CDJMC, TU

Toolkit for Regulators on Digital Platforms Governance

Based on the UNESCO Guidelines for the Governance of Digital Platforms



Published under the initiative

"Safeguarding Freedom of Expression and Access to Information through the Implementation of the UNESCO Guidelines for the Governance of Digital Platforms,"

Jointly undertaken by
Tribhuvan University, Nepal; Jahangirnagar University, Bangladesh; and the University of Vocational Technology, Sri Lanka,
with the support of UNESCO.

April 2026

A Toolkit for Regulators on Digital Platforms Governance

ISBN: 978-9905-0-1075-8 (Print version)

ISBN: 978-9905-0-1109-0 (e-Book)

Edition: 1st | Print: 1000 Copies

This Toolkit is available at: cdjmc.tu.edu.np

© UNESCO/CDJMC, TU

Cover, Typesetting and Graphic Design: UNESCO Template

Published by:

Central Department of Journalism and Mass Communication (CDJMC), Tribhuvan University, with the support of UNESCO.

Layout & Typesetting: Jit B. Pun
Printed by: Thememaker Pvt. Ltd, Adwait Marg, Kathmandu

Toolkit for Regulators on Digital Platforms Governance

Based on the UNESCO Guidelines for the Governance of Digital Platforms

unesco
United Nations
Educational, Scientific
and Cultural Organization

UNIVOTEC

TABLE OF CONTENTS

5 **Foreword**

7 **Preface**

11 **Executive Summary**

14 **The UNESCO Guidelines and the role and responsibility of regulators: An overview**

15 **Role and responsibilities of independent regulatory authorities**

26 Acting as an Independent Oversight Agency
28 Holding Digital platforms Accountable
30 Audits for self-regulation systems
31 Co-regulation
33 Regulatory mandate and procedure to oversee, review and audit
35 Manifestation of the multistakeholder approach
37 Way Forward: Practical Guide to Integrating the Toolkit for Regulators
42 Annex-I
50 Annex-II
52 Annex-III
52 Harmful Content Decision Flowchart for Regulators
54 Annex IV
54 Case Studies
62 References

Foreword

Digital platforms have become central to how people speak, listen, organize, and learn. They carry public information and debates in dozens of languages and across communities that may have long had little access to the public sphere. Meanwhile, they also carry harmful content, misinformation, and disinformation that shape what millions of people see. The question before South Asia region is no longer whether digital platforms should be governed, but how — in ways anchored in international human rights standards and pressing national realities.

UNESCO's Constitution commits the Organization to promoting the free flow of ideas by word and image. It is under this mandate that UNESCO developed the Guidelines for the Governance of Digital Platforms, published in November 2023 after an extensive multi-stakeholder consultation that engaged 134 countries in total. The Guidelines set out a systemic, human rights-based approach to platform governance transparent, accountable, proportionate and evidence-based. It made clear that regulators need not choose between freedom of expression and user safety, or between innovation and rights.

Regulatory authorities carry particular responsibility for translating these principles into practice. Their independence, their procedural fairness, and their capacity to look beyond individual pieces of content to the systems and safeguards behind them are what distinguish rights-respecting regulation from restriction. This Toolkit for Regulators responds to that demand. Developed under the project "Safeguarding Freedom of Expression and Access to Information through the Implementation of the UNESCO Guidelines for the Governance of Digital Platforms" and as part of the Internet for Trust initiative, it offers regulators in Bangladesh, Nepal and Sri Lanka practical guidance on independent oversight, platform accountability, audits of self-regulation systems, role in co-regulation, algorithmic and systemic oversight, among others, and is supported by checklists, decision flowcharts and case studies drawn from the region itself.

The strength and credibility of the Toolkit lie in the inclusive and evidence-based process through which it was developed. It draws on national consultations and on interviews and workshops held in Colombo, Dhaka, and Kathmandu between December 2025 and March 2026, and on a systematic review of the laws in force in the three countries. It was validated at a regional workshop in Kathmandu in March 2026 that brought together parliamentarians, regulators, media, academia, civil society, and youth.

UNESCO expresses its appreciation to the European Union, the participating universities and all partners and stakeholders who contributed to this important regional effort.

This Toolkit is offered as a living resource, to be tested, adapted and improved through use. UNESCO hopes that this Toolkit will support regulators in developing independent, capable and rights-respecting institutions as well as encourage continued cooperation across South Asia.

Jaco du Toit
UNESCO Representative to Nepal and Head of Office

Preface

The Toolkit for Regulators, developed to support the implementation of the UNESCO Guidelines for the Governance of Digital Platforms in the South Asian context, is now in your hands. On behalf of the Departments of Media Studies at Jahangirnagar University (Bangladesh), the University of Vocational Technology (Sri Lanka), and Tribhuvan University, (Kathmandu, Nepal). I am pleased to present this Toolkit as the outcome of extensive observations of the digital platform landscape, consultations with users and policymakers, and a review of relevant legal frameworks across these three countries.

The project, Safeguarding Freedom of Expression and Access to Information through the Implementation of the UNESCO Guidelines for the Governance of Digital Platforms, was initiated in August 2025. At the outset, only a preliminary framework was available, and we planned to employ multiple approaches to map the existing landscape of digital platform governance across Bangladesh, Nepal, and Sri Lanka. We closely examined similarities in their socio-political contexts, including growing frustration among youth over governments' inability to adequately protect citizens' right to freedom of expression. We also engaged with diverse stakeholders—including government officials, politicians, media professionals, academics, and members of civil society—to address an important question: How can the rights and freedoms of citizens be better protected within the contemporary digital media environment?

The process began with individual consultations and subsequently expanded through workshops conducted in Colombo, Dhaka, and Kathmandu, with significant participation from women. In parallel, country briefs were prepared to assess the legal provisions governing digital platforms in Bangladesh, Nepal, and Sri Lanka. The Toolkit evolved through an empirical process involving both individual and group consultations conducted through interviews and workshops between December 2025 and March 2026. More than 300 individuals contributed their expertise and perspectives throughout this process.

Alongside these efforts, a systematic review of relevant laws and policies was undertaken to ensure that the Toolkit was grounded in the legal and regulatory realities of Bangladesh, Nepal, and Sri Lanka. Findings from this review, together with insights from interviews and workshops, were further tested and refined through continued engagement with a broad range of stakeholders. These included government agencies, lawmakers and political actors, law enforcement bodies, ministries responsible for law and communication, digital platforms, telecommunications authorities, Press Councils and Information Commissions, journalists' unions, academia, media organizations, civil society representatives, and the technical community. This process helped ensure that the Toolkit reflects diverse institutional, professional, and public-

interest perspectives and is grounded in a genuinely inclusive and multi-stakeholder consultation process across the three countries.

Before its finalization, the Toolkit was validated and refined through structured feedback received during a regional workshop held in Kathmandu in March 2026. The workshop brought together a diverse range of stakeholders from Bangladesh, Nepal, and Sri Lanka, as well as observers from the Maldives. Participants included policymakers - such as Members of Parliament - alongside officials from UNESCO and I4T at both headquarters and country levels.

The Toolkit embodies the spirit of the Pretoria Proposition for Action (2026), which recognizes that effective governance cannot rest solely on digital platforms themselves or on regulators acting independently. The Proposition further emphasizes that civil society organizations, researchers, educators, and affected communities play a critical role in identifying systemic risks, supporting redress mechanisms, and strengthening media and information literacy.

An important aspect worth highlighting is that the Toolkit also outlines several future steps that UNESCO may consider operationalizing in the years ahead. It further includes provisions for institutional adoption and curriculum integration within universities. Designed specifically for the regulators, the Toolkit aims to create meaningful opportunities for sharing experiences, good practices, and challenges while contributing to a coordinated and multi-stakeholder regional approach.

The practical checklist and monitoring guide developed within the Toolkit are intended to capacitate regulators to respond effectively to online harm. They can play proactive role and promote accountability and transparency in digital platforms in a systematic manner. The subsequent units and case studies included in the annexes provide practical and engaging examples that help civil society actors better understand the issues and indicators they are expected to examine.

Careful attention has also been given to the structure and presentation of the Toolkit to ensure that it remains both comprehensive and accessible. It broadly follows American Psychological Association (APA) style conventions. Necessary explanations and contextual clarifications have been integrated into the text where appropriate to enhance readability.

At this moment of successfully completing this initiative and presenting the Toolkit for regulators, I would like to express my sincere gratitude to UNESCO officials, from the Kathmandu Office to Headquarters. I would particularly like to acknowledge the support and encouragement provided by Mr. Jaco du Toit, UNESCO Representative to Nepal and Head of Office, and his colleagues, including Ms. Nirjana Sharma, Lead for

the Communication and Information Sector/Programme Officer; Ms. Aruna Joshi, Digital Media Associate; and Ms. Yujie Fan, Trainee. Their unwavering support throughout the preparation process significantly contributed to the completion of this Toolkit.

I would also like to express my sincere appreciation to Ms. Ana Cristina Ruelas, Senior Programme Specialist, Section for Freedom of Expression and Safety of Journalists, Communication and Information Sector, UNESCO; as well as Mr. Christophe Gauthier and Mr. Chandra Bhanu Patnaik, Co-Chairs of the I4T Knowledge Network, for their valuable technical expertise, without which this Toolkit would not have taken its present shape.

The preparation and publication of this Toolkit would not have been possible without the invaluable contributions, hard work, and dedication of H.A. Gayan Madushanka, Head of the Department of Film & Television Production Technology at the University of Vocational Technology (Sri Lanka), and Rakib Ahmed, Associate Professor in the Department of Journalism & Media Studies at Jahangirnagar University (Bangladesh). Both colleagues have been closely involved in this initiative from its inception. They played a key role in organizing the respective national consultation workshops in Sri Lanka and Bangladesh and actively participated in the regional workshop in Kathmandu, and contributed significantly to the development and refinement of the Toolkit's content. Their expertise, thoughtful insights, and sustained commitment substantially enriched the intellectual and practical dimensions of this publication. I sincerely appreciate their valuable support and contributions throughout the process. This Toolkit is the outcome of a rigorous collaborative effort involving experts and stakeholders from various countries and institutions, including UNESCO and IUT. I gratefully acknowledge Dr. Shree Ram Paudel's contribution throughout the process from research to the compilation of materials.

Last but not least, I would like to thank my team, including faculty members at the Central Department of Journalism and Mass Communication, Hiroyuki Tiara, Dr. Ghama Raj Luitel, Dr. Rishikesh Dahal, Dr. Deb Raj Aryal, and Dr. Shashi Marasini. I also extend my gratitude to experts beyond the Department, including Mr. Ujjwal Acharya, Mr. Santosh Sigdel, and Mr. Tara Nath Dahal, as well as the administrative staff of the Department, Ms. Kalpana Bajracharya and Mr. Eka Raj Kadel. I would like to express my sincere thanks to Ms. Iksha Limbu, and MPhil-PhD scholar at CDJMC, for her carefull and meticulous final proofreading. I firmly believe that without the dedication and hard work of all these individuals, the publication of this Toolkit would not have been possible.

