Status of Digital Rights in Nepal; A Review

Media Monitoring Report 2023

Body & Data

STATUS OF DIGITAL RIGHTS IN NEPAL; A REVIEW

Body & Data, 2024
Writer: Vivek Baranwal
Editor: Vivek Baranwal, Nabina Gyawali
and Nuva Rai
Layout: Nuva Rai

Publication: Body & Data
Support: Vision for Change

https://bodyanddata.org/

@bodyanddata

BRIEF REPORT ON THE STATUS OF DIGITAL RIGHTS IN NEPAL

This annual report reviews the content — particularly topics, messages and trends related to digital rights — that the Nepali media covers. Beginning in 2021, the objective of subsequent annual reports has been to inspire a discussion and debate on the content as in how media encodes and analyses events concerning our human rights on the internet and the digital spaces.

In this Annual Media Monitoring Review Report 2023, we present our analysis based on news reported in the media outlets per Schedule 1 by applying the method per Schedule 2.

1. EXPERIENCE AND SITUATION OF OUR GOVERNMENT DIGITAL SPACE

The government is seemingly moving towards digitising government services under the 'Digital Nepal' campaign. However, the government efforts seem careless and overly imposed rather than being user-friendly and for the users' interests. The country celebrated the Sixth National Information and Communication Technology Day (ICT Day) with the slogan 'Surakshit Suchana Prabidhi, Sushasan ra Samriddhi' which translates to 'Safe Information Technology for Good Governance and Prosperity'.

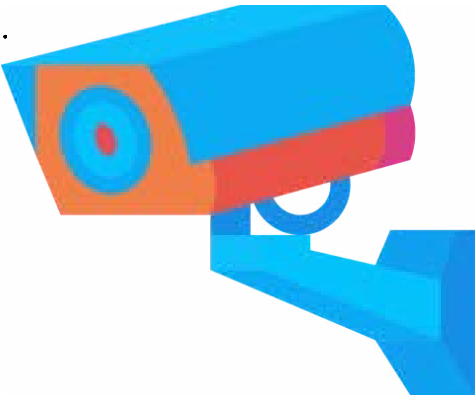
1.1. ATTACKS IN CYBERSPACE

Nepali cyberspace, especially the government servers, faced attacks at the beginning of the year — taking down at least 400 sites for five hours, including the Immigration Office which affected international flights. The Prime Minister's Office's X (formerly Twitter) account was also hacked. It was learnt that the government data centre lost data without backup. Hackers, by publishing site codes, further threatened to take down more government and news media websites. Travel companies also faced the brunt as foreign travel tickets worth millions of rupees were issued by hackers. This raises serious doubts about the government's cyber security policy. According to the Ministry of Communication and Information Technology, Nepal is among the most cyber attacks prone countries. The government server also contains personal details of citizens and sensitive national documents. Notably, the attack was no surprise but speculated in a Ministry of Home Affairs report the previous year. However, the government does not seem to prioritise cyber security.

1.2. FAILED ATTEMPTS TO CURTAIL THE RIGHT TO INFORMATION AND INJUNCTIVE ATTEMPTS AT CITIZEN SURVEILLANCE

The government decided to keep 87 types of information confidential. Following widespread criticism in social media and news media, the government stepped back from the decision, which was taken forward by exploiting some loopholes in the Right to Information Act 2007. It can be understood that the state intended to curtail citizens' right to information. Another incident — In the Gaushala 26 v. Sandeep Lamichhane case, the Patan High Court ordered 'lawful interception' to monitor the accused Lamichhane for investigation. But no such provision exists in any of Nepal's laws. Under the interception, whether voice calls can also be intercepted or not was not explained. Perhaps, the investigating agency was given the prerogative of 'lawful interception' — to use as they want. This order of the court is understood to be given to help conduct an effective investigation into sexual violence against minors intending to deliver justice to the victim.

