



POLICY BRIEF ON THE SOCIAL NETWORK BILL, 2081

Policy Brief *prepared by* **Body & Data**

July 2025

“The initiation of the bill is plausible... but it's not prepared with critical thought. The lack of clarity allows the government to penalise anyone, which is dangerous.”

- *Respondent*, Body & Data's **Survey on Social Network Bill** (2025)

Note for Readers

Why are we (Body & Data) advocating for awareness of and amendments to the Bill?

- As an organisation working to establish just, accessible and safe digital spaces, Body & Data has undertaken advocacy for the Social Network Bill to facilitate meaningful amendments and change the Bill to a form that directly addresses the actual needs of service providers, platforms and users in the digital space through lenses of human rights, marginalization, and decriminalization.
- Our approach to the Bill is informed primarily by the survey we conducted to understand public attitudes towards the Bill, the results and preliminary analysis of which can be accessed through this link: [Survey Results](#)

How can you (the reader) use this Policy Brief?

- This Policy Brief is meant to be an **introductory document** for the **general public, activists, advocacy groups, and policymakers**, allowing us to understand the following:

○ On the Bill:	(Headings in the Policy Brief)
■ scope and content of the Bill.....	Introduction & Overview
■ policy landscape in which the Bill has arrived.....	Policy Landscape & Contextual Analysis
○ On possible changes and amendments:	
■ ways in which we meaningfully transform the Bill.....	Potential for Value Creation

- Since the Bill, along with other laws and policies, is only officially available in Nepali, **we use both English and Nepali** throughout the Policy Brief for an easier understanding of the Bill.
- The Policy Brief draws on various sources to inform our analyses. While **publicly available sources are cited in the footnotes**, some sources and information will be formatted as follows for convenience:
 - **Analyses of Survey Results:** highlighted in **yellow**
 - **Examples:** highlighted in **purple**
 - **Section-wise notes:** highlighted in **red**
 - **Important Analyses:** Included in **pink** callout boxes
- The **suggestions and analyses** undertaken in this Policy Brief **are not exhaustive**, and we encourage readers to treat this Brief as a departure point for further research and inquisition.
- We've also compiled an explainer for first-time readers of the bill that you can access through this link: [Explainer](#)

Table of Contents

Note for Readers.....	3
Table of Contents.....	5
Preliminary.....	8
INTRODUCTION.....	8
OVERVIEW OF THE BILL.....	8
CHAPTER-1: PRELIMINARY.....	9
परिच्छेद-१: प्रारम्भिक.....	9
दफा १: संक्षिप्त नाम, प्रारम्भ र विस्तार (Short Name, Commencement, and Explanation).....	9
दफा २: परिभाषा (Definitions).....	9
CHAPTER-2: LICENSE FOR THE OPERATION OF SOCIAL NETWORK PLATFORMS.....	11
परिच्छेद-२: सामाजिक सञ्जाल प्लेटफर्म सन्चालन अनुमति.....	12
धारा ३: अनुमति पत्र लिनुपर्ने.....	12
धारा ४: अनुमतिपत्रको लागि निवेदन दिने (Application for License).....	13
धारा ५: निवेदन उपर छानबिन गर्ने (Review of Application).....	14
धारा ६: अनुमतिपत्रको प्रदान गर्ने (Provision of License).....	14
दफा ७: अनुमतिपत्रको अवधि र नवीकरण (Validity and Renewal of License).....	15
दफा ८: अनुमतिपत्रको खारेजी (Invalidation of License).....	16
दफा ९: प्लेटफर्म संचालनमा रोक लगाउनसक्ने (Prohibition on Operating Platforms).....	16
CHAPTER-3: INSTITUTIONAL ARRANGEMENTS.....	17
परिच्छेद-३: संस्थागत व्यवस्था.....	17
दफा १०: संस्थागत व्यवस्था (Institutional Arrangements).....	17
दफा ११: सम्बद्ध निकाय (Related Institutions).....	17
CHAPTER-4: Conditions to be abided by License Holders or Social Network Users.....	18
परिच्छेद-४: अनुमतिपत्र प्राप्त व्यक्ति वा सामाजिक सञ्जालको प्रयोगकर्ताले पालन गर्नु पर्ने शर्त.....	18
धारा १२: अनुमतिपत्र प्राप्त व्यक्तिले पालना गर्नु पर्ने शर्तहरू (Conditions that License Holders must Abide By).....	18
धारा १३: सामाजिक सञ्जाल प्लेटफर्मबाट विषयवस्तु हटाउन निर्देशन दिन सक्ने (Department to Direct Platform to Remove Content).....	19
धारा १५: अनुमतिपत्र प्राप्त व्यक्तिले गुनासो व्यवस्थापन गर्ने (License Holder to Handle Grievances).....	20
धारा १६: सामाजिक सञ्जाल प्रयोगकर्ताले पालना गर्नु पर्ने शर्त (Conditions that Users must Abide By).....	20

CHAPTER-5: Offences and Punishment.....	21
परिच्छेद-५: कसूर र सजाय.....	21
दफा १७-२७: कसूर तथा सजायहरू.....	21
दफा २८: थप सजाय हुने (Additional Punishment).....	23
दफा २९-३५: अन्य अपराधसँग सम्बन्धित तथा प्रक्रियागत व्यवस्थाहरू (Procedures Related to Other Crimes and Procedures).....	24
CHAPTER-6: MISCELLANEOUS.....	25
परिच्छेद-६: विविध.....	25
दफा ३६: द्रुत प्रतिकारी समूह गठन गर्ने (Formation of Rapid Response Team).....	25
दफा ३७: सचेतनामूलक कार्यक्रम सन्चालन गर्ने (Conducting Awareness Programs).....	25
दफा ३८-४१: सम्बद्ध निकायका अधिकार तथा दायित्व.....	26
How is our digital landscape changing?.....	27
POLICY LANDSCAPE & CONTEXTUAL ANALYSIS.....	27
Constitution of Nepal, 2072 (2015).....	27
Statutes.....	28
Nepal Telecommunications Act, 1997 (2053).....	28
Electronic Transaction Act, 2063 (2008).....	28
National Penal (Code) Act, 2074 (2017).....	29
Directive for Managing the Use of Social Networks, 2023.....	30
Information Technology and Cyber Security Bill, 2082 (2025).....	31
Policies & Guidelines.....	32
Science, Technology and Innovation Policy, 2075 (2019).....	32
Digital Nepal Framework, 2075 (2019).....	32
National Cyber Security Policy, 2080 (2023).....	32
National Information and Communication Technology Policy, 2072 (2015).....	32
Draft Policies.....	32
AI Policy, 2081 (2024).....	32
Personal Data Protection Policy, 2082 (2025).....	32
Other.....	32
[Repealed] Information Technology Bill, 2019.....	32
How can we critically engage with the Bill?.....	33
PROVISIONAL ANALYSIS.....	33
A. Legal Foundation and Selective Reform.....	33
B. Overbroad Non-Definitions and Arbitrary Powers.....	34
C. Impossibly Burdening the Business Ecosystem.....	35
D. Ignorance of Technology Facilitated Violence.....	36
E. Non-consideration of Marginalised Identities.....	36

F. Over-criminalisation and Crushing Fines.....	37
1. Arbitrary/Over-criminalisation.....	37
2. Restrictions on Anonymity.....	38
3. Metered Punishment.....	38
How and where do we lead the Bill?.....	39
POTENTIAL FOR VALUE CREATION.....	39
A. Envisioning a Feminist Internet.....	39
1. Special Protections for Marginalised Identities.....	39
2. Safeguards for Consensual Online Sexual Expression.....	40
3. Protections Against Technology-Facilitated Violence.....	40
4. Ensuring Accessibility for Disabled Persons.....	41
5. Approaching a Pleasure-Centric Internet.....	41
B. Adopting Rehabilitation and Facilitation.....	42
1. Human Rights-Based Legislation.....	42
2. Teachability over Disproportionate Fines.....	42
C. Simplifying Compliance for Businesses.....	43
D. Strengthening Digital Infrastructures.....	43
1. Independent Regulatory Bodies.....	43
2. Establishing Federal Bodies.....	43
3. Delimiting and Strengthening the “Department”	44
4. Duly and Equitably Established Rapid Response Team.....	44
E. Synthesising Legal Regimes.....	44
1. Bracing for Emerging Technologies.....	44
2. Furthering Private International Law.....	45
3. Defining Criminal Jurisdictions.....	45

Preliminary

INTRODUCTION

The **Social Network Bill, 2081, [“SNB”]** was introduced in the Upper House of the Federal Parliament by Minister Prithivi Subba Gurung on behalf of the Ministry of Communications and Information Technology. Approved by the Council of Ministers on Magh 7, 2081, the bill aims to regulate the use and operation of social media platforms.

The intended purpose of the bill is to facilitate the “correct” (सहि) and “regulated” (व्यवस्थित) use to uphold social harmony, religious tolerance, and good governance by holding social media platforms and users accountable and responsible.¹ The Bill also intends to make the operation and use of social networks more dignified, protected, and regulated.²

The Bill has come into force after the **Directives for Managing the Use of Social Networks, 2023**, was deemed *decidedly* insufficient³ to regulate the use of social networks in Nepal. It has since garnered significant criticism from civil society⁴ and international bodies⁵ for criminalising free political expression and imposing overbroad regulatory mechanisms. While public attitudes towards the Bill do not inspire confidence in the state’s ability to effectively regulate social networks, on account of our pervasive use of social networks, we can no longer postpone legal protections.