Kundan Aryal, PhD
Professor and Head of the Department
Central Department of Journalism and Mass Communication
Tribhuvan University, Nepal

Executive Summary

This Toolkit, designed for regulators, aims to provide practical guidance for operationalizing the UNESCO Guidelines for the Governance of Digital Platforms in Bangladesh, Nepal, and Sri Lanka. While developed in the context of these three countries, it may also be broadly applicable across South Asia and other regions with similar socio-political and economic conditions. As the Toolkit identifies eight common concerns related to digital platform governance across these countries, many of these issues may also be relevant in other regional and global contexts. This initiative has been undertaken as a collaborative effort between UNESCO and partner universities under the project titled "Safeguarding Freedom of Expression and Access to Information through the Implementation of the UNESCO Guidelines for the Governance of Digital Platforms."

The introductory and preliminary sections explain the roles and responsibilities of independent regulatory authorities in promoting safer digital platforms and outline the current state of regulatory mechanisms in Bangladesh, Nepal, and Sri Lanka. The Toolkit is grounded in five key principles: platforms conduct human rights due diligence; platforms adhere to international human rights standards, including in platform design, content moderation, and content curation; platforms maintain transparency; platforms provide users with access to relevant information and tools; and platforms remain accountable to relevant stakeholders. Building on these principles, the Toolkit presents six core standards that should guide officials and members of regulatory institutions responsible for platform content governance.

The Toolkit highlights the role of regulators in fostering safer and more accountable digital environments. Through an examination of the socio-political context of the three countries, it concludes that Bangladesh, Nepal, and Sri Lanka face comparable challenges in digital platform governance. Although multiple regulatory bodies exist, their mandates and jurisdictions often remain fragmented, overlapping, and insufficiently defined.

The Toolkit primarily aims to support regulators in these countries by equipping them with the knowledge, frameworks, and practical tools necessary to engage effectively in digital platform governance. It envisions regulators to play an active role in overseeing platform practices, ensuring compliance with international Human rights standards, promoting Human rights based digital policies, addressing systemic risks related to content governance, and enhancing transparency, accountability, and user empowerment.

The Toolkit was developed through an empirical process involving individual and group - consultations conducted through interviews and workshops across Bangladesh, Nepal, and Sri Lanka between December 2025 and March 2026. As a result, it reflects the realities of digital platform governance within these countries. More than 300 individuals contributed their expertise and perspectives during the consultation process. In parallel, a systematic review of relevant laws and policies was undertaken, which played an instrumental role in shaping the Toolkit. Before finalization, the Toolkit was validated and refined during a regional workshop held in Kathmandu in March 2026. The workshop brought together a diverse range of stakeholders from Bangladesh, Nepal, and Sri Lanka, including policymakers such as Members of Parliament as well as officials from UNESCO and I4T at both headquarters and country levels.

Following the introductory section, the Toolkit is organized into seven thematic units that progressively move from practical approaches to broader strategies for strengthening digital platform governance. It begins with practical guidance on enabling independent oversight agencies to function effectively (Unit I). It then presents measures for holding digital platforms accountable (Unit II), methods for auditing self-regulatory systems (Unit III), approaches to co-regulation (Unit IV), and regulatory mandates and procedures for oversight, review, and auditing (Unit V). The Toolkit further explores multistakeholder approaches by recommending practical measures for regulators to facilitate inclusive engagement in governance processes (Unit VI). Finally, it presents a forward-looking perspective (Unit VII), offering practical guidance for integrating the Toolkit into university curricula and other institutional settings.

The Toolkit is particularly well-suited for educational purposes. Its clearly-structured units, supported by practical scenarios, checklists, tools, and monitoring indicators related to harmful content, provide a valuable framework for learning and practical application. Furthermore, its emphasis on human rights due diligence, multistakeholder approaches, transparency, and systemic oversight, rather than heavy-handed content regulation, makes it highly relevant in both academic and professional settings. The Toolkit also aligns closely with UNESCO's broader initiatives on Media and Information Literacy (MIL), AI competency frameworks for students and teachers, and the ethical integration of artificial intelligence in higher education.

In addition to the thematic units, the annexes provide practical materials, including case studies, checklists for regulators, and harmful-content classification frameworks. The case studies demonstrate how similar risks emerge across different contexts and reveal recurring patterns in Bangladesh, Nepal, and Sri Lanka. They further illustrate why a purely content based regulatory approach remains insufficient without considering systemic processes and safeguard mechanisms.

Overall, the Toolkit envisions a proactive and constructive role for regulators in strengthening trust in the Internet and fostering a more inclusive and rights-based digital environment. It directly reflects UNESCO's broader objectives of ensuring that freedom of expression, access to information, and diverse cultural content are protected for all. At the same time, it recognizes the importance of collaborative efforts among multiple stakeholders, including government agencies, in addressing challenges such as disinformation, misinformation, and online hate speech.

The UNESCO Guidelines and the role and responsibility of regulators: An overview

The UNESCO Guidelines provide a comprehensive framework for governing digital platforms in ways that safeguard human rights, particularly freedom of expression and access to information (UNESCO, 2023). The guidelines recognize that digital platforms play a central role in shaping public discourse, cultural exchange, and information ecosystems worldwide. Therefore, their governance requires regulatory approaches that balance innovation, accountability, and the protection of human rights.

The key principle of the Guidelines is that digital platform governance should be carried out through a multistakeholder approach involving governments, independent regulators, and digital platforms, along with civil society organizations, academia, and users. This ecosystem should function through complementary regulatory arrangements-regulation by platforms and industry bodies, co-regulation involving shared responsibilities between private actors and public authorities, and statutory regulation established by states. Independent regulatory authorities would be required to maintain such an ecosystem. Independent regulatory authorities play a pivotal role within this governance structure. In this context, the Guidelines emphasize that where statutory regulation is required, it should be administered by regulators that are institutionally and operationally independent from political or commercial influence. Independence is essential to ensure that regulatory decisions are impartial, transparent, and aligned with international human rights standards.

The Guidelines highlight overarching principles applicable to a wide range of governance processes concerning digital platform content. They stress that an effective governance system should combine complementary regulatory arrangements to address the needs and responsibilities of different actors in the digital ecosystem. In particular, the Guidelines call for a multistakeholder approach, which includes identifying all relevant stakeholders including platforms within the regulatory scope ensuring inclusive participation and balanced representation, promoting transparency and accountability, fostering collaborative decision-making and dialogue, coordinating implementation among stakeholders, and supporting iterative processes with periodic evaluation and review.

Role and responsibilities of independent regulatory authorities

The responsibilities of independent regulators in the governance of digital platforms include overseeing the implementation of regulatory frameworks, monitoring compliance by digital platforms, and ensuring accountability mechanisms are effective. Regulators may be tasked with supervising platform transparency obligations, assessing compliance with codes of conduct, and ensuring that content moderation policies respect due process and users' rights. They also play an important role in coordinating with other stakeholders, such as civil society, industry bodies, and technical experts, to ensure that regulatory responses remain adaptive and evidence based.

Furthermore, the guidelines highlight that independent regulators should facilitate transparency, stakeholder participation, and periodic evaluation of regulatory measures. This includes promoting open dialogue among stakeholders, reviewing the effectiveness of governance arrangements, and adjusting regulatory strategies in response to technological and social developments in the digital ecosystem.

The UNESCO Guidelines, position independent regulators as key institutional actors within a broader multi-stakeholder governance framework. Their independence and oversight functions are critical for ensuring that regulatory systems governing digital platforms remain transparent, accountable, and consistent with the protection of human rights in the digital age.

The UNESCO Guidelines emphasize that the governance of digital platforms involves a complex ecosystem of stakeholders, regulatory arrangements, and institutional mechanisms. Existing governance frameworks -such as those related to elections or data protection- must be interpreted and adapted to address the evolving challenges of the digital environment, while new governance structures are also emerging specifically to regulate digital platforms. Because these regulatory arrangements can have significant implications for freedom of expression, access to information, and the availability of diverse cultural content online, the Guidelines underscore the need for governance approaches that safeguard human rights.

Within this framework, the Guidelines recognize different forms of regulatory arrangements that may operate in a complementary manner. These include self-regulatory mechanisms, where industry bodies or social media councils oversee and enforce rules; co-regulatory mechanisms, where codes of conduct may receive legal recognition and operate as regulatory instruments; and statutory regulatory frameworks-such where independent regulators have the authority to set and enforce

rules for digital platforms. Given the complexity of the digital environment, statutory frameworks may be necessary in certain domains where self- or co-regulation is insufficient.

Importantly, the Guidelines stress that when statutory regulation is established, independent regulatory authorities play a central role. Such regulators should operate autonomously, oversee the implementation of regulatory frameworks, and monitor compliance by digital platforms. At the same time, states retain the responsibility to establish regulatory systems that protect human rights and ensure transparency in platform operations, while regulatory bodies ensure that these frameworks are effectively implemented in line with the Guidelines' human rights based approach to digital governance. The UNESCO Guidelines explicitly state that every statutory regulatory intervention should be evidence-based, proportionate, and include procedural safeguards, including by ensuring the platform access to all facts and considerations upon which the decision is made. This process should involve multiple stakeholder groups, considering a broader view of the sustainability, effectiveness, and impact of the intervention. The call for an evidence-based process cannot be an excuse to delay necessary regulatory actions to protect human rights. The Guidelines also outline that regulatory authorities should identify those platforms that have relevant presence, size, and market share in a specific jurisdiction. These should be determined through an independent assessment of the risks they pose to human rights, including groups in situations of vulnerability and marginalization, as well as to democratic institutions. The definition of the scope should protect the right to privacy and not result in the weakening of protections for encryption or other privacy-protecting technologies.

Only statutory regulation would not be effective. It must be supplemented with co-regulation and self-regulation. In statutory regulation, official regulatory authorities, though constituting part of the executive state apparatus, should be wholly independent of the government and be primarily accountable to legislatures for fulfilment of their mandates. This applies to existing regulatory bodies that have a legitimate interest in content on platforms, such as electoral management bodies, advertising authorities, child protection entities, data and privacy commissions, competition bodies, etc., as well as any new dedicated or coordinating regulatory instances that may be established. With regard to all statutory bodies engaging in platform regulation, either solely or jointly, periodic review should be performed by an independent body reporting directly to the legislature. Statutory interventions should also be subject to review in the courts if authorities are believed to have exceeded their powers, acted unreasonably, or acted

in a biased or disproportionate manner.

Official regulatory authorities need to be independent and free from economic, political, or other pressures. Their power and mandate should be set out in law. They should also comply with international human rights and promote gender equality standards.

Official regulatory institutions must have sufficient funding and expertise to carry out their responsibilities effectively. The sources of funding must also be clear, transparent, and accessible to all, and not subject to governmental discretion.

Governing officials or members of the official regulatory institutions working on the issue of content on platforms should meet following standards:

a. Be appointed through a participatory, transparent, non-discriminatory, and independent merit-based process.
b. Be accountable to an independent body which could be the legislature, judiciary, an external council, or an independent board.
c. Include relevant expertise in international human rights law and the digital ecosystem.
d. Deliver an annual public report to an independent body, ideally the legislature, and be held accountable to it, including by informing the body about their reasoned opinion.
e. Make public any potential conflicts of interest and declare any gifts or incentives.
f. After completing the mandate, for a reasonable period, hired by or provide paid services to those who have been subject to their regulation, to avoid the risk known as "revolving doors."

