challenges.³³ Existing laws prohibit repurposing data collected for one specific purpose and restrict third-party access to personal information.³⁴ This raises concerns about the potential for non-compliance, unauthorized access, and the misuse of citizens' sensitive data.³⁵
19. In September 2024, the Supreme Court directed Nepal Telecom to prevent unauthorized access to personal information, emphasizing the right to privacy, personal freedom, and dignity.³⁶ The verdict follows concerns raised over the procurement of a new “billing” system, which could potentially grant suppliers access to sensitive customer data. The court ruled that unauthorized access to personal information would violate fundamental constitutional rights, threatening citizens’ privacy and national security.³⁷ Yet NTA is willing to implement the MDMS and TERAMOCS system, which experts say have the serious threat to the privacy of an individual.³⁸
20. The Supreme Court’s September 2024 ruling against unauthorized data access by Nepal Telecom underscores privacy risks as per Article 17 of the ICCPR and Article 28 of the Constitution of Nepal.

Recommendation:

- Enact a comprehensive data protection law aligning with the principles of ICCPR while regulating public and private agencies.
- Establish a National Data Protection Authority (NDPA) to oversee data protection, clarify roles of NTA (telecom) and NRB (finance), and ensure inter-ministerial coordination.
- Mandate transparency in data use, require annual compliance reports, and impose penalties for breaches by public and private entities.

c. Non-Proportionate Surveillance, Media Monitoring, and Prosecution

21. Social media surveillance by the Nepal Police Cyber Bureau has proliferated without legitimate aim and judicial oversight, creating a chilling effect on freedom of expression in the discussions of national importance.³⁹
22. The expansion of AI-enabled CCTV, Facial Recognition Systems (FRS), and Automatic Number Plate Recognition Systems (ANPRS) lacks legal oversight, risking privacy violations. For instance, Kathmandu Metropolitan City allocated 169 million rupees in the fiscal year 2023-2024 to install CCTV cameras.⁴⁰ The trend of installing more such cameras is on the rise. Likewise, Bhaktapur Metropolitan plans to install 418 high-capacity cameras with ANPRS capabilities.⁴¹ Without proper legal frameworks and oversight governing the collection, use, and storage of such

data, significant privacy concerns are raised. These measures could facilitate state surveillance and censorship.

23. Although retracted in March 2024⁴², the Media Monitoring Directive introduced by the Ministry of Home Affairs⁴³ authorized chief district officers to monitor online and print media following backlash from civil society and media organizations.⁴⁴ The directive was initially intended to increase oversight of media content, but it raised concerns about press freedom and the potential for government overreach. The retraction came after widespread criticism from journalists, civil rights groups, and international bodies, who warned that such actions could stifle free speech.⁴⁵
24. In April 2024, the publisher and editor of the Kathmandu-based news website and YouTube channel, Sidhakura.com, were convicted for contempt of court.⁴⁶ The Supreme Court found that they had aired baseless content, which claimed that media house chairpersons had met with judges to dismiss corruption cases.⁴⁷ The court imposed jail sentences on the publisher and editor, concluding that they had failed to verify the content's authenticity, thus defaming the judiciary. This raises serious concern about judicial accountability and proportionality of punishment.⁴⁸

Recommendation:

- Establish a legal framework governing surveillance technology, ensuring compliance with privacy and freedom of expression rights as enshrined in Articles 17 and 19 of the ICCPR.
- Enable judicial oversight over social media surveillance, ensuring transparency, legitimacy, proportionality, and legality of such action.
- Strengthen oversight mechanisms to check and balance arbitrary media monitoring and ensure accountability for state actions.
- Reform and review contempt and defamation laws to align with international best practices by decriminalizing defamation and limiting contempt powers to cases where there is no real and immediate harm to the judicial process.
- Ensure proportionality in judicial responses to contempt cases with civil remedies before resorting to imprisonment.

d. Cybersecurity Vulnerabilities

25. Individuals' personal data are under systemic vulnerabilities due to failure to invest in cybersecurity infrastructure and resources.⁴⁹ Persistent cyberattacks, including DDoS attacks on government servers,⁵⁰ breaches of local government websites, and malware incidents on critical state units such as the Passport Department and⁵¹ Tribhuvan University (TU), are further concerning. The TU faced challenges in implementing online services as its website was hacked by a 12th grader in February 2024.⁵² These breaches in the local governments disrupted administrative operations and left essential services such as public notices, advertisements, and social security systems in limbo. The National Vigilance Center's website was hacked, resulting in the loss of five months' worth of property details registration data.⁵³ Similarly, the Passport Department suffered a malware attack that crippled its application system, causing significant delays in passport-related services.⁵⁴ Additional breaches of the teacher personnel records system and Tribhuvan University's online exam platform exposed glaring inadequacies in Nepal's cybersecurity measures.⁵⁵

26. Negligence in renewing critical software licenses caused over half a dozen ministry websites to go offline.⁵⁶ Additionally, funding shortages jeopardized operations at the Integrated Data Management Center and Disaster Recovery Centre (DRC), further disrupting emergency services and destabilizing the nation's digital infrastructure.