However, this order should have set a precedent in the future for the state or its organs to whimsically monitor citizens. On the other hand, this incident has encouraged the government to give such interception a full legal form through the Telecommunications Bill 2023. In the said bill, a provision was found to propose to "reveal the identity of any person, including the recording of conversations, and obtain other service-related details from the service provider for investigation." Similarly, it was found that the Nepal Telecommunications Authority has put pressure on the telecommunication service providers to immediately implement Teramocs technology for collecting personal information such as call details and SMS. In this way, we must be alert and cautious that misuse of such technology will add challenges to the protection of personal privacy.



In August, the government tried to practice controlled internet in Nepal through the National Cyber Security Policy. Although this policy is expected to play an important role in setting the legal and structural basis of cyber security, the government has seemingly included a brand new theme — the creation of a National Internet Gateway — that was not included in the draft and was not discussed with the stakeholders. Only in countries with autocratic regimes have all internet traffic routed through government gateways. Through such gateway, the state monitors the internet traffic, controls the online content and even imposes censorship. The policy under the strategy of creating a safe online space by continuous monitoring for cyber security has taken a prohibitive and control-oriented approach. It emphasises continuous monitoring of citizen behaviour on the Internet and cyberspace, and poses restrictions rather than regulation of online space. As a result, freedom of expression may be unnecessarily restricted. Through this policy, the government will create its gateway/firewall like China, and the possibility of controlling the Internet according to its own will be high. (Translation of Digital Rights Nepal statement on Internet Gateway, 2023)

1.3. DIGITISATION: QUESTIONS LOOMING OVER ONLINE GOVERNMENT SERVICES

Year after year, the government has been introducing new technology to expand the state services provided to the citizens digitally. For example, the national identity card (NID) was moved forward as a citizen’s integrated identity card, as an alternative to the use of citizenship — where all the details including biometrics to driver’s licence, educational certificate, passport, mobile number, health information and so on would be linked. This is yet to happen, but questions have been raised about the technology since its inception. However, it has been pushed forward ignoring the right to data security and personal privacy. The annual report of the Auditor General of the government has also raised subsequent questions. Nonetheless, the government launched an app called ‘Mero Poshan Saathi’, which asks to keep a record of biometrics and other health-related details with the aim to digitise health services. Registering health information in the government data system through this app however appears risky.

1.3.1. AUDITOR GENERAL'S COMMENT ON NATIONAL IDENTITY CARD, AND OTHERS

The Auditor General's 60th annual report questioned the utility of the National Identity Card as well as the entire technology of the online services provided by the government saying that nothing could be included/linked except the details of citizenship. Another example, the traffic police did not accept the license on the Nagarik App rather they looked for a physical copy. Government silos create a burden on users. Security concerns around unauthorized access to personal information already make the Nagarik App risky. Without clear benefits, the app's purpose becomes questionable, discouraging citizen adoption. On the other hand, technology has changed the way states operate. The government agencies have accumulated their data in different databases of their own. Uploading errors can lead to inconsistencies in personal details within the system, hindering cross-verification. The digital shift must address equitable access for different sections and social classes within society, including both users and system operators.

For example:
A woman who came to Kathmandu from Baglung to correct the details of her passport was reported to the police by the passport department because the appointment date on the application form and the date given per the department's database record did not match.

Also, how does the government database accommodate marginalised people and community (for example: Musahar) who are by principle citizens but do not have access to citizenship and are in a state of statelessness; The system's accessibility for Persons with Disabilities and queer individuals need to be addressed, particularly for those who cannot obtain citizenship documents reflecting their identity. Concerns regarding data security of the Nagarik App and National Identity Card (NID) persist. The issue of state surveillance through these apps and cards remains unresolved. The question of the state monitoring its citizens through such apps and electronic cards remains as unanswered.

1.3.2. REGISTERING HEALTH INFORMATION IN GOVERNMENT DATA SYSTEMS RISKY

The government launched an official app 'Mero Poshan Saathi' which supposedly helps in the health and care of pregnant women, children, teenagers and elderly. In the Nepali language-based app, the user has to enter their identity details such as name, phone or email, location, and health-related information such as pregnancy or child's weight, diet, age and so on. This app provides information about essential health behaviours and recommendations accordingly. Although it is said to be brought for the convenience of the people, the data security of the users remains at risk with the government. There have been incidents of cyber-attacks and data theft in government data centres. Digital services released by the government (such as Nagarik App, national identity card, smart driver's licence) have been at risk in terms of cyber security, personal information, and privacy. In the meantime, if health-related information is also collected in the government data system, it will enable state monitoring of safe abortion under SRHR (Sexual Reproductive Health Rights). Women and individuals who can get pregnant may be more at risk. The state machinery as a whole is not generous towards women and people of gender and sexual diversity. They become more marginalised by those who occupy the power and sit in the state system. In conclusion, such digital services can become a monitoring tool for the state.