OVERVIEW OF THE BILL

The Bill has 6 Chapters and a total of 41 sections (provisions). All the provisions of the Bill have been tabulated (categorised when necessary) and graphically represented on a chapter-by-chapter basis for convenience.

¹ Social Network Bill, Theoretical Background, No.1 (2025) [SNB].

² Id.

³ The SNB enlists “The insufficiency of the existing Directive for Managing the Use of Social Networks, 2023 to regulate the use of social networks” as one of the reasons for the introduction of the Bill.

⁴ Bal Krishna Sah, [Social Media Bill Gets Heavy Criticism](#), The Himalayan (Jan 30, 2025);

⁵ [UNESCO Slams Social Media Bill for Overreach, Ambiguity](#), The Kathmandu Post (Mar. 19, 2025).

CHAPTER-1: PRELIMINARY

परिच्छेद-१: प्रारम्भिक

दफा १: संक्षिप्त नाम, प्रारम्भ र विस्तार (Short Name, Commencement, and Explanation)

दफा Section	उपदफा Sub-Section		प्रावधान
१	१	ऐनको संक्षिप्त नाम	"सामाजिक सञ्जाल ऐन, २०८१"
		Short Title	"Social Network Act, 2081"
१	२	प्रारम्भ	प्रमाणीकरण भएको मितिले एकसत्तीसौं दिनपछि प्रारम्भ
		Commencement	Act shall come into force on the thirty-first day following the date of its authentication
१	३	विस्तार	नेपालभर लागू हुनेछ र नेपाल बाहिरबाट नेपाल वा नेपाली नागरिकविरुद्ध यस ऐन बमोजिम कसुर गर्ने व्यक्तिको हकमा समेत लागू
		Scope of Application	Act shall be applicable throughout Nepal, and shall also apply to any person who commits an offence under this Act from outside Nepal against Nepal or a Nepali citizen

दफा २: परिभाषा (Definitions)

दफा Section	खण्ड Clause	शब्द Term	परिभाषा Definition
दर्ता & अनुमति Registration & Licensing			
२	क	अनुमतिपत्र	धारा ६ बमोजिमको सामाजिक सञ्जाल प्लेटफर्म सञ्चालन अनुमतिपत्र
		License	License to operate a social network platform as referred to in Section 6
२	ख	अनुमतिपत्र प्राप्त व्यक्ति	धारा ६ बमोजिम अनुमतिपत्र प्राप्त कम्पनी, फर्म वा संस्था
		License	A company, firm, or institution that has obtained a license pursuant to

		Holder	Section 6
संस्थागत व्यवस्थाहरु (सरकारी निकाय) Institutional Arrangements (Governmental Bodies)			
२	ङ	मन्त्रालय	नेपाल सरकारको सञ्चार तथा सूचना प्रविधि मन्त्रालय
		Ministry	Ministry of Communication and Information Technology of the Government of Nepal
२	च	विभाग	नेपाल सरकारको सूचना प्रविधि सम्बन्धी विषय हेर्ने विभाग
		Department	Department under the Government of Nepal responsible for matters related to information technology
२	ज	सम्बद्ध निकाय	धारा ११ बमोजिमका निकाय
		Related Agencies	Agencies as referred to in Section 11 of this Act
संस्थागत व्यवस्थाहरु (गैरसरकारी निकाय) Institutional Arrangements (Private Body)			
२	छ	सम्पर्क बिन्दु	धारा १४ बमोजिम अनुमतिपत्र प्राप्त व्यक्तिले नेपालमा स्थापना गरेको कार्यालय वा तोकिएको व्यक्ति
		Contact Point	An office established in Nepal or the designated person by the licensed person as referred to in Section 14 of this Act
नियन्त्रित विषयहरु Regulated Subjects			
२	घ	प्लेटफर्म	इन्टरनेट प्रयोगकर्ताका व्यक्ति-व्यक्ति, व्यक्ति र समूह वा संस्था, तथा समूह वा संस्थाबीच विचार वा जानकारी आदान-प्रदान गर्न वा सामाजिक अन्तरक्रिया गर्न सकिने गरी विद्युतीय प्रविधिको माध्यमद्वारा साइबर स्पेसमा सञ्चालन गरिएको एप, वेबसाइट, ब्लग, एआई टुल्स वा यस्तै प्रकारका सार्वजनिक रूपमा उपलब्ध सामाजिक सञ्जाल प्लेटफर्म
		Platform	app, website, blog, AI tools, or similar publicly available social network platforms that are operated in cyberspace using electronic means and allow users, including individuals, groups, or institutions to exchange information or ideas, or to engage in social interaction through the internet.

२	झ	सामाजिक सञ्जाल	कम्प्युटर, कम्प्युटर नेटवर्क, इन्टरनेटलगायतका विद्युतीय प्रविधि र उपकरणको माध्यमबाट उपलब्ध गराइएको सुविधा तथा प्रक्रिया बमोजिम कुनै व्यक्ति, समूह वा संस्थाबीच एक-आपसमा अन्तर्क्रियात्मक सञ्चार गर्ने वा विषयवस्तु (कन्टेन्ट) प्रसार गर्न सकिने प्रणाली
		Social Network	A system that enables interactive communication or dissemination of content among individuals, groups, or institutions using computers, computer networks, internet, and other electronic technologies and devices
नियन्त्रित कार्यहरू Regulated Actions			
२	ञ	सामाजिक सञ्जालको दुरुपयोग	यस ऐन वा प्रचलित कानून विपरीतका विषयवस्तु सामाजिक सञ्जालमा पोष्ट, सेयर, कमेन्ट, लाइभ स्ट्रिमिङ, रिपोर्ट, ट्याग, ह्यासट्याग, मेन्सन गर्ने वा यस्तै प्रकारको अन्य कार्य
		Misuse of Social Networks	Posting, sharing, commenting, live streaming, reporting, tagging, hashtagging, mentioning, or performing similar acts involving content on social networks that are contrary to this Act or prevailing laws
२	ट	सामाजिक सञ्जालको प्रयोग	व्यक्ति, समूह वा संस्थागत पहिचान बनाई कुनै अक्षर, चित्र, आवाज, संकेत, दृश्य वा श्रव्य-दृश्यलाई सार्वजनिक रूपमा प्रयोगमा आएको सामाजिक सञ्जालमा पोष्ट, सेयर, कमेन्ट, लाइभ स्ट्रिमिङ, रिपोर्ट, ट्याग, ह्यासट्याग, मेन्सन गर्ने वा यस्तै प्रकारको अन्य कार्य
		Use of Social Networks	Posting, sharing, commenting, live streaming, reporting, tagging, hashtagging, mentioning, or performing similar acts involving words, images, sounds, signs, visuals, or audiovisuals publicly on a social network using an individual, group, or institutional identity
अन्य Others			
२	ग	तोकिएको वा तोकिए बमोजिम	यस ऐन अन्तर्गत बनेको नियममा तोकिएको वा तोकिए बमोजिम
		Specified or as specified	As specified in the provisions of this Act