Recommendations

- Develop a robust national cybersecurity strategy with adequate funding for infrastructure and regular audits.
- Strengthen cybersecurity for public services through capacity building and stakeholder engagement.
- Enhance forensic investigation capabilities with a dedicated digital forensics unit to address cybercrimes and TFGBV.

e. Digital Divide and Access to Civic Space

27. Despite judicial recognition of internet access as a fundamental right, only 37.8% of households have internet connectivity,⁵⁷ disproportionately excluding marginalized communities (e.g., women, dalits, ethnic minorities, persons with disabilities) from online civic spaces, violating non-discrimination principles (ICCPR Article 26). The rural internet program in Nepal faces significant challenges, hindering its effectiveness in bridging the digital divide. These challenges include infrastructure limitations, lack of access to electricity and devices, high costs, and insufficient technical skills. While the government has made efforts to expand broadband, particularly through rural telecom funds, the focus has largely been on urban areas, leaving many rural communities with limited or no internet access.⁵⁸

Recommendation:

- Expand affordable internet access and digital infrastructure in rural and marginalized areas/groups.
- Implement digital literacy programs for marginalized groups, emphasizing TFGBV awareness and online safety.
- Develop STEM programs encouraging young people especially girls and women to pursue the professions that are safe from disruptions in fast paced technological environment.
- Recognize digital rights, including internet access and privacy, as fundamental rights in national legislation.

f. Lack of Institutional Capacity

28. Public institutions, such as the judiciary, investigators and prosecutors, and the NHRIs, are not adequately capacitated to address newly developing forms of online challenges such as TFGB, AI-enabled abuses, online child sexual abuse and exploitation, and digital rights violations, limiting effective remedies.⁵⁹

Recommendation:

- Build capacity of the judiciary, NHRC, prosecutors, and law enforcement officials through training on digital rights, TFGBV, and AI, incorporating GEDSI principles.
- Enact a “Comprehensive Act to amend specific Act” to integrate TFGBV, forms of cybercrimes, and technology-facilitated child sexual abuse into relevant laws (e.g., ETA, Domestic Violence Act, Children’s Act).

g. Responsible Technology and Tech Diplomacy

29. Tech companies like Meta lack localized accountability for addressing TFGBV and context-specific abuses (e.g., caste-based harassment).⁶⁰ Limited capacity in tech corporate diplomacy hinders Nepal’s ability to tackle cross-border digital crimes.⁶¹

Recommendation:

- Promote tech corporate diplomacy through engagement in global forums (e.g., Budapest Convention) to address cross-border TFGBV and AI abuse and ensure effective coordination with law enforcement agencies to address TFGBV, and content moderation, with transparent policies.

h. Absence of Safe Cyberspace for Users

30. Many internet users in Nepal lack safe practices when using internet technologies, digital platforms, and social media, making them vulnerable to online abuse, exploitation, harassment, bullying, deception, and fraud, among others. Women, girls, influencers, and artists are often harassed and trolled through hateful comments and manipulated videos, making them feel unsafe on social media platforms.⁶² Such abusive behaviors through fake accounts and pseudonyms go unchecked and the abusers remain scot-free. Children do not have safe cyberspace, having access only to the age-appropriate content.

31. Dalits are frequently targeted on social media with casteist slurs, threats, and demeaning content on social media platforms, perpetuating discrimination and social exclusion.⁶³

i. Absence of Safe and Confidential Reporting Mechanisms

32. Victims of TFGBV and internet-related offences struggle to receive accessible, guided, safe, and confidential reporting mechanisms, discouraging women and children from reporting such cases to the concerned authorities.⁶⁴

Recommendation:

- Establish a dedicated helpline and online portal for TFGBV, managed by the Ministry of Women, Children, and Senior Citizens, with multilingual access.
- Ensure victim-centric protocols with anonymity and data protection, aligned with General Data Protection Regulation (GDPR) principles.
- Raise awareness about reporting mechanisms through campaigns targeting youth and vulnerable groups.

j. Challenges related to Budgetary and Policy Integration

33. Initiatives related to digital literacy, advocacy and TFGBV mitigation are underfunded and not prioritized in national budgets or educational plans, limiting their impact.