The official regulatory authorities should be able to request that digital platforms provide periodic reports on the application of their terms of service/community guidelines and take enforcement action against digital platforms deemed non-compliant with their own policies or failing to fulfill their responsibilities to safeguard freedom of expression and access to information and diverse cultural content. However, the enforcement action should strictly be aligned with Article 19 of the International Covenant on Civil and Political Rights (United Nations General Assembly, 1966). Thus the regulators are required to be able to establish a complaints process and issue public recommendations that may be binding or non-binding and be empowered to issue transparent and appropriate directives to the platforms for the promotion and respect of human rights, based on international human rights

standards.

Role of regulators to meet five principles of Digital Platform Governance

Regulators should act as primary custodians by establishing a systematic governance framework aligned with the five core principles of the UNESCO Guidelines: human rights due diligence, adherence to international standards, transparency, accessibility of information and tools for users, and accountability. Rather than micromanaging platforms, regulatory authorities should focus on the systems and processes through which platforms govern content, setting clear standards to address systemic risks to human rights stemming from product and service design and from content moderation and curation practices (UNESCO, 2023; Sharma & Bandara, 2022). Any moderation or curation measures should be grounded in international human rights norms and remain open to judicial review to ensure accountability and the protection of freedom of expression.

Regulators should require platforms to conduct human rights impact assessments and apply the "three-part test": legality, legitimacy, and necessity to all moderation policies. They should also establish standards for transparency reporting, ensure that freedom of expression is not constrained by linguistic or digital barriers, and hold platforms accountable for systemic failures. In this way, regulators function as guarantors of procedural justice for users. Their role should be that of a process auditor rather than a content police, focusing on the oversight of governance frameworks and accountability mechanisms rather than intervening in individual content decisions.

What are digital platforms?

In the context of digital platform governance, digital platforms are online services that facilitate interactions between users, businesses, and content through digital infrastructure and algorithms. They are the online systems that organize and distribute information and interactions on the internet, making them central actors in digital communication and public debate.

The UNESCO Guidelines for the Governance of Digital Platforms refers to large online intermediaries that organize and moderate information flows and social interactions online, influencing how information is produced, shared and consumed.

Common characteristics of digital platforms:

- **Intermediation:** They act as intermediaries connecting users, creators, advertisers and other actors.
- **User-generated content:** Users can create, upload and share content such as posts, videos, comments, or reviews.
- **Algorithmic curation:** Platforms use algorithms to recommend, rank or prioritize content.
- **Large-scale reach:** They enable mass communication and information sharing.
- **Data-driven operations:** Platforms collect and process user data to personalize content and services.

Examples of digital platforms

- **Social media platforms:** Facebook, X (Twitter), TikTok, Instagram
- **Video-sharing platforms:** YouTube
- **Messaging platforms:** WhatsApp, Telegram
- **Search engines:** Google Search
- **App Stores:** Apple Appstore, Google Play Store, Samsung Galaxy Store
- **Content and discussion platforms:** Reddit, forums, blogs
- **Online marketplaces and service platforms:** Pathao, Foodmandu
- **Artificial Intelligence:** Google AI Studio, Deepseek, ChatGPT, Claude

Role of Regulators in Promoting Safer Digital Platforms

The UNESCO Guidelines emphasize that digital platforms should act as responsible stewards of the digital ecosystem by shifting from reactive content removal to a proactive, system-based approach to content governance that allows to identify the way diverse digital products, services or features may have an impact in the rights of users, including their safety (UNESCO, 2024). For this shift to occur, regulators need clear and explicit mandate to guide platforms in aligning their operational practices with international human rights standards rather than allowing economic incentives to prioritize engagement over public safety.

Regulators should therefore ensure that digital platforms incorporate human rights considerations into their fundamental architecture, from algorithmic design to content

curation. This requires platforms to conduct ongoing human rights due diligence to identify and mitigate systemic risks such as misinformation, hate speech and coordinated manipulation including through risk assessment before deploying new features and enhanced monitoring during high-stakes periods such as elections, disasters both natural and human created, riots or similar kind of social crises.

Through consultation with relevant stakeholders, regulators should also encourage platforms to prevent the amplification of content that undermines social harmony that resulted in incitement to violence, discriminatory hate speech, or coordinated harassment. Likewise, the platforms are expected to mitigate the contents that hamper religious tolerance, and democratic discourse, while adhering to the United Nations Guiding Principles on Business and Human Rights, 2011 (United Nations, 2011). The Guiding Principles, under the provision of general State regulatory and policy functions, gives the State effective guidance to business enterprises on how to respect human rights throughout their operations.

To promote trustworthy digital platforms, regulators should establish governance frameworks that require platforms to ensure transparency, due diligence and strengthen user empowerment. Platforms should be required to clearly disclose their content moderation policies and procedures, provide accessible reporting mechanisms in local and indigenous languages, and maintain transparent, human-operated appeals processes. Regulators should also encourage platforms to support media and information literacy by equipping users with the knowledge and tools necessary to critically engage with online content.

Within a multistakeholder governance framework, regulators should ensure that platforms' private governance practices align with international human rights standards in order to foster an "Internet of Trust." In this regard, regulators play a crucial role in overseeing key areas of platform responsibility, including content governance, algorithmic accountability, user grievance mechanisms, and human rights compliance. This includes setting standards for fair and transparent moderation processes, requiring audits of algorithmic systems to assess human rights risks, ensuring effective mechanisms for handling user complaints and appeals, and mandating the publication of human rights due diligence and transparency reports. Through such regulatory oversight, platforms can be guided toward safer, more accountable, and rights-respecting digital environments.

Regulators in Bangladesh, Nepal and Sri Lanka

Bangladesh, Nepal, and Sri Lanka exhibit similar regulatory challenges in the governance of digital platforms. Although multiple regulatory bodies are involved, their mandates and jurisdictions often remain fragmented and poorly defined (Bangladesh Telecommunication Regulatory Commission, n.d.; Government of Bangladesh, n.d.; Government of Nepal, n.d.; Press Council Nepal, n.d.; AHN Legal, n.d.; Parliament of Sri Lanka, 2024; Telecommunications Regulatory Commission of Sri Lanka, n.d.; Digital Watch Observatory, 2024; International media monitoring discussions, n.d.). This institutional overlap creates uncertainty in regulatory authority, weakens accountability, and complicates the effective governance of digital platforms.

In Bangladesh, the authorities that regulate the landscape of media and freedom of expression include – the Ministry of Information and Broadcasting, Bangladesh Press Council, Bangladesh Telecommunication Regulatory Commission (BTRC), Bangladesh Film Certification Board (BFCB), Information Commission of Bangladesh, Film Censor Board, and Cyber units of Bangladesh police.

In Nepal, there are various institutions authorizing for regulating social media and their contents including the Ministry of Information and Communication Technology (MoCIT), Press Council Nepal, Nepal Telecom Authority, Department of Information and Broadcasting, Advertising Board of Nepal, National Information Commission, Film Development Board and Cyber Bureau of Nepal Police.

In Sri Lanka, Online Safety Act (OSA) of 2024 provisioned the 'Online Safety Commission' to regulate online content. Other authorities responsible for regulating landscape of media and freedom of expression include Ministry of Mass Media, Sri Lanka Press Council (SLPC), Telecommunications Regulatory Commission (TRC) for electronic & digital media, and Right to Information Commission for access to information.

Across the three countries, regulatory frameworks for platform governance face significant institutional and operational challenges. In Sri Lanka, for example, the establishment of the proposed Online Safety Commission has faced prolonged delays. In Nepal, the Press Council Nepal (PCN) has faced public criticism in relation to certain enforcement actions involving digital media content, additionally there have also been concerns regarding varying levels of compliance with its directives, including those related to the election code of conduct.

More broadly, all three countries exhibit gaps in the clarity of mandates and jurisdictional authority for platform governance. Regulatory bodies in these contexts are also shaped, to varying degrees, by political appointment processes, which have contributed to periodic public debate regarding their independence and the perceived neutrality of certain decisions.

In all three countries, there is a lack of clear mandate and jurisdiction regarding platform governance. These regulating agencies are also influenced by political appointments resulting in low credibility and decisions are sometimes blamed as politically motivated.

Aim of the Toolkit

This Toolkit aims to support regulators of these three countries with the knowledge, frameworks and practical tools needed to engage and participate in the governance of digital platforms in line with the UNESCO Guidelines for the Governance of Digital Platforms. In advancing platforms governance issues from a multistakeholder perspective, the I4T mission, a trusted partner to UNESCO in order to oversee the implementation of the Guidelines, is adequately consulted. The Toolkit aims to regulators to oversight platform practices, take necessary actions, taking care of international human rights standards, for human-rights–based digital policies, address systemic risks linked to content governance and promote transparency, accountability and user empowerment.

By strengthening the capacity of regulators, the Toolkit supports multistakeholder collaboration and encourages the development of a trustworthy and rights-respecting digital information environment in Bangladesh, Nepal, and Sri Lanka.

Overall, this Toolkit aims to help up practical guidelines for regulators to safeguard freedom of expression, protect users from online harms and contribute to accountable digital platform governance in the region.

Why this Toolkit?

In the evolving digital ecosystem, regulators play a pivotal role in enabling the state to meet its obligations to respect, protect, and fulfil human rights for internet users. As digital platforms increasingly shape public discourse by amplifying voices, enabling diverse expressions, and influencing access to information, regulatory oversight becomes essential to ensure accountability and rights protection. Regulators should therefore adopt comprehensive governance strategies that promote market

contestability and fair competition, ensure transparency in data practices and algorithmic systems, and introduce proportionate content and safety regulations. In addition, the establishment of independent oversight mechanisms and the application of structural and behavioral remedies where necessary can help address systemic risks. Through such measures, regulators can guide digital platforms toward operating in a manner consistent with democratic values, public interest, and international human rights standards.

Digital platforms have become central actors in modern information ecosystems. Their algorithms determine which information is amplified, which voices are prioritized or deprioritized, and how users interact with content online. As a result, platforms hold significant influence over the formation of public opinion and democratic discourse. However, the rapid growth of these platforms has also revealed structural challenges. Misinformation has affected elections and public discourses. Algorithmic recommendation systems may amplify sensational or harmful content in order to maximize user engagement. Furthermore, the concentration of power in a few major technology companies has raised concerns about transparency, accountability and the protection of fundamental rights.

Governments around the world have attempted to address these issues through various regulatory initiatives. Yet some regulatory efforts risk undermining freedom of expression or enabling censorship. Recognizing this paradoxical situation, UNESCO developed guidelines to provide a human-rights-based framework for digital platform governance. The framework aims to help states to build digital platform governance approaches while safeguarding human rights. Another key rationale behind the development of guidelines is to address the challenges created by the global nature of digital platforms. Since online services operate across national borders, isolated national regulations are often insufficient. The UNESCO guidelines therefore encourage international cooperation and common standards that can guide policy development worldwide.

Objectives of the Toolkit for regulators

- **Safeguard human rights, including freedom of expression and access to information, for both users and non-users of digital platforms.**
- **To capacitate regulator to identify harmful contents and to establish mechanisms to mitigate risk of harmful contents.**
- **Provide tools to monitor and assess online harms, disinformation, and content moderation practices of digital platforms.**

- **Ensure adherence to the five core principles of platform governance: human rights due diligence, international human rights standards, transparency, accessibility of information, and accountability.**
- **Strengthen multistakeholder collaboration among regulators, digital platforms, academia, civil society, and other relevant actors for a trustworthy internet.**

Thus, objectives of this Toolkit can be achieved when an independent regulator, accountable and subject to parliamentary oversight, is able to engage with civil society, including the media, academia, the technical community, and other stakeholders in the subregion. Its overall objective is to strengthen the regulatory body so that it is both capable and empowered with the jurisdiction to advance governance mechanisms to address the risks associated with the design, use, deployment, promotion, etc. of digital services and products. However, the annual report of the regulatory body must be presented before Parliament and remain subject to its scrutiny. The idea is to enable the regulator to play a more instrumental role in holding states and digital platforms accountable for digital rights and the full spectrum of interconnected human rights.