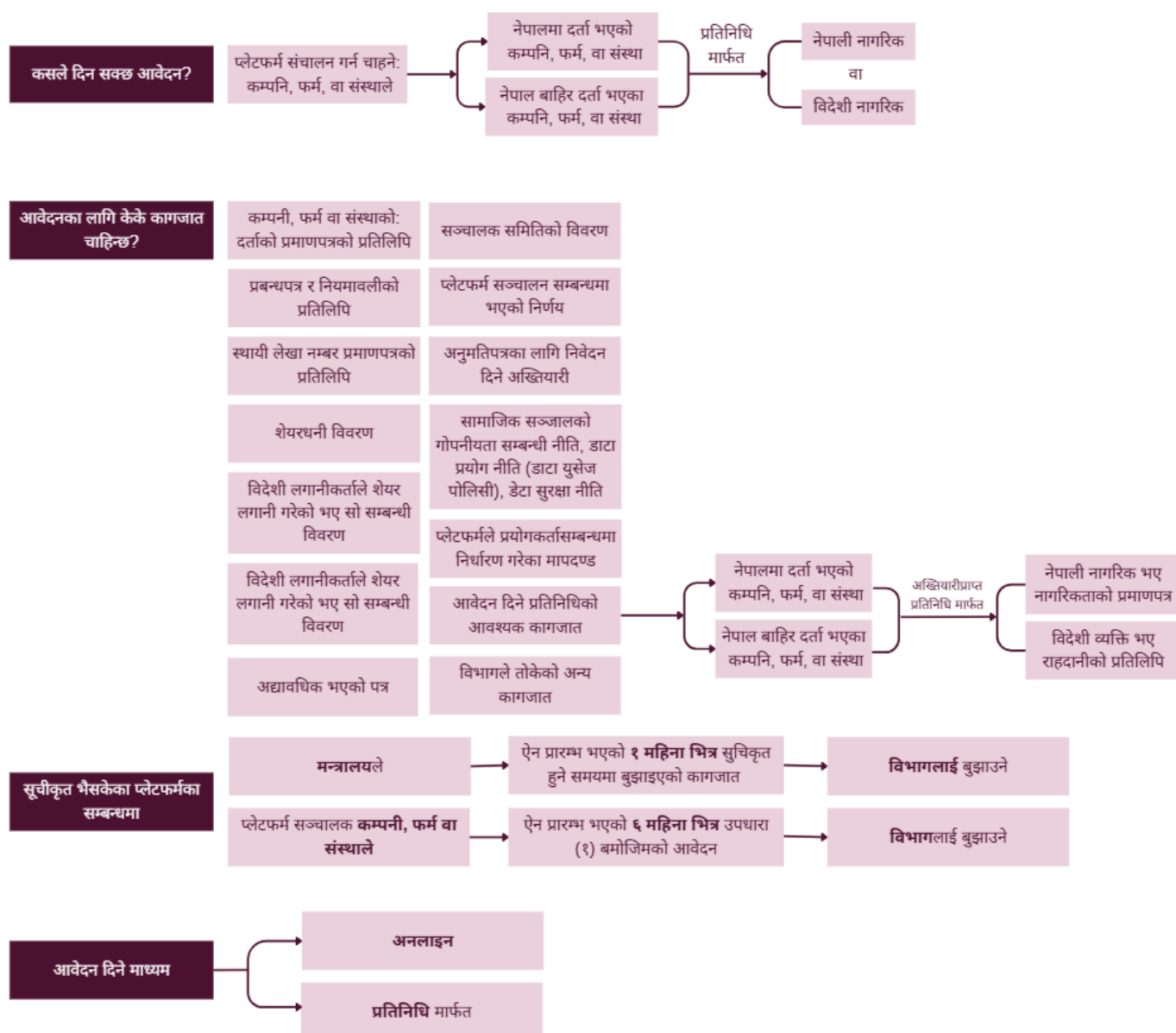
CHAPTER-2: LICENSE FOR THE OPERATION OF SOCIAL NETWORK PLATFORMS

परिच्छेद-२: सामाजिक सञ्जाल प्लेटफर्म सञ्चालन अनुमति

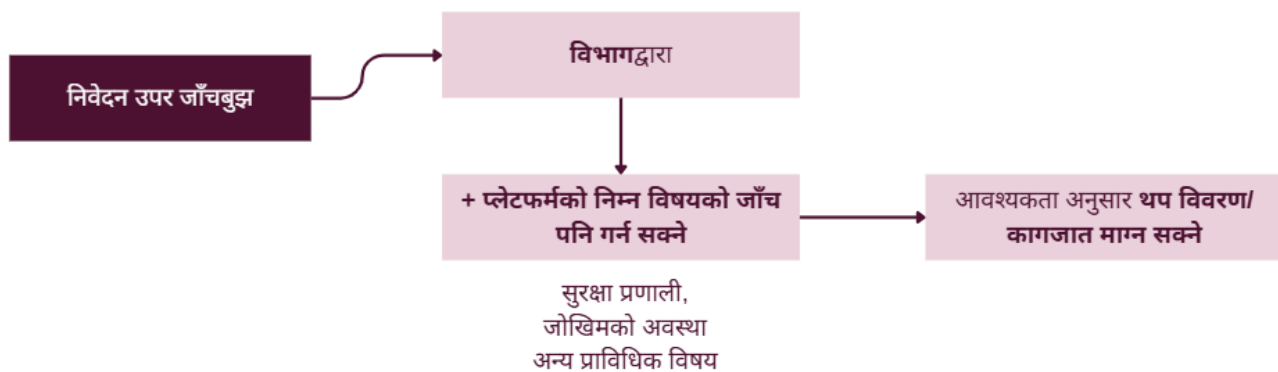
धारा ३: अनुमति पत्र लिनुपर्ने

प्लेटफर्म सञ्चालन गर्न चाहने कम्पनी, फर्म वा संस्थाले यस ऐन बमोजिम प्लेटफर्म सञ्चालन गर्न अनुमतिपत्र लिनुपर्नेछ।

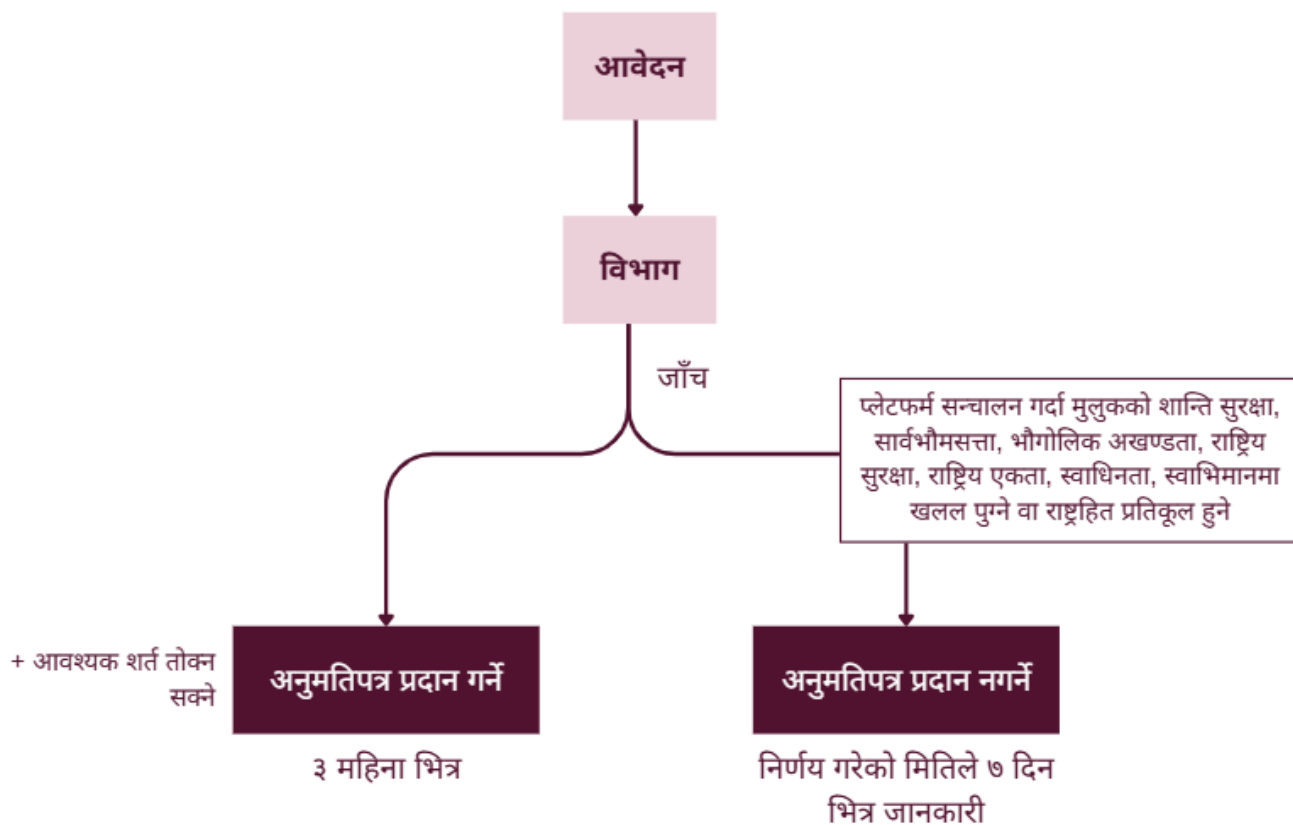
धारा ४: अनुमतिपत्रको लागि निवेदन दिने (Application for License)



