Navigating online media and controlling cybercrime & defamation in Nepal: A comparative perspective

◆ Dr. Shree Krishna Bhattarai[1]

Abstract:

Nepal's legislative frameworks are outdated in addressing the challenges posed by the rapid growth of digital media, including social networking and AI-generated content. This inadequacy hampers the nation's ability to combat cybercrime, defamation, and ensure accountability of digital platforms. A comparative analysis with international standards from the US, India, and the EU uncovers notable deficiencies. Key findings indicate that criminal defamation laws obstruct free expression without effectively deterring online harassment, and cybercrimes such as financial scams and deepfake propaganda proliferate due to a lack of targeted legislation. Additionally, inconsistencies are noted between Nepal's *Press Council Act (1992)* and *Electronic Transactions Act* (ETA, 2006) in regulating digital content, unlike the more effective measures implemented in the EU and India.

The article highlights that Nepal's laws are insufficient for managing data jurisdiction and protecting victims, particularly regarding AI-

1 Dr. Shree Krishna Bhattarai, a former judge, is a legal expert in Nepal and a PhD holder specializing in cyberlaw, cybercrime, and social media-related defamation. His extensive academic credentials include an MBA (USA), a postgraduate degree from Australia, a diploma from India, and multiple advanced degrees from Nepal (LLM, MPA, MA, BEd). He currently practices as a freelance lawyer.

generated content. It suggests reforms to balance press freedom with accountability, including a tiered regulatory model, the creation of cyber tribunals, and aligning defamation standards with the "actual malice" doctrine. Furthermore, it situates these challenges within South Asia's socio-legal context and calls for urgent updates to media legislation.

Keywords: *AI, algorithmic accountability, content moderation, cyber-enabled crime, data breach, deepfakes, digital constitutionalism, malinformation, collaboration, phishing, ransomware, SQL injection*

Introduction:

The 21st century has ushered in a significant digital revolution, altering how societies generate, utilize, and interact with information. In Nepal, the rapid adoption of digital platforms and social media brings to light critical ethical and legal challenges, particularly concerning cybercrime and online defamation. Existing legal frameworks, designed for traditional media, are proving inadequate for the dynamic and often anonymous nature of online communication. This article explores the complex "digital dilemma" facing Nepal's evolving judicial system.

This study explores the definitions and dynamics of online, digital, social, and new media from a Nepalese perspective, particularly focusing on the relationship between these media and increasing cybercrime issues. It differentiates between cyber-enabled crimes, facilitating traditional offenses like online harassment, and pure cybercrime that impacts media infrastructure. A critical examination of social media's role in such digital offenses, especially online defamation, will be undertaken. Furthermore, the research provides an in-depth look at Nepal's media laws relevant to the digital space, notably the *Electronic Transactions Act* (ETA), 2006, alongside constitutional press freedom provisions. A comparative analysis with major countries, including the US, UK, EU, and India, will contextualize Nepal's regulatory stance, revealing challenges in regulating social media and enforcing laws against online defamation within its unique context.

Strategic suggestions will focus on legal reforms, improving digital literacy, and developing institutional capacity to create a responsible and secure online media environment that safeguards public safety and freedom of expression.

Nepal's changing media environment: Delineations and mechanisms

The media landscape in Nepal has transformed from traditional forms to a technologically advanced environment, necessitating clear definitions of terms such as "digital," "online," and "social media" to understand the current dynamics of power, influence, and information in the country.

Online media: Online media refers to digital platforms that enable negotiable and interactive mass communication, including digital forms of traditional media and independent blogs (Online Media, 2016). In Nepal, the rise of online news websites has led to instant information access and a variety of perspectives.

Digital media: Digital media includes various content types such as audio, video, e-books, and interactive applications, focusing on format rather than delivery method (SCPD, 2025). It allows for instantaneous distribution, personalization, and interactivity, in contrast to analog media, which has limited distribution and delivery options.

Social media: Social media enables organizations to engage with the public and build community, significantly impacting social interactions and political discourse via platforms like Facebook, YouTube, TikTok, and X (Digital.gov, 2025). However, issues surrounding user-generated content present regulatory challenges, especially regarding privacy rights in civil cases. Legal reforms are essential to address these privacy concerns amidst the growing use of Internet evidence in legal settings.