How to use this Toolkit?

This Toolkit serves as a practical manual for regulatory bodies to navigate digital platform governance, as it includes unit-based checklists to design activities or conduct research or advocacy initiatives along with templates and examples. Some suggestive practical uses of this Toolkit are as follows:

- **Support to create an atmosphere where the regulatory body can function as an independent oversight agency:** Drawing on insights from Unit I, strengthening information integrity and enhancing platform accountability for information disorder.
- **Holding Digital Platforms accountable:** Use the 'Monitoring Framework for Harmful Content' from Unit II to identify threat actors, affected groups, and the impact of algorithmic amplification in local context.
- **Support and legal guidance by auditing self-regulatory systems:** Apply strategies from Unit III.
- **Promote shared role in maintaining co-regulation:** Drawing on insights from Unit IV by enhancing human rights-friendly legal framework.
- **Ensure a system and process for content moderation and curation:** Only with the

condition of respecting human rights as envisaged in Unit V.

- **Manifestation of multistakeholder approach:** Drawing on insights from Unit VI for safer and more trustworthy platforms.
- **Integration of the Toolkit with the University's curricula:** Drawing insights from Unit VII, the Toolkit would be instrumental to provide a practical guide to integrate the quest of digital platform governance.

The Toolkit shows how the independent regulatory body can systematically promote accountability in digital platform governance. The process begins with collaboration with CSOs that are involved in monitoring by observing platform practices, policies, and emerging online harms. Findings are then documented through evidence collection and research reports. The next step is analysis, where patterns, impacts, and systemic risks are examined to understand the broader implications. Based on this evidence, a regulatory body can be involved in change through policy recommendations and campaigns. This would be followed by engagement with CSOs and platforms, where findings are communicated to companies to encourage improvements in policies, moderation practices, and transparency. Finally, these efforts contribute to policy reform, influencing laws, regulations, and governance frameworks.

Thus, the Toolkit would be useful to:

- **monitor digital platform practices**
- **conduct digital platform research**
- **document online harms**
- **engage in policy advocacy**
- **support victims of online abuse**
- **participate in multi-stakeholder governance processes**
- **promote media and information literacy**

Unit I
Acting as an Independent Oversight Agency

As an independent oversight agency, the regulator acts as a neutral arbiter between the state, the platforms, and the public. Regulatory arrangements should be effective and sustainable, considering the available local resources and the main priorities needing attention (for example, whether to address issues primarily around elections, public health, advertising, or data protection, etc.). Independent oversight is needed for all forms of regulation. The process for developing regulation should be open, transparent, and evidence-based.

Functions of regulating bodies

1. Systemic auditing and supervision : From content policing to systems and processes oversight, algorithmic accountability, compliance audits, resource inspection. Regulatory bodies should oversee and evaluate platforms' systems for identifying and addressing misinformation and other harmful or illegal content, ensuring that such systems are transparent, accountable, and consistent with applicable human rights standards.

A Parliamentary oversight agency is necessary to ensure freedom of expression and safe internet for users and non-users. An independent regulator needs a mandate and the capacity to oversee the systems and process that platforms put in place to design new products and services as well as to moderate and curate content and to sanction in case of not compliance on their duties to be transparent, accountable and perform due diligence. However, there should be clear and comprehensive conditions for such steps and which should fall under be of judicial purview. The whole process should be reported to parliament.

Regulators need to be responsible for setting standards, overseeing compliance, and ensuring accountability, rather than directly monitoring or flagging individual pieces of content at scale. Direct content monitoring may raise concerns regarding feasibility, resource constraints, and potential risks to regulatory independence and freedom of expression.

Regulators need to be capable of enforcing mitigation of illegal content, incitement to violence, coordinated manipulation with clear boundaries and provisions that lead to consistent interpretation.

Regulators need to be more precise to framing the regulator's role as overseeing whether platforms have effective systems in place to detect, assess, and mitigate such content in line with due process, transparency, and human rights standards, rather than directly engaging in content-level flagging.

2. Managing and mitigating risk/crisis: Mandating due diligence on human rights assessments, requiring crisis protocols during high-risk events such as elections, natural disasters, or conflicts for protecting democratic integrity (Amnesty International, 2026; United Nations, 2011).

3. User protection and appeals: Regulator serves as a protector for the public when platform systems ignore or fail.

Facilitate between platforms and users to appeal content removals or account suspensions.

Sort out the problems (in some jurisdictions) as platforms remain unresponsive on the issues raised by users or civil society organizations.

4. Promotion of transparency by allowing data access to researchers: Respecting user privacy and publishing an annual report on the digital ecosystem and environment.

5. Multistakeholder coordination: Civil Society members- human rights defenders, academia, journalists, and marginalized groups, inter-agency cooperation (data protection authorities, election commission etc.)

Regulatory bodies should operate independently and impartially, ensuring that their decisions are guided by law, evidence, and the public interest rather than by political considerations..

Regulatory bodies should monitor and flag in case of circulation of misinformation, and harmful content.

Regulators should have financial autonomy to avoid political interference.

Regulators should have clear legal protection to avoid unwarranted dismissal from the government.

Regulatory decisions should be subject to judicial review to ensure due process, prevent arbitrary restrictions, and safeguard against any misuse of regulatory authority that could undermine freedom of expression or democratic accountability.

Unit II
Holding Digital platforms Accountable

Digital platforms deemed non-compliant with their own policies or failing to fulfill their duties to safeguard freedom of expression and access to information while dealing with content that could be permissibly restricted under international human rights law and standards, in accordance with the five principles described in the UNESCO digital platform guidelines, should be held accountable to relevant bodies within the governance system and subject to proportionate enforcement measures with necessary procedural safeguards.

Measures for platform accountability

1. Oversee platforms compliance with transparency reports

- Regularly publish data on content removals, account suspensions, and the number of government requests for data or removal of the content.
- Algorithmic disclosure (how content is prioritized, recommended or demoted).
- Maintain public, searchable repositories of all political and issue-based ads, showing who paid for them and who was targeted.

2. Oversee platforms risks management and due diligence

Regulators should establish clear mechanisms to communicate compliance assessments to digital platforms and ensure that appropriate accountability measures are applied in cases of non-compliance, including corrective actions, reporting requirements, or sanctions where necessary. Any sanctions imposed should always be necessary, legitimate, and proportionate in line with applicable legal and human rights standards.

3. Oversee platforms to advance user empowerment and resolving the issues

- There should be accessible reporting mechanism which provides easy to use, multilingual tools for users to report illegal or harmful content with clear tracking of the report's status.
- Allow users to adjust their own feed settings to opt out of certain types of algorithmic recommendations or sensitive content.

4. Independent Oversight and Enforcement

- Platforms should consider that it is important to ensure appropriate safeguards are in place when regulators request or access data from platforms, particularly with regard to privacy and data protection considerations.
- Statutory sanctions need to be imposed like meaningful fines or corrective orders if a platform fails to meet its obligations.

5. Crisis and Election safeguards

- Establish and ensure the rapid response protocols in coordination with concerned stakeholders.
- Use labeling and contextualization for controlled (state) media and AI-generated 'deepfake' content to provide users with the necessary context rather than just deleting them.

Regulators should establish clear mechanisms to communicate compliance assessments to digital platforms and ensure that appropriate accountability measures are applied in cases of non-compliance, including corrective actions, reporting requirements, or sanctions where necessary (United Nations Human Rights Committee, 2011). Any sanctions imposed should always be necessary, legitimate, and proportionate in line with applicable legal and human rights standards.

Unit III

Audits for self-regulation systems

Self-regulation systems can be complementary and converge with other forms of regulation. They should include independent periodic mandatory audits that assess digital platforms' compliance with self-regulatory codes, policies, or norms. Such audits should not be directly funded by industry or individual digital platforms, although levies on these entities can help cover the costs of such exercises. Nor should audits be conducted by any person or entity that would have or appear to have a conflict of interest. The terms and results of the audit should be available for public comment.

Measures for self-regulation

1. Governance and procedural audits

- Reviewing the platforms Terms of Service to ensure that they are compatible with international standards of human rights law (Article 19 and 20 of the ICCPR).
- Auditing whether the platform applies its own rules consistently across different geographic regions and languages.
- Ensuring that appeal mechanisms are subject to regular review to verify their independence, effectiveness, and accessibility, including safeguards to prevent purely automated or non-substantive review processes and to ensure meaningful human oversight of appeal decisions.

2. Algorithmic audits

- Self-regulation system also includes the monitoring of algorithmic trends to make platforms accountable on the flow of MDM. Subsequently, there should be professional code of ethics as complementary mechanism to the statutory regulations.

Unit IV
Co-regulation

Co-regulatory structures should provide a legal framework that promotes and protects freedom of expression, access to information, privacy, and other human rights. Under a co-regulatory model, responsibility for achieving regulatory objectives is shared among platforms, relevant stakeholders, and public authorities, including independent regulatory bodies where appropriate.

The role of public authorities should focus on establishing and overseeing the regulatory framework, setting minimum standards, monitoring compliance, facilitating stakeholder participation, and ensuring accountability. Public authorities may formally recognize co-regulatory schemes, audit their effectiveness, and provide or facilitate sustainable funding arrangements, including through levies on platforms where appropriate. Where agreed objectives are not being met, regulators should have the authority to impose corrective measures and, where necessary, legitimate and proportionate sanctions in accordance with applicable legal and human rights standards.

Measures for co-regulation

- **Establish clear minimum standards and baseline requirements for platform governance, transparency, accountability, and risk management.**
- **Develop certification mechanisms for industry codes of conduct, accompanied by periodic independent review to assess their effectiveness and continued compliance with regulatory objectives.**
- **Require platforms to submit regular transparency reports using standardized reporting frameworks to enable meaningful oversight and comparison across services.**
- **Establish measurable and comparable indicators to assess the effectiveness of platform governance systems, including content moderation, appeals mechanisms, risk mitigation measures, and transparency practices.**
- **Require platforms to provide formal explanations and remediation plans where significant failures in content governance, risk management, or crisis response systems are identified, and empower regulators to require corrective measures where appropriate.**

- **Convene multi-stakeholder processes involving platforms, civil society, academia, and affected communities to develop guidance and standards for emerging issues, including generative AI and synthetic media.**
- **Facilitate secure and privacy-respecting access to relevant platform data for qualified independent researchers to support auditing, accountability, and evidence-based policymaking.**
- **Support joint capacity-building initiatives for content moderators and platform personnel on local legal frameworks, linguistic contexts, and international human rights standards.**
- **Promote public awareness and media and information literacy initiatives, with platforms providing appropriate user tools and information, and public authorities coordinating broader educational efforts.**
- **Oversee whether platforms conduct appropriate risk assessments and due diligence regarding the design, deployment, and operation of their products and services, particularly where these may contribute to the amplification of harmful content or other systemic risks.**

Unit V
Regulatory mandate and procedure to oversee, review and audit

Statutory regulation of digital platforms addressing issues that might impact freedom of expression should be considered only when there is independence in decision-making of the regulatory authorities involved in its implementation. Such regulation should focus on systems and processes for content moderation and curation, rather than determining the legality of individual pieces of content, and must have a basis in law (i.e., be sufficiently defined), pursue a legitimate aim under Article 19 (3) of the ICCPR, and be necessary and proportionate.