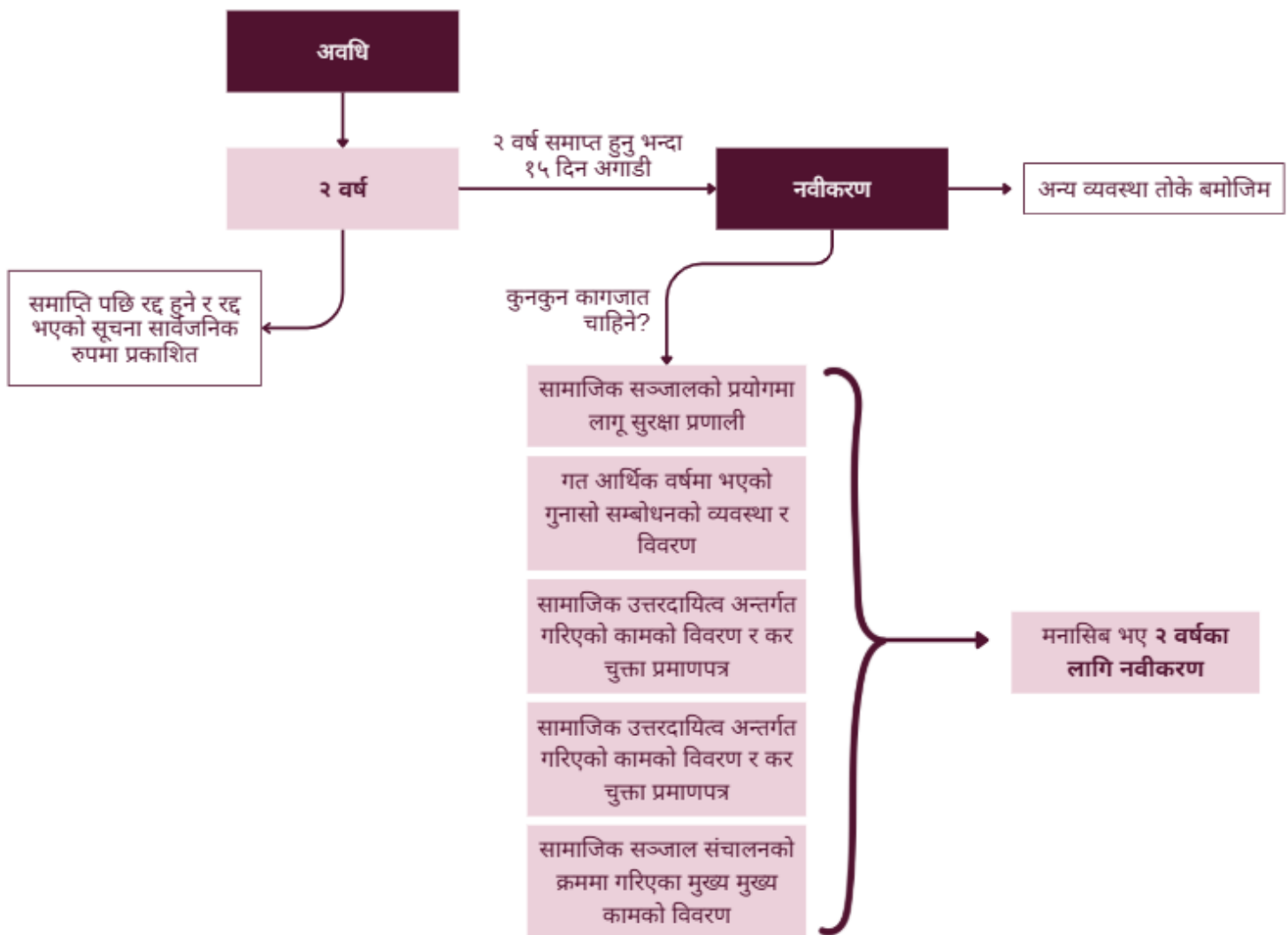
धारा ५: निवेदन उपर छानबिन गर्ने (Review of Application)



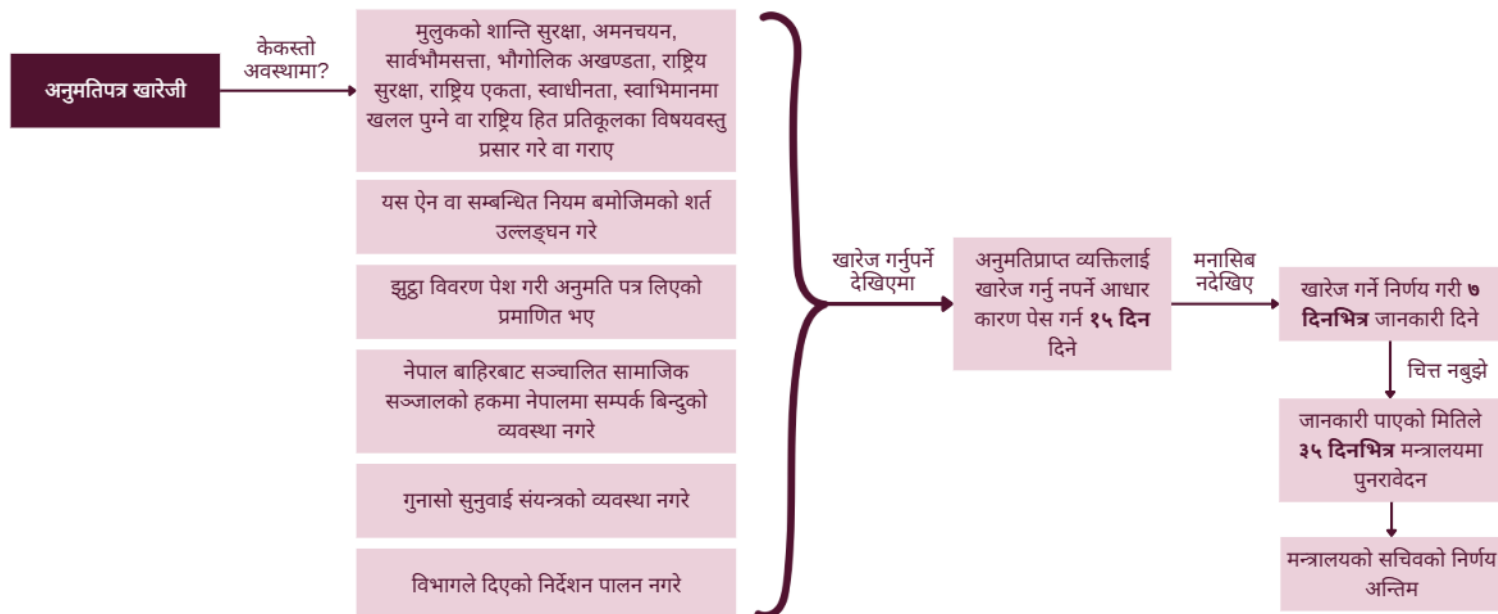
धारा ६: अनुमतिपत्रको प्रदान गर्ने (Provision of License)



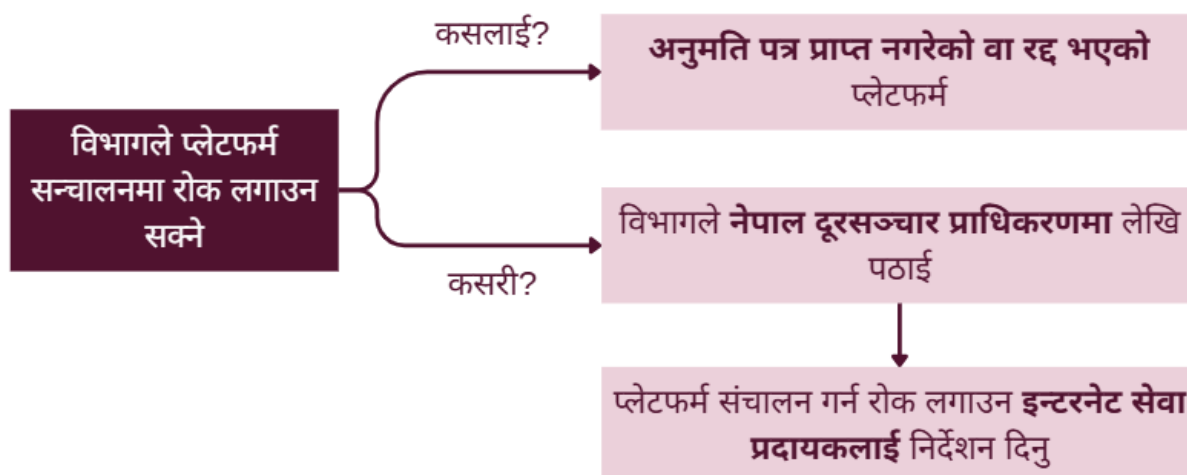
दफा ७: अनुमतिपत्रको अवधि र नवीकरण (Validity and Renewal of License)



दफा ८: अनुमतिपत्रको खारेजी (Invalidation of License)



दफा ९: प्लेटफर्म संचालनमा रोक लगाउनसक्ने (Prohibition on Operating Platforms)