New media: The term "new media" encompasses electronic communication tools like blogs, wikis, and social media that allow

user customization and interactivity (Uduak, 2021). In Nepal, increased mobile phone and Internet usage has fostered citizen journalism and user-generated content, moving from passive consumption to active engagement. This shift has democratized information, enhanced transparency, but also posed challenges to regulatory frameworks and facilitated the spread of hate speech and misinformation.

Nepal's legal framework governing the media:

Nepal's media law combines press statutes with constitutional free speech rights, posing difficulties for journalists and digital creators, further complicated by criminal and cyber laws that regulate online expression.

Constitutional guarantee: Nepal's media law combines press statutes with constitutional free speech rights, posing difficulties for journalists and digital creators, further complicated by criminal and cyber laws that regulate online expression. (*Constitution of Nepal*, 2015, art. 17)).

Key legislations: *The Press and Publication Act* (1992), *National Broadcasting Act* (1993), and *Working Journalists Act* (1995) regulate Nepal's media. The controversial *Online Media Operation Directives* (2017) introduced restrictive measures (DoIB, Nepal, 2016). The government is working on a single integrated mass media legislation, with a draft available for stakeholder debate, aiming to transform state-owned broadcasters into Public Service Broadcasting. Community radio currently follows the same laws as commercial radio, with no distinct regulations. The Supreme Court plays a crucial role in media freedom.

The Press and Publication Act: The Act established a government registry for media firms and set the foundation for subsequent media laws in Nepal, which include regulations on acceptable speech and penalties (PPA, 1991). However, the Act's focus on traditional print media renders it ineffective in addressing the rapid and global nature of online information dissemination, highlighting its inadequacies in the current digital landscape.

National Broadcasting Act: Traditional radio and television transmission is regulated by the Act, which establishes content requirements and licensing protocols that empower the government to suspend or revoke licenses for violations of content rules, including broadcasting offensive or libelous material (NBA, 1993, § 7).

Working Journalist's Act: The Act outlines the rights and obligations of journalists, ensuring job stability and fair pay, and providing the right to unionize and engage in collective bargaining while upholding ethical standards (WJA, 1995). However, it only applies to formally hired journalists, excluding non-journalists in online media, and does not address issues like misinformation on social media, indicating a gap in the media landscape.

Electronic Transactions Act: Despite not being a specific media law, this Act is crucial for digital content and online media. However, it is frequently misused to prohibit online information, raising concerns that its vague terms could be misused to suppress online expression, especially in journalism (ETA, 2006, § 47).

The Media Council Bill: The Bill aims for compulsory registration, code enforcement, and complaint resolution (National Assembly, 2080). Critics argue it allows for censorship and threatens press freedom (MCB, 2080, § 9).

Cutting-edge steps and challenges:

Nepal's government introduced the *Digital Nepal Framework* in 2019, aiming to achieve digital transformation through 80 initiatives across eight sectors, focusing on capacity building, infrastructure, and legal reforms (MoCIT, Nepal, 2023). The goal is to enhance public services, productivity, innovation, and inclusivity. However, the lack of comprehensive cyber laws regulating online content and intermediary liability poses significant challenges to advancing e-governance while protecting constitutional rights.

Node between online media and cybercrime:

Online media facilitates crimes such as fraud, radicalization, and cyber-trafficking, while also being subjected to cybercrimes like

hacking and disinformation campaigns (Morgan, 2021). This relationship complicates regulation, increases pressure on law enforcement, and threatens public safety and press freedom, highlighting the need for adaptable legal and technological solutions.

Pure cybercrime targeting media: Hacks are directly targeting digital infrastructure, news websites, and media platforms, categorizing these actions as direct cybercrime:

Defacement and hacking of websites: Malicious actors, including hacktivists[2] and cybercriminals, are increasingly assaulting news portals and digital media via tactics such as phishing, SQLI[3], and DDoS attacks (Bhattarai, 2024). These intrusions jeopardize press freedom, editorial integrity, and public trust, resulting in website defacement, service disruptions, and the theft of private source data (DefendDefenders, 2025). There is an urgent demand for robust cybersecurity measures, encrypted communication tools, and legal frameworks recognizing digital journalism as critical infrastructure to protect democratic discourse and whistleblower confidentiality.