1.4. DIGITAL BUDGET

In the national budget, the Digital Nepal Framework was said to be revised, the government financial system to be interconnected, while the work would be carried out in two shifts for the distribution of national identity cards, driving licences and passports, and Permanent Account Number (PAN) would be linked to the national identity card. Although it is worthwhile for the government to emphasise the digitisation of government services through this budget, the government did not seem concerned about personal data security policy, privacy, and protection from cyber-attacks.

Further, there was a plan to abolish the National Information Technology Center, which handles government servers, and move the management and operations of the servers under the Department of Information Technology. Likewise, Nepalis living abroad were promised that they could exercise voting rights from their place of residence. The Election Commission has publicly kept the list of voters on the website and in such a way that personal details can be extracted. Thus, it seems natural to question how confidential and secure the voter list of Nepalis living abroad would be. Although the government was set to fully implement MDMS this year, the technology procurement process faced corruption charges due to which its implementation has been put on a halt.

2. Our Right to Privacy

Many incidents of personal privacy violations were reported throughout the year. Most of these incidents appeared as identity theft.

2.1. Unauthorized but Easy Access to Personal Details

A police investigation shows that by making unauthorised access to the personal information of the users, SIM cards are issued in their names and used in organised criminal activities ranging from digital scams to murder and other activities criminalised by the laws of Nepal. For example: It was found that SIM cards were issued by misusing copy of citizenship or any valid government ID shared by email for printing, photocopying, form filling or any other specific purpose. The government is not serious about the privacy of citizens/service users which can be infered from the fact that sensitive data such as citizenship numbers was published on the Facebook page of the federal Department of Transport Management when the result of the driver's licence examination was published. In this case, the privacy provisions mentioned in the Privacy Act (2018) have been openly violated. After obtaining citizenship from the site, one can find the voter card, serial number, and date of birth respectively by placing the details on the website of the Election Commission. In both of these cases, breaching the privacy of personal information and using that information for purposes other than what is a serious issue. The IT Policy *2015), the Privacy Act (2018), the

Privacy Regulations (2020), the Advertisement (Regulation) Act (2019) etc. have given instructions to some extent regarding the safe management of highly personal electronic details of individuals. The Privacy Act classifies telephone numbers, email addresses, fingerprints, citizenship certificates, etc. as personal information. In addition, it is mentioned that such personal information collected for one purpose cannot be used for other purposes without the consent of the concerned person. Except for special cases, the law prohibits the use of such details without the required consent. However, the Privacy Act has not mentioned the necessary structure for regulation, monitoring and action for such non-compliance.

As a result, incidents related to SIM cards have been reported. For example: During the Football World Cup held in December 2022, photocopies of other people's citizenship and their photos taken from the internet were maliciously used to issue a new SIM card with the same number citing that the old SIM card was lost. Then, based on OTP, fraudsters would make unauthorised access to their bank, digital wallet and social media accounts, and the Nagarik App (which is unequivocally risky from the point of view of data privacy and security and may contain sensitive documents). This raises serious questions about the SIM card distribution system and reveals that the verification system of telecom service providers and digital wallets is weak or non-existent.

2.2. Irresponsibility of Government and Service Providers

Following the Pokhara plane crash, the Civil Aviation Authority of Nepal (CAAN) released a list of the plane's passengers with passport number, name, age, gender, contact person and nationality through their Twitter handle. Not only did it violate the right to privacy of the deceased, but it also caused unwanted attention and added mental stress to the family. This action of the authority invited widespread criticism in the social circle. Neither the organisation nor the government took any steps, implying that the authorities are not aware of or do not comply with privacy (related Act 2018). Moreover, misleading and fake materials were exchanged and broadcasted by manipulating various photos, audio, visuals, and personal details of the deceased (especially the pilot and co-pilot) in the media from social networks. Outright patriarchy dominated the news about co-pilot

Anju Khatiwada. In social media content and media reporting, Khatiwada was portrayed not as a professional pilot but as "someone's daughter, someone's wife, someone's mother" followed by "an unfulfilled husband's dream and married life." The independent identity of Khatiwada has directly been rejected.