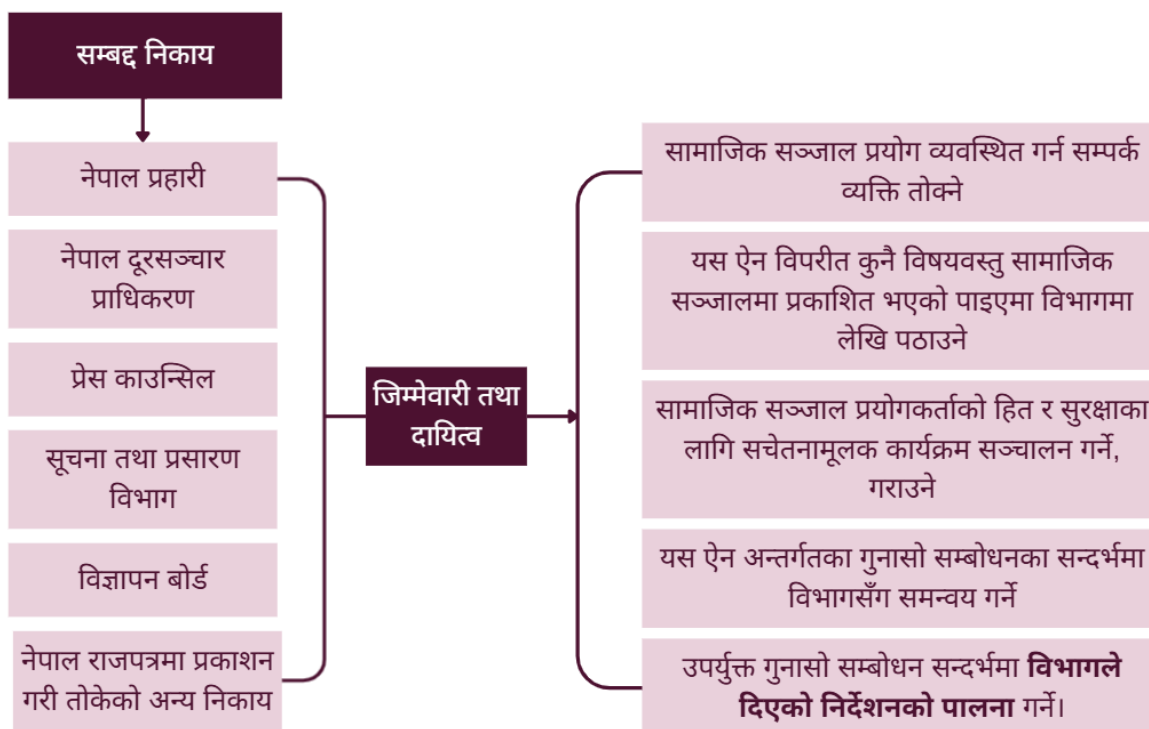
CHAPTER-3: INSTITUTIONAL ARRANGEMENTS

परिच्छेद-३: संस्थागत व्यवस्था

दफा १०: संस्थागत व्यवस्था (Institutional Arrangements)

विभागको काम, कर्तव्य र अधिकार	
प्लेटफर्मको सञ्चालन र प्रयोगसम्बन्धी नीतिगत, कानुनी तथा संस्थागत सुधारका लागि मन्त्रालयमा प्रतिवेदन पेश गर्ने	सामाजिक सञ्जाल प्रयोग सम्बन्धमा आएका गुनासोहरूको व्यवस्थापन गर्न आवश्यक व्यवस्था गर्ने
प्लेटफर्ममा प्रकाशित विषयवस्तुको नियमित रूपमा अनुगमन गर्ने	सामाजिक सञ्जालको सञ्चालन र प्रयोगसम्बन्धी सचेतनामूलक कार्यक्रम सञ्चालन गर्ने
अनुगमन गर्दा यस ऐन वा प्रचलित कानून बमोजिम प्रसारण गर्न अयोग्य ठहरिएका विषयवस्तु हटाउन सम्बन्धित प्लेटफर्मलाई निर्देशन दिने	प्लेटफर्म सञ्चालन, प्रयोग तथा नियमनसम्बन्धी सम्बन्धित निकायसँग समन्वय गर्ने
प्लेटफर्ममा पोस्ट वा सेयर भएका विषयवस्तु यस ऐन वा प्रचलित कानून विपरीत भएमा त्यस्ता विषयवस्तुको प्रकृति, असर र प्रभाव हेरी आवश्यक कारबाहीका लागि सम्बन्धित निकायमा पठाउने	तोकिएअनुसार अन्य कार्य गर्ने

दफा ११: सम्बद्ध निकाय (Related Institutions)



CHAPTER-4: Conditions to be abided by License Holders or Social Network Users

परिच्छेद-४: अनुमतिपत्र प्राप्त व्यक्ति वा सामाजिक सञ्जालको प्रयोगकर्ताले पालन गर्नु पर्ने शर्त

धारा १२: अनुमतिपत्र प्राप्त व्यक्तिले पालना गर्नु पर्ने शर्तहरू (Conditions that License Holders must Abide By)

अनुमतिपत्र प्राप्त व्यक्तिले पालना गर्नुपर्ने शर्त

नेपालको सार्वभौमसत्ता, भौगोलिक अखण्डता, राष्ट्रिय सुरक्षा, एकता, स्वतन्त्रता, स्वाभिमान वा राष्ट्रिय हितमा आँच पुग्ने तथा सामाजिक, सांस्कृतिक वा धार्मिक सद्भाव भङ्काउने विषयवस्तु प्रसारण नगर्ने

प्रचलित कानून विपरीतका विषयवस्तु पोस्ट वा सेयर हुन नदिन प्लेटफर्ममा आवश्यक प्रविधि विकास गर्ने वा आवश्यक उपाय अवलम्बन गर्ने

कुनै व्यक्तिको चरित्रहत्या गर्ने खालका सामग्री, घृणास्पद भाषा, हिंसा भङ्काउने वा साम्प्रदायिक सद्भाव बिगार्ने खालका सामग्री अपलोड वा प्रचार प्रसार गर्न नदिने

प्रचलित कानूनले तोकेको अवस्थाबाहेक सामाजिक सञ्जाल प्रयोगकर्ताको व्यक्तिगत विवरणको गोपनीयता र बौद्धिक सम्पत्तिसम्बन्धी अधिकारको संरक्षण गर्ने

प्रयोगकर्ताको भलाइ र सुरक्षाका लागि आवश्यक सूचना तथा जनचेतनामूलक सामग्री निरन्तर प्रसारण गर्ने

प्रयोगसम्बन्धी आएका गुनासोको व्यवस्थापन गर्ने

प्रसारित सामग्रीको तथ्य परीक्षण गर्ने

प्रयोगकर्ताको वास्तविक परिचय लिई मात्र प्लेटफर्म प्रयोग गर्न दिने

प्लेटफर्ममा हुने आर्थिक कारोबार बैङ्किङ प्रणालीमार्फत मात्र हुने सुनिश्चितता गर्ने

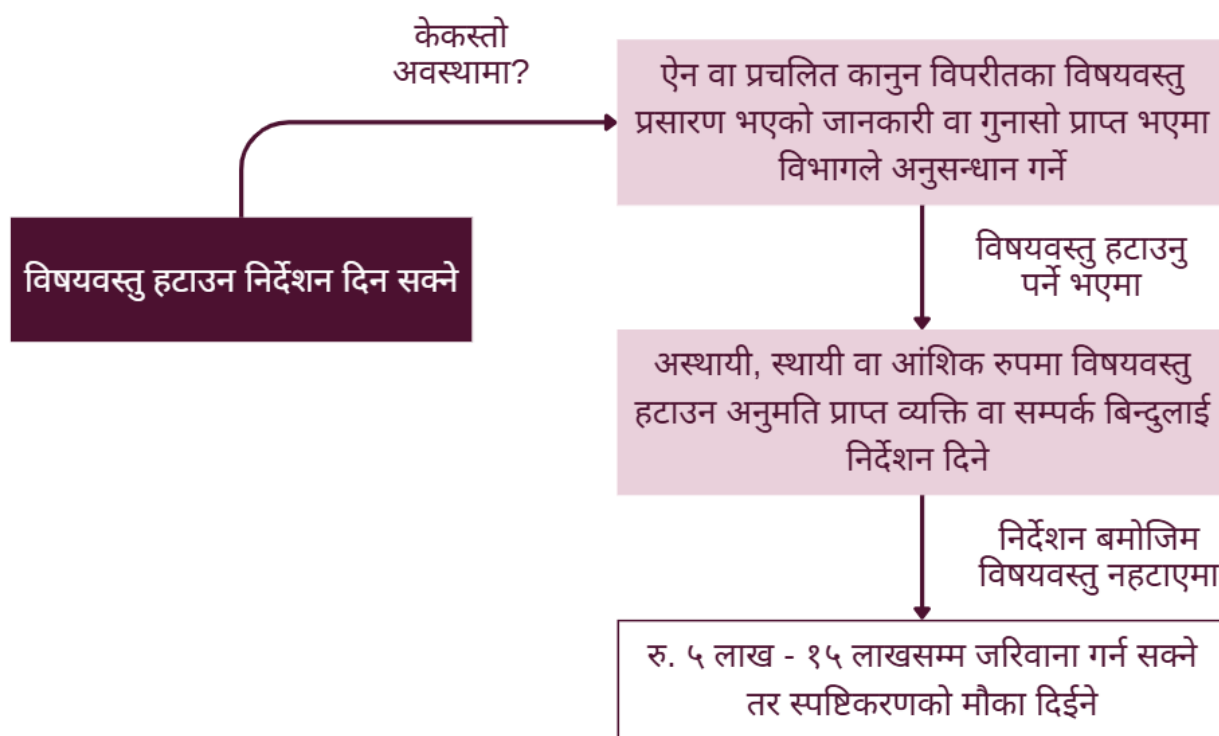
अनुसन्धान प्रयोजनको लागि प्रयोगकर्ताको विवरण सम्बन्धित निकायलाई उपलब्ध गराउने