DDoS[4] attacks: DoS[5] or DDoS attacks flood the web with traffic, making critical resources unavailable, particularly targeting media websites (DHS-STD, 2025). This digital censorship, termed "JIT blocking[6]," restricts public access to essential news and undermines investigative journalism, thus eroding confidence in media organizations. To mitigate these attacks, advanced DDoS mitigation

2 Hacktivist is a person who obtains illegal access to computer networks or files for social or political purposes.

3 SQL injection is a popular attack method that manipulates backend databases using malicious SQL code to get access to private consumer information, user lists, and sensitive data.

4 Distributed Denial-of-Service

5 Denial-of -Service

6 Just-in-time blocking is a governmental practice that temporarily restricts Internet access in specific regions to control information flow, prevent communication, and suppress dissent, often during elections or political unrest.

services, strong cyber-resilience strategies, and legal recognition of these crimes are essential.

Breach of data and surveillance: Platforms face significant risks from APTs[7] cyber-espionage and malicious actors (Citron & Wittes, 2017). This data theft endangers institutional security and democratic processes, compromising the identities of whistleblowers and journalists (NIST, 2018). The resulting digital surveillance poses a threat to press freedom and public knowledge, highlighting the urgent need for robust cyber-hygiene protocols.

Malware and ransomware: Ransomware attacks target cites, risking sensitive data and undermining press integrity (Sophos, 2025). These attacks disrupt news production, demand ransoms, and threaten private journalistic information. To safeguard, urgent cyberlaw is needed with the latest provisions of digital assets, clear criminalization of cyber coercion against media, and increased penalties for attacks that compromise information integrity.

Online media as a tool for cyber-enabled crime: Social media has become a significant facilitator of cyber-enabled crimes, including extortion, fraud, and theft (AAG IT Services, 2025). Criminals, particularly traffickers, exploit these platforms to recruit and communicate with vulnerable individuals through encrypted messaging, private chats, video calls, and fake accounts. This trend has contributed to an increase in human trafficking, complicating detection efforts (UNODC, 2023).

Spread of misinformation, disinformation and malinformation: Social media facilitates the rapid spread of misleading information, whether unintentionally (misinformation), intentionally (disinformation), or through the contextual misuse of accurate information (malinformation) (Wardle & Derakhshan, 2017). These

7 Advanced Persistent Threats (APTs) are sophisticated cyberattacks aimed at achieving long-term goals, usually executed by state-sponsored actors or skilled organizations to maintain unauthorized access to a target's network over prolonged periods.

tactics are often employed to manipulate political landscapes, incite social unrest, or damage reputations, potentially triggering crimes such as defamation and incitement to violence, despite not always qualifying as direct cybercrime.

Concept	Journalist's Action	Outcome & Harm
Disinformation	In a news setting, a journalist uncritically reproduces the false claims of a blog post, presenting them as a legitimate alternative viewpoint, without fact-checking or including expert rebuttals.	A journalist spreads a known lie, potentially due to pressure or bias, which undermines public health and represents a failure of journalistic responsibility.
Misinformation	A reporter, believing a popular blog post may contain truth, produces a "breaking news" story about a disturbing claim to alert the public rather than mislead them.	The reporter unintentionally disseminates false information, resulting in significant harm, despite the absence of malicious intent. This reflects a flawed professional decision.
Malinformation	Internal emails from an alternative medicine group reveal intentional falsification of a microchip claim. Despite the publication of these emails, the journalist suggests that the presence of doubt could imply potential dangers associated with vaccines.	In an attempt to sensationalize the narrative, the writer misrepresents actual emails, reflecting a deliberate and unethical choice to provoke a response or cause harm.

Harassment and cyberstalking of journalists: Online abuse and threats towards journalists covering sensitive topics are rising on social media, involving intimidation, hate campaigns, and doxing to obstruct critical reporting (Media Defence, 2024).