1. Algorithmic and systemic oversight

- Regulators oversee platforms to ensure rights-respecting, consistent, and culturally sensitive on their systems and processes for curating and moderating content.
- Regulators should request for plain language explanations of how platform's recommendation algorithms curate content and the measures they take to ensure that harmful content (like hate speech or incitement to violence) is not amplified.
- Regulator has to audit the error rates (over-censor or under-protect specific groups) of AI tools and ensure that automated moderation systems (AI) are subject to regular human oversight. Likewise, they are subject to undergo third-party audits.
- The regulators should develop comprehensive parameters to ensure non-discrimination by design. It should refrain from discrimination based on race, gender, religion, or ethnicity. Platform's curation should not marginalize protected groups.

2. Procedural fairness and due process

- Transparency of terms of services
- Standardized notification systems
- Ensure that the platforms provide a functional, human-led appeals mechanism for timely resolutions.

3. **Linguistic and cultural competency**

- Localized moderation capacity
- Make sure that moderators understand local sociopolitical nuances, slurs, and cultural contexts during contextual training (automated systems often miss).

4. **Periodic risk management and safeguards**

- Emerging threats of deepfakes and coordinated inauthentic behavior (bots).
- Crisis response protocols during high-stakes events (e.g., riots or natural disasters) to slow the spread of life-threatening misinformation.

5. **Data access**

- Research API access
- Sample test for platform moderation systems

Unit VI
Manifestation of the multistakeholder approach

The multistakeholder approach in statutory regulation should be reflected in an arrangement by which: a. Relevant State authorities, including official independent regulatory authorities, set the legitimate aim of the regulation through participatory and inclusive legislative processes. b. Digital platforms report publicly to official regulatory authorities. c. Civil society organizations, artists, independent researchers, and other relevant institutions provide inputs into rule making, contribute to oversight, and achieve the necessary procedural safeguard.

Appropriate measures for regulators to manifest this approach include

1. **Inclusive institutional design**

   - Multistakeholder advisor boards
   - Public consultation for regulatory decisions, codes of conduct, or policy change
   - Diversity in leadership (representation on regulatory agency- diverse professional backgrounds including human rights law and digital technology).

2. **Collaborative oversight and monitoring**

   - Joint working groups consisting of platforms, fact-checkers, journalists working for thematic issues like election integrity or AI ethics. The groups are expected to perform fact-checking and observe the state of ethical domain.
   - Providing observer status to civil society in order to ensure safe internet.
   - Technical community engagement (partner with internet engineers and data scientists for ensuring technical reality of how platforms work is reflected in the law.

3. **Transparency and shared knowledge**

   For open data frameworks, annual multistakeholder forum (annual report or digital ecosystem), joint media and information literacy campaign (civil society and media and information literacy).

4. Crisis and rapid response coordination

- Multi-agency partnership with election commissions, platforms, civil society members and academia
- Information sharing channel needs to exist to mitigate Misinformation, Disinformation and Malinformation.

5. International & regional cooperation

- Sharing best practices across the region and ensuring global platforms are following consistent standards across borders.
- Alignment with Pretoria Proposition for Action wording in order to create peer dialogue and share knowledge and then to create standardized parameters to advance on the principles set in the guidelines.

Unit VII
Way Forward: Practical Guide to Integrating the Toolkit for Regulators

This section, a practical guide, to integrating the Toolkit for Regulators, is developed in the context of South Asia based on the UNESCO Guidelines 2023 into university curricula and other institutions. It aims at contextualizing the guidelines in Bangladesh, Nepal, and Sri Lanka, where resources are limited, political sensitivities exist, and digital challenges such as MDM, linguistic diversity, elections are acute.

Why the Toolkit Fits Education

The Toolkit is well suited for educational purposes. Its structured organization into clear units (I–VI), complemented by practical annexes such as checklists, platform classification tools, and decision-making flowcharts, makes it accessible for teaching and learning. The Toolkit places strong emphasis on human rights due diligence, multi-stakeholder governance, transparency, accountability, and systemic oversight, rather than content-level regulation or censorship.

This approach is consistent with UNESCO's work on Media and Information Literacy (MIL), AI competency frameworks for learners and educators, and the responsible integration of AI and digital technologies in education. It can contribute to building the capacity of future regulators, policymakers, journalists, lawyers, researchers, technology professionals, and informed citizens by equipping them with the knowledge and skills needed to assess platform governance, accountability mechanisms, and systemic risks in digital environments. In doing so, it promotes critical understanding of how digital platforms operate and how they can be governed in a manner that respects human rights and democratic values.

Step-by-Step Integration into University Curricula

1. Embed as a Standalone or Core Module

- Create a 3-credit elective or required course titled something like "Digital Platform Governance and Human Rights" or "Regulating the Digital Ecosystem: South Asian Perspectives."
  - **Target audience:** Undergraduate, graduate and post-graduate students in Media Studies and other branches of Humanities and Social Sciences, Law and Human Rights Studies, Computer Science/IT and Public Policy.
  - **Structure around the Toolkit's units:**
  - Unit I (Independent Oversight) + Annexes Core reading for "Regulatory Independence and Accountability."
  - Units II–V (Accountability, Audits, Co-regulation, Moderation Systems) Modules on transparency reporting, algorithmic audits, and content classification.
  - Unit VI (Multistakeholder Approach) + deepened AI sections Capstone on co-designing rules for deepfakes/generative AI.
  - Teaching methods: Case studies from Bangladesh (BTRC challenges), Nepal (Press Council critiques), Sri Lanka (Online Safety Act delays); role-playing regulator-platform-civil society negotiations; group audits using the Toolkit's checklists.

2. Transdisciplinary Approach

- **Law/Policy programs:** Use as core texts for courses on cyber law, media regulation, or data protection - pair with ICCPR three-part tests and global comparisons such as EU AI Act, UNESCO AI Ethics.
- **Media Studies and other branches of Humanities and Social Sciences:** Link to MIL - teach students to analyze platform moderation failures, fact-check deepfakes, and advocate for user empowerment.
- **Computer Science/IT**: Add technical modules on algorithmic accountability, watermarking/C2PA standards, red-teaming AI moderation systems, and human oversight of automated tools.
- **Education/Faculty Development**: Train future teachers using UNESCO's AI Competency Frameworks alongside the Toolkit for classroom discussions

on ethical AI use and combating disinformation. The training also needs to be based on the guidelines for the governance of digital platforms and all the companion documents:

- a) Guidance for risk assessment.
- b) the companion document on generative AI
- c) the about to be consulted fair compensation guidance.
- **Cross-cutting:** Make it part of general "Digital Citizenship" or "Ethics in the Digital Age" requirements for all levels of university education.

3. Practical Learning Activities

- **Simulate regulatory decisions:** Using Annex-III flowchart during mock elections or crisis scenarios, e.g., viral deep-fake in local context.
- **Student projects:** Conduct mock audits of local platforms, e.g., how TikTok or Facebook handles multilingual hate speech; draft co-regulatory codes for generative AI.
- **Guest lectures:** From actual regulators such as Press Council Nepal, BTRC, Bangladesh, Online Safety Commission, Sri Lanka, followed by Toolkit-based debriefs.
- **Capstone:** Multistakeholder Policy Lab where students propose adaptations of the Toolkit for their country's context.

4. Faculty and Institutional Support

- Offer short faculty workshops for 1–2 days on using the Toolkit, co-organized with UNESCO's regional and national office or local digital rights groups.
- Update existing syllabi gradually, start as optional readings, then adopting them as mandatory.
- Partner with UNESCO's South Asia initiatives, e.g., AI Readiness Assessments in Bangladesh, digital learning policies in Nepal, for resources and credibility.

Integration Beyond Universities

- **Regulatory Bodies and Government Training Academies**
  - Mandatory induction/refresher training for staff at BTRC, Nepal Telecom Authority, Press Council Nepal, Sri Lanka's Online Safety Commission, etc.
  - Use Units I–III for acting as independent oversight workshops; Annexes for day-to-day tools, e.g., harmful content classification during elections.
  - Annual multistakeholder forums (per Unit VI) could double as training events.
- **Civil Society and NGOs**
  - Capacity-building workshops for digital rights organizations, fact-checkers, and journalists, focus on using checklists to monitor platforms and advocate for better policies.
  - Integrate into MIL programs for communities, youth, and vulnerable groups such as women, ethnic minorities, empower them as watchdogs per UNESCO guidance.
- **Media Training Institutes**
  - Embed in professional development courses: Teach reporters how platforms moderate content and how to push for transparency without self-censorship.
- **Tech Companies and Private Sector**
  - Internal compliance training for local platform teams or ad agencies — especially on context to evaluate risk and perform due diligence, watermarking, and co-regulation (Unit IV).
  - Joint academies with universities for "platform governance certification."
- **Libraries, Community Centers & Lifelong Learning**
  - Short public sessions or MIL clubs using simplified Toolkit materials, e.g., harmful content table translated into Nepali, Bangla, Sinhala.
  - Libraries as neutral hubs for digital ecosystem reports discussions.

Realistic Implementation Roadmap for Bangladesh, Nepal and Sri Lanka

- **Phase 1 (Short-term, 6–12 months):** Pilot in 2–3 universities, e.g., Tribhuvan University in Nepal, Jahangirnagar University in Bangladesh and University of Vocational Technology in Sri Lanka. Run one faculty workshop and one student simulation based on the translated version of the Toolkit in local language.
- **Phase 2 (1–2 years):** Scale via national education ministries or University Grants Commission (UGC) equivalents. Link to existing digital transformation efforts in higher education. Explore support from UNESCO, other development partners and platforms.
- **Phase 3 (Ongoing):** Annual reviews, updates with new AI developments such as watermarking and red teaming. Measure success via student/regulator feedback, not just exam scores: Are participants better at spotting systemic risks?

Potential Challenges and Coping Strategies

1. **Resource constraints**: Start low-cost, use the open Toolkit PDF and free UNESCO MIL resources. Blend online and offline module.
2. **Political sensitivities**: Frame as "capacity building for responsible governance" aligned with national laws and human rights, not anti-government critique. Emphasize multistakeholder balance.
3. **Relevance**: Supply sufficient local examples, e.g., election disinformation in Nepal, linguistic moderation challenges in Bangladesh.
4. **Evaluation**: Use pre/post knowledge tests on the five UNESCO principles, plus qualitative feedback on practical skills.

Annex-I

Checklist for regulators

1. Checklist for Identifying Digital Platforms

(For determining whether a service qualifies as a digital platform subject to governance)

A. Nature of the Service

- Enables users to create, upload, or distribute content.
- Facilitates interaction between users (commenting, messaging, sharing, reposting, or community participation).
- Organizes, curates, recommends, ranks, or prioritizes content, accounts, products, or services.
- Disseminates content, information, or services to public, large scale or undefined audiences.