अनुमतिपत्रमा उल्लेखित शर्तहरू

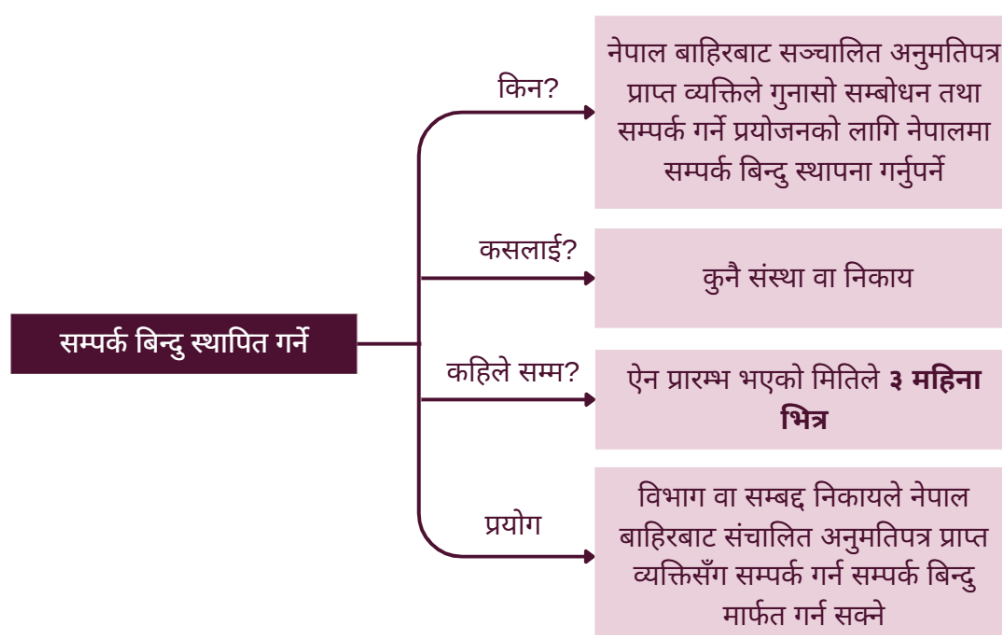
तोकिएअनुसार अन्य शर्तहरू

यी शर्त पालाना नगरेमा, विभागले **रु. २५ लाख - १ करोड सम्म** जरिवाना गर्न सक्छ, र यसरी जरिवाना तिर्नु पर्दा, सम्बन्धित व्यक्तिलाई स्पष्टिकरण दिने मौका दिनुपर्छ

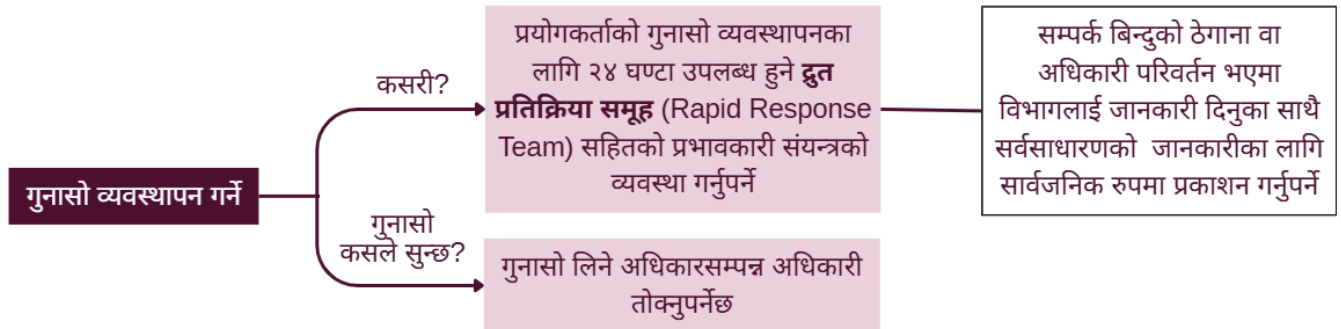
धारा १३: सामाजिक सञ्जाल प्लेटफर्मबाट विषयवस्तु हटाउन निर्देशन दिन सक्ने (Department to Direct Platform to Remove Content)



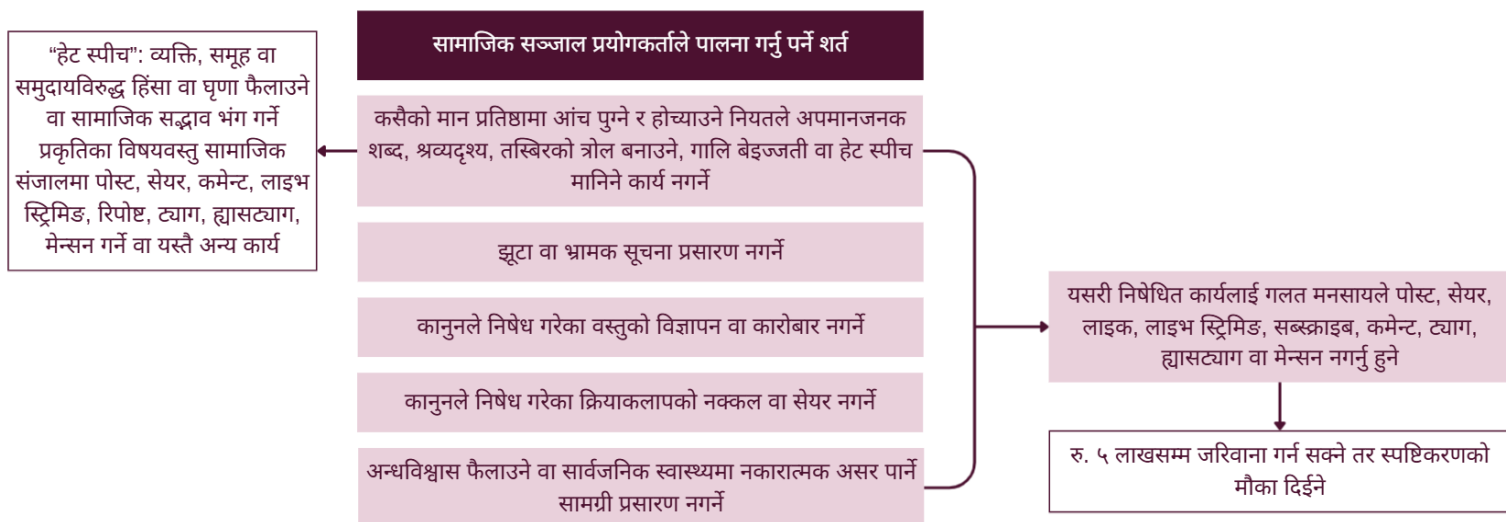
धारा १४: सम्पर्क बिन्दुको व्यवस्था गर्नुपर्ने



धारा १५: अनुमतिपत्र प्राप्त व्यक्तिले गुनासो व्यवस्थापन गर्ने (License Holder to Handle Grievances)



धारा १६: सामाजिक सञ्जाल प्रयोगकर्ताले पालना गर्नु पर्ने शर्त (Conditions that Users must Abide By)



CHAPTER-5: Offences and Punishment

परिच्छेद-५: कसूर र सजाय

दफा १७-२७: कसूर तथा सजायहरू

दफा	अपराध	प्रावधान	सजाय (जरिवाना वा दुबै)	
			कैद	जरिवाना
१७	अनुमतिपत्र नलिई वा रोक लगाएको सामाजिक सञ्जाल प्लेटफर्म संचालन			२५ लाख
१८	राष्ट्र हित प्रतिकूल हुने कार्य	नेपालको सार्वभौमसत्ता, भौगोलिक अखण्डता, राष्ट्रिय सुरक्षा, राष्ट्रिय एकता, स्वाधीनता, स्वाभिमान वा राष्ट्र हित वा सङ्घीय इकाईबीचको सु-सम्बन्धमा प्रतिकूल हुने गरी वा वर्गीय, जातीय, धार्मिक, सांस्कृतिक, क्षेत्रीय, साम्प्रदायिक, यस्तै आधारमा घृणा वा द्वेष उत्पन्न हुने काम गर्ने गराउने वा विभिन्न जात, जाति वा सम्प्रदायबीचको सु-सम्बन्धमा खलल पार्ने विषय सामाजिक सञ्जालमा प्रसारण	५ वर्ष सम्म	५ लाख सम्म
१९	साइबर बुलिङ	इन्टरनेट जडान भएको डिजिटल उपकरणको माध्यमबाट सामाजिक सञ्जाल प्रयोग गरी साइबरस्पेसमा गलत वा हानिकारक वाक्य, अक्षर, चिन्ह, चित्र, तस्बिर, स्केच, फोटो, अडियो, भिडियो, श्रव्य-दृश्य, सङ्केत वा संदेश पठाउने, पोष्ट गर्ने, सेयर गर्ने वा सोहि कार्यबाट कसैलाई सताउने, तर्साउने, धम्काउने, लज्जित गराउने, अपमान गर्ने, मानमदन गर्ने वा अफवाह फैलाउने जस्ता कार्य	२ वर्ष सम्म	रु. ३ लाख सम्म
२०	साइबर स्टकिङ	इन्टरनेट प्रविधिको प्रयोग गरी कसैलाई झुठ्ठा आरोप लगाउने, धम्की दिने, जालसाजी गर्ने, दुर्व्यहवार गर्ने, निगरानी गर्ने, व्यैक्तिक गोपनियता भङ्ग गर्ने, बारम्बार अनावश्यक सन्देश पठाउने, गोप्य जानकारी खुलासा गर्ने वा वैयक्तिक सुरक्षामा खतरा पुर्याउने कार्य गरी कसैलाई हैरानी दिएमा	३ वर्ष सम्म	रु. ५ लाख सम्म