Online fraud and scams: Social media platforms are increasingly used for online fraud, as scammers exploit public trust through methods such as phishing. They impersonate legitimate organizations to steal personal information and commit financial fraud by creating fake opportunities (Cropink, 2025). Identity theft is also common, with offenders extracting data from public profiles for fraudulent purposes.

Incitement to hate speech: Hate speech aimed at specific groups spreads quickly online, promoting prejudice and violence. Legal frameworks find it challenging to address the extensive content and jurisdictional complexities, compounded by the varying content moderation practices of platforms that impede international enforcement (UNHRC, 2011, para. 10).

Comparative practices for media and cybercrime:

Countries are combating cybercrime by creating specialized laws, forming cyber police teams, developing digital forensic labs, and collaborating with ISPs, social media platforms, and financial institutions.

USA: The CFAA serves as the main federal law against hacking, while the 1st Amendment safeguards online expression (CFAA, 1986, § 1030). However, laws exist to combat cyberstalking and harassment (U.S. Const. art. I, § 8). Media organizations are particularly vulnerable to cybercrime, which threatens their sensitive information and intellectual property. An example of this is the 2014 Sony Pictures hack by a North Korean group, which exposed employee data, unreleased films, and inflicted serious damage through malware (FBI, 2014).

EU: The Cybercrime Directive standardizes anti-cybercrime laws among member states. In addition, the DSA[8] imposes significant obligations on online platforms concerning content moderation, transparency, and accountability for illegal content, such as hate speech and disinformation (Regulation (EU) 2022/2065, DSA).

8 Digital Services Act

India: A number of cybercrimes are prohibited under the ITA[9], which include regulations for intermediaries and content filtering (ITA, §§ 66, 67, 69, 79). Additionally, IT Rules, 2021 impose significant due diligence obligations on social media intermediaries, including prompt content removal and grievance redressal procedures (IT (Intermediary Guidelines and Digital Media Code) Rules, 2021, § 1).

Nepal: Nepal lacks a specific cyberlaw; the ETA 2006, is not precise in terms of intermediary liability and proactive content control (Bhattarai, 2024).

Online-defamation: Legal remedy

Defamation involves publishing false statements that damage an individual's reputation, and it poses distinct challenges in the digital age due to the fast, anonymous, and broad distribution of information, heightening risks of reputational harm. (Doe v. Cahill, 884 A.2d 451, 458 (Del. 2005)).

Nepalese scenario:

The Criminal Code, 2017 outlines defamation as consisting of libel (written) and slander (verbal), while online-defamation remains unregulated in Nepal. However, the ETA panelizes publishing certain contents on electronic media (ETA, 2006, § 47).

The primary factors that make online-defamation challenging are (Bhattarai, 2022):

- **Anonymity:** Finding and prosecuting criminals is difficult due to the ease of creating anonymous or pseudonymous profiles on social media.
- **Reachability:** Defamatory content can cause extensive and irreversible damage to a person's reputation, spreading globally within seconds before it is addressed.
- **Jurisdiction:** Determining jurisdiction is challenging when the perpetrator, victim, and servers are situated in different locations.

9 Information Technology Act of 2000

- **Persistence:** Defamatory content can persist online even after deletion, exemplifying the "Streisand effect[10]").
- **Admissibility:** The court requires that digital evidence of defamation, like screenshots, timestamps, and IP addresses, be collected through a forensically sound process for it to be accepted.

Judicial response:

There is no specific online-defamation law in Nepal; defamation is addressed under the general law (*Criminal Code, 2017*, §§ 305, 308), which outlines definitions, penalties, and limitations. While courts have made rulings on libel and slander, they struggle with cyber jurisprudence, causing misclassification of online-defamation as cybercrimes (ETA, 2006/2017, § 47). Prosecutors and judges often lack understanding of these areas, leading to inconsistent verdicts and potential miscarriages of justice.

Comparative scrutiny of selective online-defamation laws

USA: The 1st Amendment strongly protects online-defamation under a civil tort. Platforms are often exempt from accountability for user-posted defamatory content (CDA, 1996, § 230), which shifts the burden of proof to the original speaker. Accordingly, victims usually bring legal action against the specific poster rather than the platform.