B. Type of Platform

- Social networking platforms
- Video-sharing or content-sharing platforms
- Search engines or content discovery service
- Messaging or communication service
- Online community forums or discussion platform
- Online marketplaces and app stores

C. Scale and Reach

- Has significant reach or user base in the country or region.
- Shapes public discourse or political communication.
- Plays a significant role in the dissemination of news, cultural content, or public information.
- Serves as an important channel for political, civic, educational, or commercial communications.

D. Functionalities and technical characteristics

- Operates recommendation, ranking, or personalization systems.
- Provides features that may increase the reach, visibility, virality, or discoverability of content.
- Provides advertising, targeting, or content promotion services.
- Enables automated or large-scale dissemination of content, including through bots, AI systems, or bulk messaging functionalities.
- Collects, processes, or uses user data to personalize content, services, or advertising.

E. Risk Indicators

a. Country and societal context

- Operates in a context affected by elections, political instability, conflict, public emergencies, or heightened social tensions.
- Operates in multilingual environments where local and indigenous languages may be insufficiently supported.
- Has significant influence on communities that may be disproportionately affected by online harm.
- Has substantial cross-border reach or influence within the national information ecosystem.

b. Service-Related Risk Factors

- Potential to influence elections or democratic processes.
- Risk of coordinated disinformation campaigns.
- Potential harm to vulnerable communities.
- Cross-border influence affecting national information ecosystems.

2. Checklist for Identifying Regulators

Who can regulate digital platforms?

Although there are various agencies functioning with partial regulatory mandates in Bangladesh, Nepal and Sri Lanka, a quest is in place to transit to single independent and capable regulatory body. Such single regulatory authority would also need to see issues on markets competition and data protection. Since the sub-region is in the transitional phase in terms of ideal mechanisms for digital platform governance, new legislation is expected from newly elected parliaments in all three countries.

A. Institutional Status

- Established through law or statutory authority.
- Mandate includes media, telecommunications, digital services, market competition, data protection and information governance.
- Possesses authority to monitor, supervise, or enforce compliance.

B. Independence

- Institution operates independently from political influence.
- Leadership appointed through transparent and merit-based procedures.
- Funding mechanisms are transparent and secure from political pressure.

C. Functional Capacity

- Ability to audit platform policies and transparency reports.
- Ability to investigate complaints from users or civil society.
- Authority to issue directives, recommendations, or sanctions.
- Capacity to coordinate with other agencies and stakeholders.

D. Human Rights Safeguards

- Decisions aligned with international human rights standards.
- Regulatory actions follow procedural fairness and due process.
- Regulatory decisions are subject to judicial review.

E. Examples of Potential Regulators (Country Context)

Prime regulating agency in three countries are: Bangladesh Telecommunication Regulatory Commission (BTRC) which basically focuses on OTT services and revenue, Ministry of Communication and Information Technology of Nepal supervises all concerned sectors including licensing and monitoring, and Online Safety Commission is proposed in Sri Lanka under Online Safety Act, 2024.

In contexts such as Nepal, regulators may include:

Various bodies such as the Ministry of Information and Communication Technology, Press Council Nepal, Nepal Telecommunications Authority, Department of Information and Broadcasting, Advertising Board of Nepal, National Information Commission, Film Development Board, the Cyber Bureau of Nepal Police, and the AI Cell of Nepal Police perform partial regulatory functions.

(These operate within fragmented mandates and may require coordination).

3. Checklist for Determining Regulatory Jurisdiction

(What authority regulators should exercise over platforms)

A. Legal Authority

- Jurisdiction clearly defined in legislation or regulatory frameworks.
- Regulatory mandate includes digital platforms or online intermediaries.
- Powers include monitoring, oversight, and enforcement.

B. Scope of Regulation

- Platform operates within national territory or provides services to users in the jurisdiction.
- Platform has significant market presence or user base in the country.
- Platform activities impact people in situations of vulnerability and marginalization.

C. Regulatory Functions

- Oversight of platform transparency reporting.
- Supervision of content moderation systems and processes.
- Regulation of political advertising to enhance the state of information integrity by mitigating prevalence and impact of misinformation, disinformation, and algorithm-driven content.
- Monitoring algorithmic accountability
- Risk assessment

D. Enforcement Mechanisms

- Authority to request data and transparency reports from platforms.
- Authority to conduct audits or independent assessments.
- Ability to issue binding directives or recommendations.
- Ability to impose proportionate sanctions or fines.

E. Procedural Safeguards

- Decisions based on evidence and proportionality.
- Platforms have the right to respond before enforcement action.
- Regulatory decisions open to judicial review.

F. Coordination Across Agencies

- Cooperation with data protection authorities
- Cooperation with election management bodies.
- Cooperation with competition authorities.
- Cooperation with law enforcement agencies.

G. Primary role of Regulators

Regulators' role should focus on systemic oversight, including:

- Ensuring platforms have transparent moderation policies.
- Monitoring algorithmic amplification of harmful content.
- Requiring human rights impact assessments.
- Facilitating user complaints and appeals mechanisms.

4. Checklist for Platform Accountability Compliance

- transparency reporting
- human rights due diligence
- user complaint mechanisms
- algorithmic audits

5. Checklist for Identifying Harmful Content on Digital Platforms

A. Assessing the Legality of Restrictions on Content (Three-Part Test – International Human Rights Standard)

- **Legality**
  Is the content restricted under clearly defined national law consistent with international human rights standards?
- **Legitimate Aim**
  Does the restriction aim to protect legitimate interests such as:
  - Public safety (Does it pose clear and present danger?)
  - National security
  - Protection of reputation or rights of others
  - Public health
- **Necessity and Proportionality**
  Is intervention genuinely required to prevent or mitigate a clearly identifiable harm?

Do the expected benefits of the intervention outweigh its potential impact on freedom of expression and public access to information?

B. Types of Potentially Harmful Content

Harmful contents comprise of disinformation including electoral, gendered, and climaterelated disinformation, misinformation, hate speech, incitement to genocide or violence and child sexual abuse material including child pornography. The other categories often mentioned are the mechanisms or vectors through which harmful content is directed at individuals or groups. These include harassment and cyberbullying, deepfakes and synthetic media.

Regulators should assess whether the content falls into one or more of the following categories:

- **Disinformation**
  False or misleading information intended to deceive the public.
- **Hate Speech**

Content attacking individuals or groups based on race, religion, gender, ethnicity, nationality, or other protected characteristics. In the Rabat Plan of Action, hate speech refers to *advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence* (UN High Commissioner for Human Rights, 2013).

- **Incitement to Violence**
  Content encouraging violence, discrimination, or hostility against individuals or communities.
- **Harassment and Cyberbullying**
  Systematic online abuse or intimidation targeting individuals.
- **Extremist or Terrorism-related Content**
  Content promoting or supporting violent extremist organizations or acts.
- **Coordinated Manipulation**
  Organized campaigns using fake accounts, bots, or networks to manipulate public discourse.
- **Deepfakes and Synthetic Media**
  AI-generated or manipulated media designed to mislead or damage reputations.
- **Election-related Disinformation**
  False information that may undermine electoral integrity or democratic institutions.
- **Content Harmful to Children**
  Sexual exploitation, grooming, or other forms of child abuse material.

C. Risk Indicators

Regulators should assess whether the content has the potential to cause systemic harm.

- Does the source of the harmful content have the power, reach, and capacity to amplify content?
- Does it target vulnerable or marginalized communities?
- Is the intent of the content possibly trigger violence, conflict, or social unrest?
- Does it occur during high-risk events such as elections, crises, or disasters?
- Is it part of a coordinated campaign or network activity?

D. Platform due diligence

Regulators should examine whether the platform has taken adequate measures.

- Has the platform reviewed its systems and processes when a systemic risk -such as a coordinated hate-speech campaign- arises?
- Has it provided clear labeling, contextualization, or warning notices?
- Has the platform reduced algorithmic amplification of the harmful content?
- Has the platform demonstrated risk-mitigation measures to prevent the virality of harmful content?
- Are transparent moderation policies applied consistently?
- Has the platform offered user reporting mechanisms?

E. User Protection and Remedies

Regulators should verify whether affected users have adequate protection.

- Users can report harmful content easily.
- Users receive clear explanations of moderation decisions.
- Users have access to a human-led appeals process.
- Vulnerable communities receive additional protection.

Annex-II

Harmful Content Classification Table for Regulators

Category	Definition	Examples	Risk Level	Possible Regulatory Response
1. Illegal Content	Content that clearly violates national law and international human rights standards. Platforms are legally required to remove or restrict such content.	Child sexual abuse material, terrorist propaganda, direct incitement to violence, explicit death threats, criminal fraud, illegal hate speech under national law.	Very High	Immediate removal or restriction by platforms; law enforcement involvement; regulatory oversight of platform compliance; transparency reporting.
2. Harmful but Legal Content	Content that does not violate the law but may cause serious harm to individuals, communities, or democratic processes.	Disinformation campaigns, hate speech not meeting legal threshold, harassment, coordinated manipulation, deepfakes, health misinformation, election misinformation.	High	Labeling, contextualization, algorithmic demotion, transparency requirements, risk assessments, user reporting mechanisms, regulatory monitoring.
3. Legitimate and Protected Expression	Content protected under freedom of expression and democratic discourse even if it is controversial or offensive.	Political criticism, satire, artistic expression, investigative journalism, advocacy for social change.	Low	No restriction. Ensure freedom of expression and prevent unjustified censorship.

Supporting Assessment Criteria for Regulators

When classifying content, regulators may consider the following questions:

Intent

- Is the content deliberately deceptive or manipulative?

Impact

- Does it risk causing harm to individuals, communities, or democratic institutions?

Reach

- Is the content widely amplified by platform and relevant community members algorithms?

Context

- Is it appearing during high-risk events such as elections, conflicts, or public health crises?

Target

- Does it target vulnerable or marginalized groups?

Annex-III
Harmful Content Decision Flowchart for Regulators

This decision chart is designed to enable regulators to understand that there is a fundamental difference between assessing pieces of content and assessing broader systematic risks. For individual pieces of content, the analysis is often relatively straightforward. The content may be determined to be either legal or illegal, with each outcome leading to a different process or response.

However, when it comes to harmful content that contributes to systemic risks, such as disinformation campaigns or coordinated hate speech campaigns, the assessment becomes much more complex. In these cases, the risk does not necessarily arise from a single piece of content, but rather from patterns, scale, amplification mechanisms, and cumulative effects. Hence, this flowchart is not a straightforward decision-making process and requires a much more nuanced framework than a simple binary decision tree.

START

↓

1. Is the content circulating on a digital platform accessible within the jurisdiction?

↓

2. Does the content potentially cause harm to individuals, communities, or democratic processes? (e.g., disinformation, hate speech, incitement)

↓

3. Does the content violate national law or internationally recognized human rights standards?

YES → Classify as ILLEGAL CONTENT → Notify platform for removal and consider

enforcement action.

NO→ Continue assessment

↓

4. Does the content pose significant societal risks even if it is legal?

(e.g., election disinformation, coordinated manipulation, harmful deepfakes)

YES → Classify as HARMFUL BUT LEGAL CONTENT

↓

5. Has the platform taken adequate mitigation measures?

- Labeling or contextualization
- Algorithmic demotion
- User reporting mechanisms
- Transparency disclosure

↓

6. If mitigation measures are inadequate?

→ Request transparency report

→ Require risk assessment or algorithmic audit

→ Issue regulatory recommendations or directives

↓

7. If content is controversial but lawful and poses minimal systemic risk?

→ Classify as LAWFUL BUT PROBLEMATIC CONTENT

→ Encourage factchecking, media literacy, and user empowerment tools

↓

END: Focus on SYSTEMIC PLATFORM ACCOUNTABILITY rather than policing individual content.