२१	आईडी तथा सूचना हत्याक	कसैको कम्प्युटर प्रणाली वा सामाजिक सञ्जालको पासवर्ड वा सिरियल नम्बर क्रयाक गरी त्यस्तो कम्प्युटर प्रणाली वा सामाजिक सञ्जालको गुप्त सङ्केत, पासवर्ड वा सिरियल नम्बर चोरी गरी त्यस्तो कम्प्युटर प्रणाली वा सामाजिक सञ्जालमा अनधिकृत रूपमा पहुँच प्राप्त गरी तथ्याङ्क भण्डारमा हस्तक्षेप गर्ने कार्य	३ वर्ष सम्म	रु. १५ लाखसम्म
२२	फिशिङ वा इम्पोस्टर स्क्याम	फिसिङ: विधुतीय सञ्चार माध्यमबाट कुनै कुरा सत्य हो भन्ने विश्वासमा पारी कुनै व्यक्तिको युजरनेम र पासवर्ड, क्रेडिट कार्ड नम्बर, बैंक एकाउन्ट जस्ता संवेदनशील सूचना प्राप्त गर्ने कार्य इम्पोस्टर स्क्याम: कसैबाट पैसा वा व्यक्तिगत विवरण चोर्ने उद्देश्यले फोन वा ईमेल वा विधुतीय उपकरण वा प्रणालीद्वारा आफू चिनजान भएको वा विश्वासयोग्य व्यक्ति भएको भन्ने विश्वासमा पारी उपहार वा पुरस्कार पठाउन व्यक्तिगत पासवर्ड र संवेदनशील जानकारी लिएर पछि कुनै रकम माँग गर्ने कार्य सम्झनु पर्छ	३ वर्ष सम्म	रु. १५ लाख सम्म
२३	सेक्सटोर्सन वा एक्सटोर्सन	सेक्सटोर्सन: कसैको नितान्त व्यक्तिगत तथा निजी तस्बीर अडियो वा भिडियो सामाजिक सञ्जालको प्रयोग गरी सार्वजनिक गर्ने वा कसैसँग सेयर गर्ने धम्की दिई यौन शोषण, आर्थिक लाभ वा हिंसाका लागि बाध्य पार्ने कार्य एक्सटोर्सन: कसैले कुनै व्यक्तिलाई सामाजिक सञ्जालको प्रयोग गरी निज वा अरु कसैलाई कुनै क्षति पुर्याउने डर त्रासमा पारी निजबाट बेइमानीपूर्वक आफ्नो वा अरु कसैका लागि कुनै लाभ उठाएमा वा त्यस्तो लाभ उठाउने नियतले कुनै काम गराउने कार्य	३ वर्ष सम्म	रु. १५ लाख सम्म
२४	बीभत्स तस्बीर वा अडियो वा भिडियो पोस्ट वा सेयर	सामाजिक सञ्जालमा बीभत्स तस्बिर वा अडियो वा भिडियो पोष्ट वा सेयर गर्ने	३ महिना	रु. ५० हजार सम्म
२५	अश्लील, मिथ्या वा भ्रामक सामग्री	सामाजिक सञ्जालको प्रयोग गरी अश्लील शब्द, तस्बिर, सङ्केत, भिडियो, अडियो, मिथ्या वा भ्रामक सूचना प्रसार गर्ने, त्यस्तो सूचनाको दुष्प्रचार वा तौडमरोड वा कमेन्ट गरी प्रसार	२ वर्ष सम्म	रु. ३ लाख सम्म
२६	डिपफेक भिडियो अपलोड वा प्रसार	आर्टिफिसियल इन्टेलिजेन्सको प्रयोग गरी कुनै व्यक्तिको अनुहार, आवाज वा हाउभाउलाई नेक्कल वा प्रतिस्थापन गरी गलत सूचना प्रवाह गर्ने, अश्लीलता फैलाउने वा चरित्रहत्या गर्ने कार्य	२ वर्ष सम्म	रु. ३ लाख सम्म
२७ (१)	बेनामी वा छद्मभेषी पहिचान बनाउनु वा प्रयोग गर्नु	सामाजिक सञ्जालमा बेनामी वा छद्मभेषी (फेक आइडी, पेज, समूह) वा अरुको नामबाट पहिचान गर्ने, त्यस्तो बेनामी वा छद्मभेषी पहिचान मार्फत विषयवस्तु उत्पादन गरी पोष्ट वा सेयर गर्ने, अरुको विषयवस्तु सेयर गर्ने, कमेन्ट वा कल गर्ने कार्य	३ महिना	रु. ५० हजार सम्म

२७(२)	(छद्म पहिचानमार्फत राष्ट्रविरोधी सामाग्री सम्प्रेषण)	प्लेटफर्ममा व्यक्तिगत वा सामूहिक रूपमा छद्मभेषी, स्थायी वा अस्थायी समूह, पेज वा अन्य कुनै प्रकारको आइडी खोली नेपालको सार्वभौमसत्ता, भौगोलिक अखण्डतामा खलल पुग्ने वा राष्ट्रिय हित प्रतिकूल हुने गरी गलत वा भ्रामक सूचना सम्प्रेषण	प्रचलित कानून अनुसार र व्यवस्था नभए:	
			५ वर्ष सम्म	रु. १५ लाख सम्म

दफा २८: थप सजाय हुने (Additional Punishment)

थप सजाय हुने	
कसैले सामाजिक सञ्जालको प्रयोग गरी कसूर वा कसूर गर्न <u>दुरुत्साह</u> न गरे	हुने सजाय + थप १ वर्ष
यस ऐन बमोजिम पटके कसूर गरेको भए	पटकै पिच्छे दोब्बर सजाय
सार्वजनिक पद धारण गरेको वा राज्य कोषबाट सुविधा लिएको व्यक्तिले कसूर गरेमा	ऐनको सजाय + ५०%
बालबालिकाको प्रयोग गरेर ऐन बमोजिम कसूर गरे	थप १ वर्ष

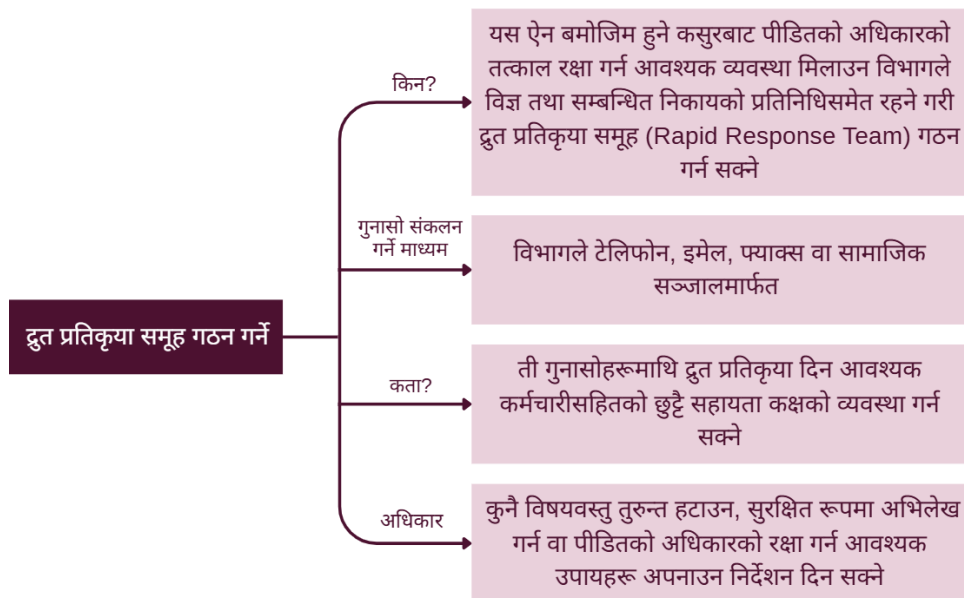
दफा २९-३५: अन्य अपराधसँग सम्बन्धित तथा प्रक्रियागत व्यवस्थाहरू (Procedures Related to Other Crimes and Procedures)