Similarly, an unauthorized fundraising campaign emerged online, urging support for Prem Acharya's family through his wife Nanuka Adhikari's bank account. Adhikari found out about it only when screenshots of her bank account details and along with the amount received as assistance began going viral on social media. Adhikari never authorized the social media post with her bank details, which went viral and caused her privacy to be breached. This incident highlights both the spread of misinformation online and potential weaknesses in banking security.

2.3. Data Theft by Phishing

In February, a digital fraud gang was busted for staging frauds via an app called 'Nepali Keti' claiming to find sex partner. It was found that they would send the link to this app on WhatsApp for downloading. After the user installed it, the fraudsters would make unauthorised access to the bank details saved on the mobile phone. Then they would transfer the money to their bank account via digital wallets like e-Sewa and Khalti, and withdraw the amount from their ATM card. This incident reveals that our banking and digital wallet security systems are not secure and that the companies should be held accountable and responsible.

In March, a Google Drive link was shared from the official Facebook page of news portal Online Khabar claiming "hot footage" of Actress Swastima Khadka. Online Khabar removed the post and apologised saying that 'third party' access has been removed from the page. It was suspected that one of the devices used to access the page was hacked. A few days later, the same drive link (and other links too) was shared from a fake Facebook page called Online Khabar in English with the name and photo of Actress Khadka. According to analysts, there might be malware in that link which gets downloaded when the link is opened and stores itself in the browser used to open the link. The malware was spread to steal browser history, saved passwords and other information.

2.4. India's Aadhaar Card Data Leak and Nepal's National Identity Card

Despite differences in registration procedures and legal frameworks, both India's Aadhaar card and Nepal's National Identity Card aim to be multipurpose digital IDs for accessing public and private sector services. These cards typically contain basic information like name, date of birth, address, and phone number. Additionally, some may offer linkages to other documents like driver's licenses, tax identification numbers (PAN), passports, and even family details or health information. In October, data of more than 815 million Indian Aadhaar cardholders leaked online. It contained personal information such as Aadhaar card and passport details, name, phone number, and address. Biometrics are also included in the Aadhaar card.

The details collected by the digital identity cards of both countries are stored in a central database. Aadhaar card, which has been in operation for the past 13 years, the data security infrastructure appeared weak. The same risk applies to Nepal's National Identity Card which started with low infrastructure and chaotic preparation. A study by Body and Data (p.20) says that users may not understand terms like digital privacy or biometrics, although they understand the dangers of sharing confidential information and data breaches (leaks). The work of collecting data from various government agencies at the local level is ongoing and often the same type of personal information has also been collected over and over again. It is the practice of the government to collect more data than necessary so that it can often be used in the future. It has been speculated that this is the global level of the mass digitisation program, ignoring data reduction or proportionality. In the absence of user-friendly data protection laws, and the government's sluggishness to make them or based on those laws that can be defined according to their own preferences, there is a strong possibility that such digital ID cards will become a state surveillance tool over time.

2.5. Government Contemplation of User Privacy

In April, Italy imposed a temporary ban on ChatGPT for violating European data protection rules, citing privacy concerns. Italy's ChatGPT ban ended in May after an agreement was reached. This is an example where a country advocated for the protection of its citizens’ data using data protection and privacy laws. A lawsuit filed in California in June accuses OpenAI, the creator of ChatGPT, of scraping a vast amount of user data from the internet. The rise of tech giants has been accompanied by growing concerns about user privacy and data security. While technological advancement is inevitable, it shouldn't come at the expense of our digital well-being. We need to find ways to ensure innovation happens alongside robust data protection for individuals. In our country presently and in the days to come, AI technology and other technologies will be entering our lives. In preparation for that situation, a question must be asked — when will our country be able to negotiate and advocate with the tech giants for the data security and privacy of its citizens as Italy did?