Annex IV

Case Studies

The objective of the case studies from Bangladesh, Nepal and Sri Lanka is to show how similar risks have been manifested in different context that illustrate systematic patterns. These studies also demonstrate why a purely content-based approach is inadequate in absence of examination of system process and safeguard mechanism. Hence, regulators need to understand that regulatory action never occurs in vacuum, and that risk related to content must be analyzed contextually and periodically.

a. Case Study- Bangladesh

The spread of lies and harmful content on digital platforms is a common phenomenon in the Bangladeshi digital ecosystem, as it is elsewhere in the world. The results of the dissemination of disinformation on digital platforms, including social media, are often disturbing, and they affect human lives and property. The following are two cases in which journalism organizations, religious places, and people were affected by the spread of lies on digital platforms, particularly social media. These two incidents drew national and international attention.

Case 1: Attack on *Prothom Alo* and *The Daily Star*

The offices of the country's two leading media organizations – *Prothom Alo* and The Daily Star came under violent mob attacks on 18 December 2025 New Age, 2025). An investigation jointly conducted by The Daily Star and Dismislab, a fact-checking organization, reveals that threats against both media outlets had been spreading on social media for months. Days before the attacks were made, these two media outlets were being labelled as Indian agents and anti-national forces on social media by many social media users. They even made calls to burn and attack the offices of these two media outlets (Amnesty International, 2026). According to a New Age news report, a mob entered the *Prothom Alo* office at around 11:00pm and vandalized it. Later, around 1:15am, the mob moved to the Daily Star office in the capital, and they vandalized glass panels, dragged out chairs, tables, and papers and set them on fire.

Case 2: Attacks on Buddhist monasteries, shrines and Buddhist houses

On September 29, 2012, an image depicting the desecration of a Quran, was posted on the wall of a Buddhist person's Facebook profile. It triggered a series of attacks

on Buddhist monasteries, shrines and Buddhist houses in Cox's Bazar, Bangladesh. Investigation later found that the picture that instigated the violence against the Buddhist community had been doctored (Business Standard, 2019). The BBC reports that an agitating mob set fire to homes and temples of the Buddhist community, forcing families to flee. A curfew was imposed as part of security measures. Police said the man accused of posting the image was tagged in the photo but did not post it himself on Facebook (BBC, 2012).

b. Case Study- Nepal

Social media platforms governance is becoming a crucial issue since 2023 in Nepal. There were continuous efforts by government to regulate the platforms: banning the TikTok, formulating directive, drafting bill, frequent call for registration and barring 26 platforms. Government steps invited wide criticisms from all corners of society. Platforms ignored the frequent call by the government to register in Nepal. Subsequently, government took strong move to ban 26 social media platforms in September 2025. The Gen Z protest erupted right away, and protest went violent and government was overthrown. Subsequently, a civilian government was formed that withdrew the social media bill, 2023 registered in parliament. Newly formed youth led party, Rastriya Swatantra Party, has got tremendous victory in recent election and new government was sworn in on 28 March 2026. It is widely observed that digital spaces were utilized during election campaigns which reflected strong digital democracy.

Chronicle

Government of Nepal banned TikTok on November 13, 2023, stating that its content was detrimental to social harmony. This marked Nepal's first major direct intervention against a global platform. TikTok was banned during festive days and right before the politically motivated protest program called by a controversial medical entrepreneur, known as pro-monarchist activist.

Alongside the ban, Nepal introduced *'Guidelines for Regulating the Use of Social Media, 2080 (2023)'*, requiring platforms to register, establish local contact points (which has 100,000 users), and comply with content regulation norms. This directive was widely criticized by journalists' associations, civil society groups, and international communities as well.

TikTok ban lifted after 283 days on August 22, 2024, as TikTok agreed to cooperate with authorities including monitoring misuse. TikTok officials were of the view that they had cooperated with the government to delete hundreds of improper videos from

the platforms upon the government request (Discussion program organized with TikTok officials by CDJMC on May 1, 2025). This reflected a shift toward conditional engagement rather than outright prohibition. Prior to the ban, there were 2.2 million TikTok users in Nepal. However, people were using it through virtual private network (VPN).

During TikTok banned period, Viber became the first to get registered in Nepal on March 7, 2024, despite the frequent call by the government. Other platforms straightly ignored the bell.

Controversial *social media Bill, 2025AD*

To regulate both social media companies (platforms) and individual users, the social media Bill, 2081 (Official name *Bill on the Operation, Use, and Regulation of social media*) was tabled in National Assembly on February 9, 2025. It aimed to provide a comprehensive legal framework for digital platforms, following the precedent set by the *Social Media Directives, 2023*. The Bill had the provisions for platforms of mandatory registration of all platforms, local presence with point of contact, content (harmful and illegal) takedown within specific timeframes, and taxation (local tax net). Likewise, it had provisions for users to have identity verification, strict provisions for spreading misinformation and cyberbullying, and heavy penalties for offenders with cash fines and prison tenure. Later, on February 2026 the bill was withdrawn from the National Assembly by Sushila Karki, who led civilian government formed after the Gen Z movement. There were 155 amendments (majority were by the ruling parties' parliamentarians) against the bill which was widely observed by national and international organizations including the UN agency UNESCO.

Mandatory registration order: August 25–28, 2025

Following a Supreme Court directive, the government issued a 7-day ultimatum to all social media platforms to register in Nepal and comply with regulatory requirements. Court directive was misinterpreted by the government.

Ban on 26 social media platforms: September 4, 2025

After non-compliance, Nepal blocked 26 major platforms (including Facebook, Facebook Messenger, Instagram, YouTube, WhatsApp, X, LinkedIn, Snapchat, Reddit, Pinterest, Signal, Threads, WeChat, Quora, Tumblr, Clubhouse, IMO, and Hamro Patro etc.). The move aimed to enforce sovereignty, accountability, and content control through registration and local oversight mechanisms.

Nationwide protests: September 8–9, 2025

Following the *'Nepo-kid'* trend which remained for a few weeks, and the ban triggered massive Gen Z protests across the country on September 8, with at least 19 deaths and hundreds injured. The shutdown was widely perceived as an attempt to suppress dissent. Although the government lifted the ban on the evening of September 8, with the resignation tendered by the then minister for Home Affairs due to the escalating unrest. On September 9, the protests spun out of control across the country with at least 57 deaths on second day alone. The Gen Z revolution costed high on human loss (76 including protesters and police), economic impact (84.5 billion Nepali rupee loss and damage), political shift and societal disruption (widespread looting, setting fire on government building, private residence and luxury hotels). Protestors vandalized and set fire at parliament buildings, the Supreme Court building and the Singha Durbar, central administrative building of the country. The crisis also led to resignation of KP Oli the then Prime Minister even having huge majority in parliament.

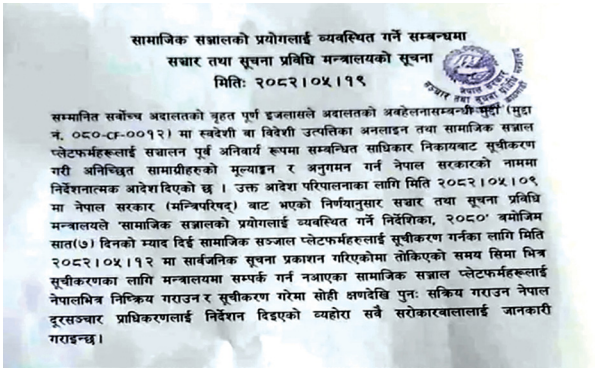
Implications of government steps

Nepal's regulatory efforts, including widely criticized bans seen as threats to free speech, sparked intense protests in 2025 that exposed deep government-youth distrust and led to political instability. These inconsistent policy reversals disrupted the economy, social communication, and key sectors like tourism, while ultimately strengthening digital political mobilization among youth. The recent election, youth and newly established political parties have gained the public support. It is widely observed that digital spaces have come to host significant discourse regarding democratic exercise of the country.

Despite public backlash, the government shifted toward a model of platform accountability requiring registration, local presence, and legal compliance reflecting a global trend. This evolution from individual platform bans to broader ecosystem regulation underscores the need to balance governance with transparency, rights, and public trust.

Notice issued for banning 26 social media platforms by Ministry for Communication

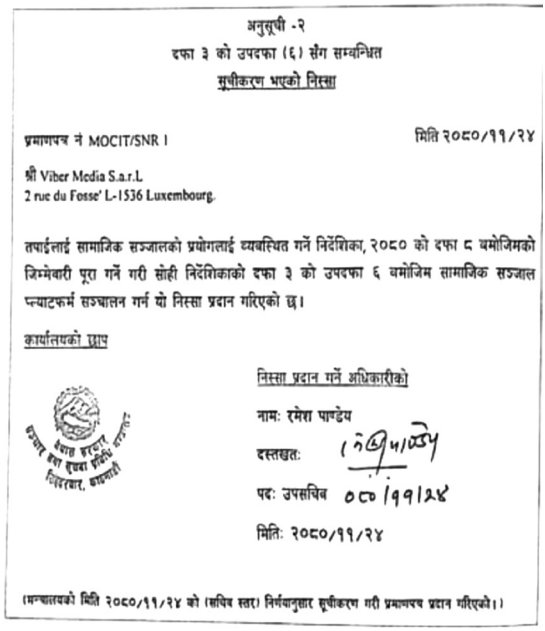
and Information Technology, Nepal



सामाजिक सञ्जालको प्रयोगलाई व्यवस्थित गर्ने सम्बन्धमा
सञ्चार तथा सूचना प्रविधि मन्त्रालयको सूचना
मितिः २०८२।०५।१९

सम्मानित सर्वोच्च अदालतको यहुत पूर्ण इजलासले अदालतको अवहेलनासम्बन्धी मुद्दा (मुद्दा नं. ०८०-CF-००१२) मा स्वदेशी वा विदेशी उत्पत्तिका अनलाइन तथा सामाजिक सञ्जाल प्लेटफर्महरूलाई सञ्चालन पूर्व अनिवार्य रूपमा सम्बन्धित साधिकार निकायबाट सूचीकरण गरी अनिच्छित सामाग्रीहरुको मूल्याङ्कन र अनुगमन गर्न नेपाल सरकारको नाममा निर्देशनात्मक आदेश दिएको छ । उक्त आदेश परिपालनाका लागि मिति २०८२।०५।०९ मा नेपाल सरकार (मन्त्रिपरिषद्) बाट भएको निर्णयानुसार सञ्चार तथा सूचना प्रविधि मन्त्रालयले 'सामाजिक सञ्जालको प्रयोगलाई व्यवस्थित गर्ने निर्देशिका, २०८०' बमोजिम सात(७) दिनको म्याद दिई सामाजिक सञ्जाल प्लेटफर्महरुलाई सूचीकरण गर्नका लागि मिति २०८२।०५।१२ मा सार्वजनिक सूचना प्रकाशन गरिएकोमा तोकिएको समय सिमा भित्र सूचीकरणका लागि मन्त्रालयमा सम्पर्क गर्न नआएका सामाजिक सञ्जाल प्लेटफर्महरूलाई नेपालभित्र निष्क्रिय गराउन र सूचीकरण गरेमा सोही क्षणदेखि पुनः सक्रिय गराउन नेपाल दूरसञ्चार प्राधिकरणलाई निर्देशन दिइएको व्यहोरा सबै सरोकारवालालाई जानकारी गराइन्छ।

Registration certificate of Viber on March 7, 2024.