Recommendation:

- Allocate budgetary resources to work for digital forensics, data storage infrastructure, and public awareness campaigns in national and provincial budgets.
- Integrate digital rights and TFGBV into annual implementation plans, educational curricula, and national development frameworks, aligning with SDGs.
- Foster inter-ministerial coordination between MoCIT, Ministry of Women, Children, and Senior Citizens, and other agencies to streamline policies.

¹ Nepal's Third Cycle of Universal Periodic Review, 2021, see A/HRC/47/10/Add.1, Para.6.

² A/HRC/47/10/Add.1 - Para.6, Recommendation 159.73 (Brazil), 159.74 (Chile), 159.75 (Czechia), 159.77 (Estonia), 159.78 (France), 159.79 (Greece), 159.81 (Iceland), 159.82 (Latvia), 159.88 (Australia), 159.84 (Mexico), 159.89 (United States of America), 159.104 (Canada)

³ See A/HRC/47/10/Add.1 - Para.6. 159.89 (United States of America).

⁴ Ibid.

⁵ Expressed by experts and participants in DRAG's consultation meeting.

⁶ Article 26, Vienna Convention on the Law of Treaties, 1969.

⁷ Digital Rights Nepal, Safeguarding Freedom of Expression Online, Media Defence, Oct. 3, 2023, available at <https://www.mediadefence.org/news/freedom-of-expression-digital-rights-nepal/#:~:text=DRN%20was%20established%20in%202020%20with%20a,digital%20space%20for%20all%20individuals%20in%20Nepal.>

⁸ <https://kathmandupost.com/national/2025/06/30/cybercrime-case-filed-against-journalist-dil-bhusan-pathak>

⁹ Asian Human Rights Commission, *Nepal: Activists and Online Critics Arrested to Stifle Dissent as Journalists Remain at Risk*, <http://www.humanrights.asia/opinions/AHRC-JST-005-2024>

¹⁰ Nepal: Activists and Online Critics Arrested to Stifle Dissent as Journalists Remain at Risk, available at <https://monitor.civicus.org/explore/nepal-activists-and-online-critics-arrested-to-stifle-dissent-as-journalists-remain-at-risk/>

¹¹ <https://www.presscouncilnepal.gov.np/en/about/>

¹² <https://www.presscouncilnepal.gov.np/en/category/acts/>

¹³ Section 4(a), Social Media Regulation Directives, 2023.

¹⁴ <https://dig.watch/updates/nepal-lifts-tiktok-ban-after-nine-months>

¹⁵ Digital Rights Nepal, State of Digital Rights and Safety in Nepal 2024, available at <https://digitalrightsnepal.org/wp-content/uploads/2025/05/STATE-OF-DIGITAL-RIGHTS-AND-SAFETY-IN-NEPAL-2024-1-1-2.pdf>

¹⁶ Ibid.

¹⁷ Article 248, The Constitution of Nepal (2015).

¹⁸ Ibid. Article 249.

¹⁹ Ibid.

²⁰ <https://monitor.civicus.org/explore/nepal-restrictive-social-media-legislation-targeting-of-journalists-and-excessive-force-at-protests-put-freedoms-at-risk/#:~:text=In%20recent%20months%2C%20the%20government,%2C%20penalisation%2C%20and%20content%20moderation.>

²¹ <https://cyberbureau.nepalpolice.gov.np/report-cyber-crime/>

²² Nepal Cyber Bureau Statistics, 2025. <https://cyberbureau.nepalpolice.gov.np/report-cyber-crime/>

²³ https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/countries.aspx?CountryCode=NPL&Lang=EN

²⁴ Ibid.