3. Status of Freedom of Expression

Content-sharing platform TikTok faced restrictions worldwide throughout the year, with Nepal garnering significant public attention when the government imposed a ban later in the year. The ban sparked debate around two key issues: freedom of expression, as critics argued it stifled online discussions and impacted content creators, and geopolitics, considering the app's Chinese ownership.

Similarly, a media story blurred the lines between sex work and forced prostitution. While the story seemed to criminalize the actions of a few TikTok users offering sex services, their accounts and the police's statement helped clarify the distinction. This story importantly amplifies the message that engaging in consensual sexual activity for money is sex work, while anything without consent is sexual exploitation.

3.1. TikTok ban in Nepal and Worldview

The Nepalese government's decision to ban TikTok has severely restricted users' freedom of expression on this widely used social network. This move comes despite government claims in official statements that TikTok disrupts "social harmony" and "national unity" by allowing "inappropriate" content. The ban disproportionately affects marginalized communities who already struggle for voice on mainstream platforms. These groups relied heavily on TikTok for self-expression and connection. It further marginalizes them and limits their participation in public discourse. The government must consider this impact and ensure their right to free speech.

This also highlights the need for a more balanced approach to regulating platforms like TikTok. A blanket ban based on subjective claims of "inappropriate" content isn't effective. Instead, collaboration with TikTok, like Italy's approach, could create user-friendly moderation policies that protect Nepali users' right to free expression. Nepal's TikTok ban exemplifies how governments grapple with social media challenges.

While regulation is crucial to curb misinformation and hate speech, it shouldn't infringe on citizens' fundamental rights.

On the other hand, discussions in the West often portray TikTok, owned by a Chinese company, as a state surveillance tool. The debate focuses on national and international cybersecurity and data security, with some fearing laws and policies that could keep citizens under state control. The TikTok controversy in the United States exemplifies these concerns. It raised questions about whether TikTok (and potentially other tech giants like Google) have been providing user data to governments for surveillance purposes.

TikTok's CEO admitted to sharing user information with China, prompting the US to threaten a ban unless the app's ownership is sold, likely to a US company. This move not only targets TikTok, but also sends shivers down the spines of other social platforms that facilitate user expression. These platforms now fear a similar fate if deemed a national security risk due to their ownership structure.

For example:France's decision to ban TikTok, while considering bans on Netflix, Twitter, and even Candy Crush, raises concerns for Nepal's digital space. Is a ban truly the only answer? User-friendly regulations could be a more effective solution. Banning platforms like TikTok hurts creators who lose their space for expression and exploration. The brunt falls hardest on underprivileged individuals and communities who already lack platforms for their voices due to political, social, and economic barriers.

3.2. Month of June: Pride Month celebration

June is Pride Month, a time for People of Marginalized Sexual Orientations, Gender Identities, and Sexual Characteristics (PoMSOGISEC) to celebrate their existence and demand equal rights from society, government, and institutions. It's a movement built on years of claiming space and demanding fair treatment. During Pride Month, PoMSOGISEC and their allies come together to express themselves, discuss their challenges, and celebrate their identities. However, Nepali media has largely missed this opportunity. While a handful of outlets published one or two articles and parade photos, a significant number offered minimal to no coverage.

Even the existing coverage often fails to grasp the complexities of gender and sexuality, leading to misrepresentation and misleading narratives. This exposes the irresponsibility and ignorance of a large portion of Nepali media.

3.3. Sex work's narrative

On April 5th, 2023, The Kathmandu Post reported on the use of TikTok's live feature to attract clients for sex work. The report framed these services provided under the guise of spas and massage therapists as morally wrong, fearing a "negative" influence on youth and calling for closure. However, the law differentiates between forced prostitution (illegal) and sex work (unregulated). Quotes from police and spa operators highlight this legal distinction. Our society often conflates the two, failing to acknowledge consensual sex work as a valid career choice.