UK: The defamation law was updated to address digital concerns by introducing a "serious harm" threshold for claims and specific defenses for intermediaries, aiming to balance reputation preservation with free speech (*Defamation Act 2013*, c. 26, § 1).

India: It is covered by the ITA and ordinary criminal legislation (IPC, 1860, §§ 499–500; ITA, 2000, §§ 66, 79). Intermediaries must remove content within 36 hours of a court order or official notification and are subject to "due diligence" requirements, which include grievance redressal procedures for defamatory content (IT

10 The Streisand effect happens when efforts to hide or restrict information unintentionally draw more attention to it, which causes it to spread and become more visible.

(Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 3(1)(d)).

EU: Strong defamation laws in EU nations are reinforced by the new *Digital Services Act,* which aims to enhance online safety by regulating unlawful content, including defamation. Platforms must establish clear notice-and-action mechanisms (Regulation (EU) 2022/2065, 2022, Recital 14, Arts. 3, 14, 20, 21, 23).

Nepal: Nepal's online defamation laws stand a double standard (ETA, § 47; *Criminal Code, 2017,* §§ 305–308), lacking the comprehensive intermediary responsibility frameworks present in developed nations.

Nepalese laws on new media:

Social media use in Nepal has outpaced the legislative framework, resulting in clashes among issues of hate speech, misinformation, disinformation, malinformation and the freedom of expression (*Constitution of Nepal, 2072,* art. 17(2)(a)).

Current regulatory attempts

- **Information Technology and Cyber Security Bill, and Social Media Guidelines:** The "Bill" and "Guidelines" direct social media must set up local offices, register, and remove illegal content. Along with harsh fines for online expression, this act has raised concerns about censorship and restrictions on free speech. *(Information Technology and Cybersecurity Bill, 2082, Guidelines for Regulating the Use of Social Media, 2080).*

- **Social Medial Bill, 2024:** The *Social Media Bill* tried to hold digital platforms legally responsible for damaging online content, such as defamation (SMB, 2024). The main difficulty is striking a compromise between protecting democratic norms and the right to free speech and minimizing digital harms[11].

11 According to Article 93 of the Constitution, the Bill expired as a result of the Gen-Z protests that led to the dissolution of the House of Representatives.

Challenges: Pairing FoE with content moderation

Accomplishing a balance between safeguarding freedom of expression and mitigating harms from unlawful content is a key challenge:

Over vs. under regulation: Calls for stricter regulations to mitigate online harms conflict with concerns about potential censorship and suppression of legitimate dissent.

Intermediary responsibility: The degree to which platforms (intermediaries) ought to be responsible for user-posted information remains a significant unsolved question. Should they be viewed as conduits or publishers?

Techno-viability: Enforcing content moderation at scale poses technical challenges for platforms and regulators, especially with regard to various languages and dialects.

Cross-border application: National laws struggle to effectively regulate content that is created or accessed across borders, reflecting the borderless nature of social media.

Best models for regulation

EU: Platforms must comply with the Digital Services Act, which mandates risk assessments for disinformation, clear notice-and-action processes for illegal content, and transparency in content management, aiming to create a safer online environment (Regulation (EU) 2022/2065, 2022, recitals 14, arts. 3, 14, 20, 21, 23).

Germany (NetzDG): The Network Enforcement Act mandates intermediaries to remove "manifestly unlawful" content, including hate speech and incitement to violence, within 24 hours of notification, exemplifying strict content regulation (Regulation (EU) 2022/2065, 2022, Art. 14).

India: Intermediaries are subject to stringent due diligence requirements under ITA *(Intermediary Guidelines and Digital Media*

Ethics Code) Rules, 2021, which include designating resident grievance officers, permitting message tracing, and eliminating specified content. They have generated controversy because of worries about censorship and privacy.

USA: CDA provides platforms with significant immunity from liability for third-party content, allowing for flexible content management, unlike the stricter regulations in Europe and India (47 U.S.C. § 230(c) (1), 2018).