अनुसूची -२
दफा ३ को उपदफा (६) सँग सम्बन्धित
सूचीकरण भएको निस्सा

प्रमाणपत्र नं MOCIT/SNR I

मिति २०८०/११/२४

श्री Viber Media S.a.r.L
2 rue du Fosse' L-1536 Luxembourg.

तपाईलाई सामाजिक सञ्जालको प्रयोगलाई व्यवस्थित गर्ने निर्देशिका, २०८० को दफा ८ बमोजिमको जिम्मेवारी पूरा गर्ने गरी सोही निर्देशिकाको दफा ३ को उपदफा ६ बमोजिम सामाजिक सञ्जाल प्लाटफर्म सञ्चालन गर्न यो निस्सा प्रदान गरिएको छ।

कार्यालयको छाप

निस्सा प्रदान गर्ने अधिकारीको
नामः रमेश पाण्डेय
दस्तखतः
पदः उपसचिव
मितिः २०८०/११/२४

(मन्त्रालयको मिति २०८०/११/२४ को (सचिव स्तर) निर्णयानुसार सूचीकरण गरी प्रमाणपत्र प्रदान गरिएको।)

c. Case Study- Sri Lanka

Freedom of Expression Under Strain in Contemporary Sri Lanka

Freedom of expression in Sri Lanka has come under increasing scrutiny in recent years, particularly in the context of political dissent, artistic expression, and digital communication. This case study examines four key instances: the media restrictions during the 2022 anti-government protests, the detention of journalists and activists for online speech, and two emblematic cases involving comedian Nathasha Edirisooriya and writer Shakthika Sathkumara. Together, these cases illustrate a broader pattern in which existing legal frameworks, especially those ostensibly designed to protect public order or prevent hate speech, are used in ways that risk undermining constitutionally guaranteed freedoms.

Media Blackout During the 2022 Anti-Government Protests

The 2022 "Aragalaya" protests represented a historic moment of mass civic mobilization in Sri Lanka, with demonstrators demanding political accountability amid economic collapse. However, the state's response raised serious concerns about freedom of expression. Authorities imposed emergency regulations and restricted media access, effectively creating a partial media blackout during critical moments of the protests.

In July 2022, protesters occupying Galle Face Green were forcibly evicted under emergency regulations. This action was later challenged before the Supreme Court. In a landmark 2025 judgment, the Court held by a 2–1 majority that the use of emergency powers to disperse a nonviolent protest violated fundamental rights, including freedom of expression and peaceful assembly (Balasuriya, 2025; Supreme Court of Sri Lanka, 2022).

This ruling affirmed that political protest constitutes protected expression under the Constitution. However, the initial suppression combined with limitations on media reporting, demonstrates how executive powers can be used to curtail information flows during politically sensitive periods.

In early 2025, U.S. President Donald Trump claimed on his social media platform that USAID (the United States Agency for International Development) had been used to spread chaos and change governments, specifically naming Sri Lanka as a recipient of such funds. Trump's post alleged that George Soros received $260,000,000.00 from USAID and used this money to spread chaos in Sri Lanka. This claim has been weaponized by local political actors in Sri Lanka to retroactively frame the 2022 protests as a foreign-orchestrated color revolution, providing a political justification

for the ongoing surveillance of civil society and independent media.

Detention of Journalists and Activists for Online Expression

Alongside restrictions on traditional media, authorities also targeted individuals for their online speech during and after the protests. Journalists, activists, and ordinary citizens faced arrest or intimidation for social media posts perceived as critical of the government.

These actions reflect a broader trend of digital surveillance and criminalization of dissent, where online platforms—once seen as spaces for democratic participation become sites of legal vulnerability. The use of laws such as the International Covenant on Civil and Political Rights (ICCPR) Act and provisions of the Penal Code have enabled authorities to frame dissenting speech as threats to public order or national harmony. This has had a chilling effect, discouraged open political discussion and weakened democratic accountability.

The Case of Nathasha Edirisooriya

The arrest of stand-up comedian Nathasha Edirisooriya in May 2023 highlights the precarious position of artistic expression in Sri Lanka. In her show *Modibhimanaya* ("Fool's Pride"), she made satirical remarks about Buddhist beliefs. Although she removed the content and issued an apology after public backlash, she was arrested and detained for several weeks under the ICCPR Act on charges related to incitement of hatred (Global Freedom of Expression, 2025).

In July 2023, the Colombo High Court granted her bail, citing insufficient grounds for continued detention (Wickramasinghe, 2023). The Human Rights Commission of Sri Lanka later found that her arrest and travel restrictions violated constitutional protections, including freedom of speech and equality before the law (Global Freedom of Expression, 2025).

This case underscores the expanding use of the ICCPR Act beyond its original purpose of preventing hate speech, raising concerns that it is being applied to suppress controversial but legitimate forms of expression.

The Case of Shakthika Sathkumara

The case of Shakthika Sathkumara further illustrates the risks faced by creative writers. In April 2019, Sathkumara was arrested for a short story titled *Ardha* ("Half"), which he shared on Facebook. The story explored sensitive themes, including homosexuality and abuse within a Buddhist monastic setting. Following complaints

by religious groups, he was detained for 127 days (about 4 months) under the ICCPR Act and the Penal Code (Amnesty International, 2021).

Although the Attorney General eventually dropped the case in 2021 without indictment (PEN International, 2025), the United Nations Working Group on Arbitrary Detention found that his arrest violated international law and called for compensation (Spector, 2020).

This case is particularly significant because it involves purely literary expression shared online, demonstrating how artistic content can be reclassified as criminal speech under broad legal interpretations.

Conclusion

These cases collectively reveal a concerning trajectory in Sri Lanka's approach to freedom of expression. While the Constitution formally guarantees this right, its practical realization is increasingly constrained by the expansive use of existing laws and regulations. The ICCPR Act, emergency regulations, and provisions of the Penal Code are being deployed not only to address genuine threats such as hate speech or violence, but also to target dissent, satire, and artistic expression.

The result is a chilling effect on public discourse, where individuals may self-censor to avoid legal repercussions. The Supreme Court's recognition of protest as protected expression offers an important counterbalance: yet systemic challenges remain. Overall, there is a clear and growing tendency toward using established legal frameworks as tools to curtail, rather than protect, freedom of expression in Sri Lanka.

References

AHN Legal. (n.d.). *Online media regulation in Nepal*. https://www.ahnlegal.com/public/legal-updates/legal/online-media-regulation-in-nepal

Amnesty International. (2021). *Sri Lanka: Writer detained for short story*.

Amnesty International. (2026). *Bangladesh: Meta's content moderation delays risk fuelling real-world violence*. Amnesty International News & Reports. Index: ASA 13/7623/2026. https://www.amnesty.org/en/latest/news/2026/03/bangladesh-metas-content-moderation-delays-risk-fuelling-real-world-violence/

Balasuriya, N. (2025). Supreme Court ruling on Galle Face protest case.

Bangladesh Telecommunication Regulatory Commission. (n.d.). *Bangladesh Telecommunication Regulatory Commission*. http://www.btrc.gov.bd

BBC. (2012). Bangladesh rampage over Facebook Koran image. 30 September 2012. https://www.bbc.com/news/world-asia-19780692

Business Standard. (2019). From Ramu to Borhanuddin: The same playbook used in inciting communal violence. 22 October 2019. https://www.tbsnews.net/bangladesh/ramu-borhanuddin-same-playbook-used-inciting-communal-violence

Digital Watch Observatory. (2024). *Sri Lanka: Online Safety Act No. 9 of 2024*. https://dig.watch/resource/sri-lankas-online-safety-act-no-9-of-2024

Global Freedom of Expression. (2025). *Case analysis: Nathasha Edirisooriya*.

Government of Bangladesh. (n.d.). *Government of the People's Republic of Bangladesh*. https://www.bangladesh.gov.bd

Government of Nepal. (n.d.). *Government of Nepal*. https://www.nepal.gov.np

International media monitoring discussions. (n.d.). *Media regulation and enforcement challenges in South Asia*.

NewAge. (2025). Prothom Alo, Daily Star offices attacked, set on fire. 19 December 2025. https://www.newagebd.net/post/country/285518/prothom-alo-daily-star-offices-attacked-set-on-fire

Parliament of Sri Lanka. (2024). *Online Safety Act, No. 9 of 2024*. https://www.parliament.lk

PEN International. (2025). *Sri Lanka drops charges against writer Shakthika Sathkumara*.
Press Council Nepal. (n.d.). *Press Council Nepal*. https://www.presscouncilnepal.gov.np

Sharma, R., & Bandara, D. (2022). Digital platform hegemony and freedom of expression in developing democracies: A comparative analysis of Sri Lanka, Nepal, and Bangladesh. *South Asian Media and Law Review*, *11*(3), 204–228. https://doi.org/10.1017/samlr.2022.204

Spector, J. (2020). UN Working Group on Arbitrary Detention opinion on Sri Lanka.

Supreme Court of Sri Lanka. (2022). *SCFR 246/2022 and related cases*.

Telecommunications Regulatory Commission of Sri Lanka. (n.d.). *Telecommunications Regulatory Commission of Sri Lanka*. https://www.trc.gov.lk

UN High Commissioner for Human Rights. (2013). *Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence* (A/HRC/22/17/Add.4). United Nations. https://www.ohchr.org/en/documents/thematic-reports/rabat-plan-action-annual-report

UNESCO. (2023). *Guidelines for the governance of digital platforms: Safeguarding freedom of expression and access to information through a multi-stakeholder approach*. UNESCO Publishing. https://unesdoc.unesco.org/ark:/48223/pf0000387339

UNESCO. (2024). *User empowerment and platform accountability: A guide for regulators*. UNESCO Document Repository. https://unesdoc.unesco.org/ark:/48223/pf0000395825

United Nations General Assembly. (1966). *International Covenant on Civil and Political*

Rights. United Nations Treaty Series, 999, 171. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

United Nations Human Rights Committee. (2011). *General comment no. 34: Article 19 (Freedoms of opinion and expression)* (CCPR/C/GC/34). United Nations. https://www.refworld.org/docid/4fe30dfb2.html

United Nations. (2011). *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*. Office of the High Commissioner for Human Rights (OHCHR). https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

Wickramasinghe, R. (2023). Colombo High Court bail decision in Edirisooriya case.

NOTES

NOTES

Toolkit for Regulators on Digital Platforms Governance

Based on the UNESCO Guidelines for the Governance of Digital Platforms

Published under the initiative **"Safeguarding Freedom of Expression and Access to Information through the Implementation of the UNESCO Guidelines for the Governance of Digital Platforms,"** jointly undertaken by Tribhuvan University, Nepal; Jahangirnagar University, Bangladesh; and the University of Vocational Technology, Sri Lanka, with the support of UNESCO.

Published by:

Central Department of Journalism and Mass Communication (CDJMC), Tribhuvan University, with the support of UNESCO

unesco
United Nations
Educational, Scientific
and Cultural Organization

UNIVOTEC