This incident on TikTok actually represents a growing voice within the sex work community. With regulation lacking, risks associated with sex work worsen. Therefore, the state should consider regulating sex work, recognizing it as a profession. This would offer legal protections and vital health services like free STD testing and treatment.

4. प्रविधिमा आधारित हिंसा

The digital space has become a breeding ground for violence against women. Take the Gaushala 26 v. Sandeep Lamichhane case, where social media plumbed new depths with its response to such sensitive charges as statutory rape. Similarly, artist Kunjana Ghimire (Suntali) being sent unsolicited nude photos and verbal abuse highlights the issue.

Even when fueled by disagreement and rage, as with the online vitriol Suntali faced during the Bharatpur cricket stadium controversy, online violence against women often takes a sexualized turn. This is further evidenced by the spread of malware disguised as "secret videos" of actress Nisha Adhikari, with a similar incident targeting Swastima Khadka according to Body & Data's recent findings.

4.1. Gaushala 26 v. Sandeep Lamichhane

A Kantipur interview with rape survivor Gaushala sparked outrage, going viral from social media to everyday conversations. She bravely shared her story, but was met with vicious online attacks attempting to discredit her. Public responses on social media overwhelmingly favored the accused, Sandeep Lamichhane. This highlights two issues:

1. Entrenched Patriarchy: Social media acts as a breeding ground for patriarchal views, making it a prime example of its rise.
2. Desensitized Society: Public reactions expose a society fueled by hero worship, quick to react without considering the facts, and ultimately, desensitized to the plight of the victim.

The situation worsened when the Supreme Court lifted Lamichhane's travel ban while tge Cricket Association of Nepal (CAN) had already lifted his ban and had allowed him back on the national team. Public arguments swirled around why his life shouldn't be on hold while accusations were pending. Yet, no one seemed concerned about Gaushala's well-being, neither the public nor the state. The biggest blow came when the Prime Minister himself felicitated Lamichhane, while the government, contradictorily, continued its case against him in court. This state-sanctioned whitewashing of the accused, while attacking the victim's courage, has deeply disappointed Nepal's women. The state must adopt a zero-tolerance policy for sensitive cases like rape. The Supreme Court's decision further exposes the deep roots of patriarchy that have infiltrated various state organs and institutions.

4.2. Definition of Rape (?)

An audio clip purporting to involve MPs Aarju Rana Deuba and Manju Devi Khand in the fake Bhutanese refugee scandal quickly became the talk of the town. MP Rana responded by filing a complaint with the Cyber Bureau, highlighting the malicious intent behind the doctored audio. In Parliament, Rana stated that this incident constituted "character rape."

This incident exposes the subjective nature of rape, extending beyond physical assault. While the fake refugee claims sparked public outrage against the politicians, it also reveals a troubling trend - the character assassination of female parliamentarians. While accountability for political figures is crucial, targeting someone's character solely because of their gender is a clear form of online violence against women.

4.3. Police data

Police data paints a grim picture: online violence against women and girls is surging. Reported incidents more than doubled from 2,389 in FY 2021/22 to a staggering 4,590 in FY 2022/23. The trend continues in the current year, with 3,309 cases already reported in just the first five months (FY 2023/24). Investigations reveal adult men as the primary perpetrators, though teenagers account for roughly 15% of these crimes.

Analyzing complaints filed over the past five years (584 total), a disturbing trend emerges: 77.4% of teenage victims are subjected to digital sexual exploitation, violence, and abuse.

The nature of abuse differs between teenage boys and girls. Boys primarily report online harassment and intimidation while playing games. Girls, however, are targeted with a calculated approach. Perpetrators often befriend them online, gaining trust with gifts and flattery before resorting to deception, threats, and attempts to coerce them into sexual activity.

Victims are further traumatized by being exposed to obscene content and having their private photos and videos shared maliciously.

However, the mainstream narrative often blames entire digital platforms for the violence that occurs on them. We must remember, the digital world has transcended mere social media habits – it's become an extension of our daily lives. Just like the physical world, the digital space reflects our society – the online sphere is no different than the one outside our phones. Demonizing these platforms ultimately throttles the freedom of expression for users, especially those most vulnerable, like women in this context.