The fall of a government: How Gen-Z protest was initiated against social media ban in Nepal:

The Government of Nepal implemented the contentious "*Directives for Managing the Use of Social Networks, 2023,*" which led to the suspension of more than 26 platforms, including Facebook, WhatsApp, YouTube, and Instagram, in a clear attempt to establish digital control (Reuters, 2024). Online annoyance swiftly gave way to the "Gen-Z Protest," a leaderless movement calling for greater economic opportunity and governmental responsibility in addition to the restoration of digital rights (Access Now, 2024).

Large-scale protests resulted in at least 74 verified deaths and several injuries were caused by the riots, according to Amnesty International (2024). This episode serves as a clear example of how a misunderstanding in digital policy can directly lead to significant political disruption and change.

Challenges and recommendation:

Nepal encounters significant challenges in addressing defamation, cybercrime, and online media, necessitating a robust and proactive approach.

Key challenges

Legislative caps: Nepal lacks a competent cyberlaw to address the intricacies of online media. Cybercrime and defamation in the digital age are the biggest obstacles. The effective prosecution is

hampered due to clear legal gaps of intermediary accountability, digital evidence standards, and online harms are required.

Capability for implementation: Significant resource limitations hinder law enforcement organizations like the Police, including a shortage of skilled digital forensic specialists, inadequate laboratory facilities, and limited access to advanced equipment for cybercrime investigations. The rapid pace of technological advancement often outstrips the tools and training available to investigators.

Techno-legal savviness: Judges and legal professionals often lack the necessary techno-legal expertise to interpret complex digital evidence and cyberlaw, leading to trial delays, inconsistent verdicts, and challenges in proving guilt based on digital traces.

Digital literacy and media ethics: Digital illiteracy makes many vulnerable to Internet fraud and misinformation, disinformation and malinformation highlighting the need for improved media ethics among online journalists and content creators.

Cross-border issues: Investigations, evidence collection, and prosecution are complicated by diverse laws, data retention policies, and slow international cooperation, as the borderless Internet allows offenders, victims, and digital evidence to cross multiple jurisdictions.

Balancing rights: Drafting and enforcing legislation involves a complex balance between protecting free speech and managing offensive Internet content to ensure reputation, privacy, and public order.

Recommendations:

To successfully tackle the digital issue, Nepal requires a multifaceted, flexible, and cooperative approach:

Legal reform: Enact a comprehensive cyberlaw to define and criminalize various cybercrimes related to online media, including data breaches, online fraud, hacking, cyberstalking, and the spread of malicious disinformation.

Explicit online-defamation provisions: Introduce measures for online defamation in techno-media laws that safeguard freedom of expression while addressing the unique characteristics of digital information, such as anonymity, permanence, and virality.

Intermediary accountability clause: Provide a precise and appropriate legal framework for online platforms' intermediary liability that strikes a balance between their duty to support free expression and their role in content regulation. Clear "notice and take down[12]" protocols for unlawful content should be part of this.

Investment on infrastructure: Invest in cutting-edge digital forensic labs (DFLs) nationwide, ensuring continual software and tool enhancements.

Capacity building of officials: Judges, prosecutors, and law enforcement should receive comprehensive training in cybercrime investigation, digital evidence handling, and cyberlaw, and cyber-expert judges should be appointed in the apex judiciary for their expertise in techno-legal matters.

Encourage media ethics and digital literacy: National Digital Literacy Programs aim to enhance digital literacy and critical thinking skills regarding online content and Internet threats, particularly targeting marginalized groups.

Code of conduct for digital platforms: Promote and assist self-regulatory organizations in creating and enforcing strong ethical standards for all online content producers, including social media influencers and citizen journalists.

Enhance cross-border collaboration: Introduce MLATs[13] to

12 The "notice and take down" is a process where requests to remove or disable access to illegal content, such as copyright infringement or material that exploits children, are sent to content intermediaries. This concept was established by statutes such as the US Digital Millennium Copyright Act (DCMA) of 1998 where no court order is required to take action.

13 Mutual Legal Assistance Treaties

facilitate the rapid sharing of digital evidence with compatible international jurisdictions.