-
- ²⁵ CCPR/C/NPL/QPR/3; available at:
https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2FC%2FNPL%2FQPR%2F3&Lang=en
- ²⁶ Ibid. Para 20 (c).
- ²⁷ CCPR/C/NPL/CO/2; Concluding observations on the second periodic report of Nepal, Para 19.
- ²⁸ Nepal Witness a Sharp Rise in Press Freedom Violations: Study, May 2, 2025;
<https://theannapurnaexpress.com/story/54009/>
- ²⁹ Section 47, Electronic Transaction Act, 2008.
- ³⁰ Based on consultation with experts.
- ³¹ Digital Rights Nepal, The State of Digital Rights in Nepal 2024. <https://digitalrightsnepal.org>
- ³² Ibid.
- ³³ Id.
- ³⁴ Id.
- ³⁵ Id.
- ³⁶ <https://newbusinessage.com/article/sc-orders-nepal-telecom-not-to-allow-unauthorized-access-to-personal-information> ; Digital Rights Weekly, September 10, 2024
- ³⁷ Digital Rights Weekly, September 10, 2024; <https://digitalrightsnepal.org/newsletter/digital-rights-weekly-year-4-issue-02/>
- ³⁸ Based on DRAG's consultation meeting with experts.
- ³⁹ Finding from the consultation meeting with rights activists and experts organized by DRAG in Kathmandu in June 2025.
- ⁴⁰ My Republica, February 24, 2023, <https://myrepublica.nagariknetwork.com/news/kmc-allocates-rs-169-million-to-install-cctv-cameras-in-all-major-thoroughfares-of-the-metropolis>
- ⁴¹ Digital Rights Weekly, Year 3 Issue 33, <https://digitalrightsnepal.org/newsletter/digital-rights-weekly-year-3-issue-33/>
- ⁴² <https://en.setopati.com/political/162789>
- ⁴³ <https://moha.gov.np/en/page/press-release>
- ⁴⁴ <https://en.setopati.com/political/162789>
- ⁴⁵ Ibid.
- ⁴⁶ <https://kathmandupost.com/national/2024/09/29/sidha-kura-found-guilty-of-contempt-of-court-jail-sentences-for-publisher-and-editor> September 29, 2024.
- ⁴⁷ Sidhakura Content Is Prima Facie A Bid To Defame Judiciary: Court;
<https://kathmandupost.com/national/2024/04/30/sidhakura-content-is-prima-facie-a-bid-to-defame-judiciary-court>
- ⁴⁸ <https://kathmandupost.com/national/2024/09/29/sidha-kura-found-guilty-of-contempt-of-court-jail-sentences-for-publisher-and-editor> September 29, 2024.
- ⁴⁹ Cybersecurity in Nepal: Addressing the Growing Digital Threats, <https://danphelink.com.np/blog/cyber-security-in-nepal> September 9, 2024.
- ⁵⁰ Krishna Verma, Nepal's Digital Frontier: How Safe Are We From Cyber Attacks? April 20, 2025.
<https://myrepublica.nagariknetwork.com/news/nepals-digital-frontier-how-safe-are-we-from-cyber-attacks-14-86.html#:~:text=Nepal's%20vulnerabilities%20are%20brought%20to,rendered%201%2C500%20government%20websites%20inoperable.>
- ⁵¹ Passport Service Halted Indefinitely, Online Khabar, November 22, 2024.
<https://english.onlinekhabar.com/passport-distribution-halted-indefinitely.html>
- ⁵² Tribhuvan University Faces Challenges with Online Services Implementation, February 8, 2024,
<https://edusanjal.com/news/tribhuvan-university-faces-challenges-with-online-services-implementation/>
<https://www.techpana.com/2024/147675/national-vigilance-center-website-hacked-data-lost>
- ⁵³ <https://www.techpana.com/2024/147675/national-vigilance-center-website-hacked-data-lost>
- ⁵⁴ Passport Service Halted Indefinitely, Online Khabar, November 22, 2024.
<https://english.onlinekhabar.com/passport-distribution-halted-indefinitely.html>
- ⁵⁵ The State of Digital Rights in Nepal, 2024. <https://digitalrightsnepal.org/wp-content/uploads/2025/05/STATE-OF-DIGITAL-RIGHTS-AND-SAFETY-IN-NEPAL-2024-1-1-2.pdf>
- ⁵⁶ Ibid.

-
- ⁵⁷ The National Census of Nepal, 2021.
- ⁵⁸ Mahabir Pun, Bridging the Digital Divide: The Case of Nepal Wireless, UN Asian and Pacific Training Centre for Information and Communication Technology for Development. <https://www.unapcict.org>
- ⁵⁹ Based on consultation meetings with experts.
- ⁶⁰ Meta Ignores Deadlines, Nepal Undecided. <https://kathmandupost.com/national/2025/05/05/meta-ignores-deadline-nepal-undecided>
- ⁶¹ Dipesh Kumar K.C., Cross-border Crime and Its Security Concern In Nepal, <https://www.nepjol.info/index.php/JAPFCSC/article/download/26729/22130/79923>
- ⁶² Singers Push Back Against Online Abuse, Harassment, <https://risingnepaldaily.com/news/65002>
- ⁶³ <https://idsn.org/un-minority-forum-dalit-activists-call-for-action-on-caste-hate-speech-political-inclusion-and-intersectional-discrimination/>
- ⁶⁴ Nepal's Digital Generation: Challenges and Solutions For Child Online Protection: A Situation Paper, 2024. <https://www.unicef.org/nepal/media/24131/file/Final%20Situation%20paper%20ai.pdf>