Discussions about digital rights are crucial, as they are essentially human rights in the online world. Data from police and concerned agencies should guide policy formulation and implementation to create a safer digital space. This is far more effective than demonizing and banning platforms like TikTok.

5. Month of March: Women's History Month

March is Women's History Month, culminating on International Women's Day (March 8th). This year's theme, "DigitALL: Innovation and Technology for Gender Equality," highlighted two key issues: the low participation of women in tech and scientific research, and the digital divide. For instance, during a program called "Women in Information Technology," MP Sumana Shrestha revealed that despite 81% of Nepali women being economically active, only 0.5% work in these fields. Gender discrimination appears to be a major barrier, as women are often denied opportunities.

The digital divide further exacerbates this inequality. According to 2022 data from the International Telecommunication Union (ITU), a global gender gap exists in internet access: 62% of men use the internet compared to 57% of women. Notably, women and teenagers make up the majority of the estimated 2.7 billion people without internet access. In Nepal, a less developed country, only 19% of women use the internet. This gap extends to social media usage. Data shows that 56.4% of Nepal's 1.26 million social media users are men, while women comprise only 43.6%. A UN Women report adds another layer. A study of 133 artificial intelligence systems worldwide found that over 44% exhibited gender bias. Additionally, a survey of women journalists in 125 countries revealed that more than 70% have faced online violence. On the other hand, according to the number of single mothers reported in the new census, it appears that 1.7 million people have been deprived of citizenship due to the inability to obtain it through their mother's name. Policy discussions are emerging to address these issues and online violence against women in general. Continuous advocacy is crucial for progress.

6. Conclusion

Body & Data utilizes this review report to analyze the intersection of technology, human rights, and digital rights within the Nepali context. The report aims to assess the current state of these issues and provide a platform for discussion. The following are the major trends and conclusions we have found regarding digital rights through Nepali media:

- SIM card verification and digital wallet verification systems should be strengthened since it is easy to re-issue a SIM card of the same number by identity theft and gain unauthorised access to the bank and digital wallet.

- Beyond dedicated months like Women's History Month and Pride Month, media reporting can be a powerful tool for inclusivity. By actively learning, unlearning, and relearning reporting techniques, journalists can effectively bring the stories of marginalized communities to the forefront.

- We must move away from demonising digital platforms (social networks) as the sole culprits for online incidents. Instead, let's focus on creating a user-friendly regulatory body that prioritises both privacy and freedom of expression. This body should regulate the internet, not control it.

- Stakeholders should organize and create a discourse to challenge the government's efforts to monitor citizens through cybersecurity policies and telecommunications-related bills.

- Expanding online government services must prioritize accessibility for marginalized communities, minorities, and People with Disabilities (PWDs). This includes incorporating features like, facilitating ALT Text, Voiceover or Talk Back technology for visually impaired people.

Schedule 1 – Media that were monitored for this report

Techpana, Ratopati, Desh Sanchar, Kantipur, Gorkhapatra, ICT Samachar, Kharibot, News 24, Nepal Live, Rajdhani Daily, Nagarik Daily, Himal Khabar, Image Khabar, Online Khabar, BBC News Nepal, Setopati, Makalu Khabar, Kathmandu Press, Shilapatra, Ujyalo Online, Nayapatrika, Thaha Khabar, Baahrakhari, The Rising Nepal, My Republica, The Himalayan Times, Khabar Hub, Nepal Khabar Patrika, The Kathmandu Post

Schedule 2 – Study Methodology

This report analysed the state of digital rights news in Nepal throughout the year of 2023. We conducted a comprehensive media monitoring review, compiling, studying, and analyzing news and discussions related to digital media, internet, technology, and related topics published by mainstream online media outlets.

Building on our previous work of publishing and disseminating quarterly brief reports on 744 collected news items, this annual report presents a thematic analysis drawn from the quarterly reports and overall monitoring efforts. It is important to note that our analysis focuses on the qualitative aspects of the issues raised by the media, rather than simply the number of news items.

Note: This review report is our sole institutional initiative. Taking into account the possibility of mistakes, we request you to contact us via email communication@bodyanddata.org for your suggestions or feedback.

Thank you!