International association: Standardizing legal processes for digital evidence may involve aligning with international conventions like the Budapest Convention on Cybercrime, regardless of signatory status.

Multi-stakeholder collaboration: The goal is to establish effective Internet governance solutions through close collaborations between various sectors, including government, law enforcement, civil society, media, academia, and technology businesses.

Research and adaptation: Monitor global trends in defamation, cybercrime, and online media, adjusting legal and policy responses to keep pace with rapid technological changes.

Conclusion:

Nepal's shift to a digital era presents a "digital dilemma" for its media and legal landscape. While social media and online platforms have transformed communication, they have also increased cybercrime and online defamation. The existing legal framework, particularly the *Electronic Transactions Act, 2063*, is inadequate for addressing these challenges. There is an urgent need for a comprehensive cyberlaw that includes provisions for online defamation and intermediary liability, supported by improved judicial literacy and enforcement capabilities through digital forensics. Additionally, fostering strong media ethics and digital literacy are key societal initiatives.

Resolving Nepal's digital challenges requires an active and flexible approach, involving legal reforms, capacity building, and multi-stakeholder partnerships. This strategy aims to enhance the safety and legality of online media, ensuring both public safety and fundamental freedoms in a rapidly digitizing society, which is essential for Nepal's progress in the global digital landscape.

References

Access Now. (2024). Statement on the Internet shutdown in [Country]. https://www.accessnow.org/

Akpan, U. (2021). The new media technologies. *IDOSR Journal of Arts & Humanities*, 6(1), 30–42. https://www.idosr.org/wp-content/uploads/2021/07/IDOSR-JAH-61-30-42-2021..pdf

Amnesty International. (2024). Country: Security forces must show restraint amidst widespread protests. Amnesty International. https://www.amnesty.org/en/latest/news/2024/statement/

AAG IT Services. (2025, July 10). The latest cybercrime statistics (updated July 2025). https://aag-it.com/the-latest-cyber-crime-statistics/

Bhattarai, S. K. (2022). Is social media defamation a civil or criminal wrong? *Nepal Law Review,* 43 (30/1), 187–219.

Bhattarai, S. K. (2024). *Cyber law and Internet crimes.* Communication Registrar's Office, Bagmati Province Government.

Citron, D. K., & Wittes, B. (2017). The problem of state-sponsored hacking. *Harvard National Security Journal,* 8, 439–476. https://harvardnsj.org

Constitution of Nepal, 2072 (Nepal). (2015). https://ag.gov.np/files/Constitution-of-Nepal_2072_Eng_www.moljpa.gov_.npDate-72_11_16.pdf

Council of Europe. (2017). *Information disorder: Toward an interdisciplinary framework for research and policymaking*. (C. Wardle & H. Derakhshan, Authors). https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

Cropink. (2025). 40+ threatening social media hacking statistics. https://cropink.com/social-media-hacking-statistics

DefendDefenders. (2025, May 2). Statement on World Press Freedom Day. https://defenddefenders.org/statement-for-world-press-freedom-day/

Department of Homeland Security, Science and Technology Directorate. (2025). Distributed Denial of Service Defense Fact Sheet. https://www.dhs.gov/publication/st-distributed-denial-service-defense-fact-sheet

Department of Information and Broadcasting, Nepal. (2016). *Online media operation directive,* 2073. https://doib.gov.np/content/585/585-online-media-operation-direc/

Digital.gov. (2025, March 25). Social media. https://digital.gov/topics/social-media

European Union. (2022). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services

(Digital Services Act) and amending Directive 2000/31/EC, 2022 O.J. (L 277) 1. https://eur-lex.europa.eu/eli/reg/2022/2065/oj

FBI. (2014, December 19). FBI's statement on the cyberattack against Sony Pictures Entertainment. U.S. Department of Justice. https://archives.fbi.gov/archives/news/pressrel/press-releases/fbi-statement-on-the-cyber-attack-against-sony-pictures-entertainment

Government of Nepal. (2006/2017). *Electronic Transactions Act, 2006,* as amended by the Act of Some Nepal Law Amendment, Repeal, Unification and Adjustment, 2017. Law Book Management Committee.

Government of Nepal. (2008). *Electronic Transactions Act, 2063*. Nepal Law Commission. https://lawcommission.gov.np/en/?cat=573

Indian Penal Code, No. 45 of 1860, §§ 499–500 (India). https://indiacode.nic.in/handle/123456789/2263

Keepnet Labs. (2025, August). 2025 phishing statistics (updated August 2025). https://keepnetlabs.com/blog/top-phishing-statistics-and-trends-you-must-know

Law Book Management Committee. (2017). *Criminal Code, 2017.* Ministry of Law, Justice and Parliamentary Affairs.

Media Defence. (2025). Online threats & harassment. https://www.mediadefence.org/ereader/publications/modules-digital-rights-europe/module-6-online-harassment-anonymity/online-threats-harassment/

Ministry of Communication and Information Technology, Nepal. (2023). *Digital Nepal framework.* https://mocit.gov.np/content/268/268-e-consultations-digital-nepal/

Ministry of Communication and Information Technology, Nepal. (2023). *Guidelines for regulating the use of social media, 2080.* https://mocit.gov.np/category/259/?page=3

Ministry of Electronics and Information Technology, Government of India. (2021, February 25). *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.* https://www.meity.gov.in/

Morgan, S. (2021, April 26). Cybercrime to cost the world $10.5 trillion annually by 2025. *Cybersecurity Ventures.* https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

National Institute of Standards and Technology. (2018, April 16). *Framework for improving critical infrastructure cybersecurity (Version 1.1).* https://www.nist.gov/cyberframework

National Assembly, Nepal. (2024). *Media Council Bill, 2080 BS,* registration no. 1 (presented Jan. 12, 2081 BS). https://na.parliament.gov.np/en/bills/xcr5Q9ZJ

Nepal Law Commission. (1991). *Press and Publication Act, 2048*. https://lawcommission.gov.np/content/13391/printing-and-publication-act--2048/

Nepal Law Commission. (1992). *National Broadcasting Act, 2049*. https://www.nta.gov.np/uploads/contents/np_The-National-Broadcasting-Act1993.pdf

Nepal Law Commission. (1995). *Working Journalists Act, 2051*. https://lawcommission.gov.np/content/13395/working-journalists-act-2051/

Parliament of Nepal. (2018). *Information Technology Bill, 2075*. https://hr.parliament.gov.np/uploads/attachments/eucmqwyeyg3nf9ov.pdf

Parliament of Nepal. (2024). *Social Media Bill, 2081*. https://na.parliament.gov.np/en/bills/JCC7TZJz

Parliament of Nepal. (2025). *Information Technology and Cyber Security Bill, 2082,* Bill No. 8 of 2082. https://hr.parliament.gov.np/np/bills?type=reg&ref=BILL

Reuters. (2024). Nation enforces sweeping social media ban. Reuters. https://www.reuters.com/

ScienceDirect Topics. (2025). Online media. https://www.sciencedirect.com/topics/computer-science/online-media

Sessions College for Professional Design. (2025, January 14). What is digital media | Types, importance, and applications. https://www.sessions.edu/notes-on-design/what-is-digital-media/

Sophos. (2025, May 31). The state of ransomware 2025. https://www.sophos.com/en-us/content/state-of-ransomware

United Nations Human Rights Committee. (2011, September 12). General comment No. 34: Article 19 – Freedoms of opinion and expression. CCPR/C/GC/34. https://www.ohchr.org/sites/default/files/english/bodies/hrc/docs/gc34.pdf

United Nations Office on Drugs and Crime. (2023). *Trafficking in persons in the digital age* (pp. 15–18). https://www.unodc.org/documents/data-and-analysis/glotip/2024/GLOTIP2024_BOOK.pdf

United States. (1986). *Computer Fraud and Abuse Act*, 18 U.S.C. § 1030.

United States. (1996). 47 U.S.C. § 230. https://www.law.cornell.edu/uscode/text/47/230

United States. (1787). U.S. Constitution, art. I, § 8. https://constitution.congress.gov/constitution/article-1/section-8/