दफा	अपराध	प्रावधान	परिणाम/सजाय/ हदम्याद
२९	दुरुत्साहन, उद्योग वा षड्यन्त्र गर्न नहुने	यस ऐन बमोजिम कसूरजन्य कार्य गर्न कसैलाई दुरुत्साहन गर्ने वा त्यस्तो कसूरको उद्योग वा षड्यन्त्र गर्ने वा त्यस्तो कसूर गर्न सघाउने वा अन्य कुनै व्यहोरा ले मतियार भई कार्य गर्ने व्यक्तिलाई	मुख्य कसूरदारलाई हुने सजायको आधा सजाय
३०	प्रचलित कानून बमोजिम सजाय गर्न बाधा नपर्ने	यस ऐन अन्तर्गत कसूर ठहरिने कुनै कार्य अन्य कानून बमोजिम सजाय हुने कसूर भई, त्यस कानून अन्तर्गत यस ऐन भन्दा बढी सजाय हुने भए कानून बमोजिम कारवाही गर्न सकिने	
३१	क्षतिपूर्ति भराउनु पर्ने	यस ऐन अन्तर्गत कसूर घटेपछि, कसैलाई हानि, नोक्सानी, हैरानी वा क्षति भएको खण्डमा कसूरदारले क्षतिपूर्ति दिनु पर्ने	
३२	नेपाल सरकार वादी हुने	मुलुकी फौजदारी कार्यविधि संहिता २०७४, अनुसूची १ बमोजिम	
३३	हदम्याद	मर्का पर्ने व्यक्तिले कसूर भए गरेको थाहा पाएको मितिले	३ महिना भित्र
३४	विधुतीय प्रमाणको ग्राह्यता	विधुतीय प्रणालीबाट सिर्जना भएको विधुतीय वा अन्य कुनै स्वरूपमा रहेको कुनै सूचना वा तथ्याङ्क मुद्दाको कारवाहीमा प्रमाणको रूपमा ग्राह्य हुने	
३५(१)	पुनरावेदन	(अपराध) यस ऐन बमोजिम जिल्ला अदालतले गरेको निर्णयमाथि थाहा पाएको मितिले ३५ दिन भित्र उच्च अदालतमा पुनरावेदन	३५ दिन
३५(२)		(जरिवाना) विभागले दफा १२, १३ र १६ बमोजिम (अनुमतिप्राप्त व्यक्ति, प्लेटफर्म, सामाजिक सञ्जाल प्रयोगकर्ताले पालना गर्नु पर्ने शर्त पालना नगरेको खण्डमा) गरेको निर्णयमाथि जिल्ला अदालतमा ३५ दिनमा पुनरावेदन लाग्ने	३५ दिन

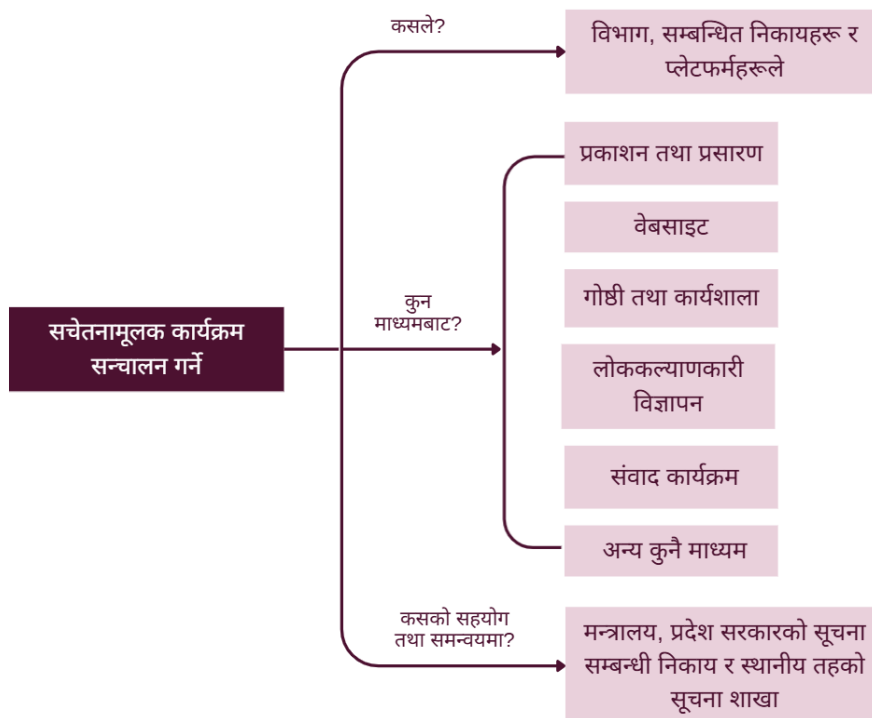
CHAPTER-6: MISCELLANEOUS

परिच्छेद-६: विविध

दफा ३६: द्रुत प्रतिकारी समूह गठन गर्ने (Formation of Rapid Response Team)



दफा ३७: सचेतनामूलक कार्यक्रम सन्चालन गर्ने (Conducting Awareness Programs)



दफा ३८-४१: सम्बद्ध निकायका अधिकार तथा दायित्व

दफा	अधिकार/दायित्व	प्रावधान
३८	निर्देशन दिन सक्ने	मन्त्रालयले → विभागलाई सामाजिक सञ्जालको संचालन र प्रयोगलाई व्यवस्थित गर्ने सम्बन्धमा विभागलाई निर्देशन दिन सक्ने
३९	प्रतिवेदन पेश गर्नुपर्ने	विभागले → मन्त्रालयसमक्ष यस ऐन र सम्बन्धित नियम बमोजिम आफू र सम्बद्ध निकायको कामको वार्षिक प्रतिवेदन पेश गर्नुपर्ने
४०	नियम बनाउने अधिकार	आवश्यकता अनुसार नेपाल सरकारले बनाउन सक्ने
४१	निर्देशिका वा कार्यविधि बनाउन सक्ने	मन्त्रालयले आवश्यकता अनुसार

How is our digital landscape changing?

POLICY LANDSCAPE & CONTEXTUAL ANALYSIS

In this section, we will contextualise the SNB against prevailing laws, policies, and Bills under consideration in the Federal Parliament. As one of our respondents said, “It [SNB] should be studied in the larger trend of digital regulations... This bill is problematic and distracts from broader concerns about digital rights in Nepal”.

Constitution of Nepal, 2072 (2015)

Article 17 of the Constitution guarantees the fundamental right of every person to their personal liberty.- includes the freedom of opinion and expression. However, Article 17(2)(1) of the constitution lays twenty distinct grounds for curtailing freedom of opinion and expression. These grounds can be broadly categorized into eight areas:

- National Sovereignty, Territorial Integrity, National Security, Nationality, and Independence of Nepal
- Harmonious Relations Among People (between Federal Units, and people of various castes)
- Caste-Based Discrimination
- Disrespect of Labor
- Defamation
- Contempt of Court
- Incitement to an Offense
- Acts Against Public Decency and Morality

Article 19 protects the **right to communication** through publications, broadcasting or dissemination of news item, editorial, feature article or other reading, audio, and audio-visual material through any means including electronic publication from censorship. **Article 19(1)** allows similar grounds of restrictions as **Article 17(2)**.

Article 17 of Nepal’s Constitution guarantees freedom of opinion and expression but does not explicitly include the right to seek, receive, and impart information. This omission weakens legal protections. Without clear constitutional guidance, Nepal’s judiciary will not be able to establish the necessary guidelines to protect these freedoms. Moreover, the Constitution equates protections and restrictions for both opinion and expression, despite international law considering opinion an absolute right, while expression can be subject to restrictions.

In addition, Article 19 prohibits prior censorship but applies only to mass media, leaving digital platforms vulnerable. Additionally, Article 17(2) justifies limitations on free expression under twenty broad grounds, including "harmonious relations among religions and communities," "nationality," and "public decency." There is no attempt to define these vague clauses, which create opportunities for suppressing marginalized voices and critical discourse through restrictive interpretation.

These restrictions can be placed through Acts- one of which the Social Network Bill could go on to become. While many of these exceptions are consistent with international law, some— such as those based on "harmonious relations between federal units" or "nationality"— set a very low threshold for restrictions, raising concerns about their potential for misuse⁶.

Statutes

Nepal Telecommunications Act, 1997 (2053)

Section 23 of the Act requires persons desiring to run telecommunications services to be licensed by submitting an application to the Nepal Telecommunications Authority. Although antiquated, the law remains in force on account of the use of telecommunications for day-to-day communication.

Electronic Transaction Act, 2063 (2008)

Section 47 of the Electronic Transaction Act (ETA) prohibits the publication or display of material on electronic media—including computers and the internet—that is deemed contrary to prevailing law, public morality, or decent behavior. It also targets materials "which may spread hate or jealousy against anyone" or "jeopardize the harmonious relations subsisting among the peoples of various castes, tribes, and communities." The prescribed penalties include **a fine of up to One Hundred Thousand Rupees, imprisonment for up to five years, or both.**

However, the provision introduces vague and problematic terminology, notably phrases like "materials that may spread jealousy." Such language fails to clearly define what constitutes incitement of jealousy, leaving the scope of prohibited content ambiguous. This vagueness raises critical questions: What precisely is deemed illegal, and which expressions should be protected under the principles of free expression and media freedom?

Repression of journalistic expression has been on the rise. For instance, in 2018, during the Oli government, six journalists were detained, resorting to Article 47 of the Electronic Transaction Act

⁶ Narayan Datta Kandel, 2017, Standard Review of freedom of Expression and Censorship in Nepal, International Journal of Culture and History, Vol. 3, No. 1, pg no.56.

(ETA). Similarly, at least 19 people are believed to have been arrested over six months up through January 2018 for their activities on “social networks.”⁷

In June 2025, the arrest warrant issued against Dilbhushan Pathak for their video entitled on “Reality of Hilton Hotel and Jaybir Connection” was also issued on the basis of Section 47 of the ETA.⁸

National Penal (Code) Act, 2074 (2017)

Section 50 (Sedition) criminalizes the use of any means to engage in baseless criticism of the government or to incite hatred or contempt towards it. The law prescribes a punishment of imprisonment for up to three years, or a fine not exceeding NRs. 30,000, or both. The lack of clear definitions for terms like “baseless criticism” and “hatred/contempt” gives authorities broad discretionary power, which can potentially be used to suppress dissent and stifle political debate.

Under **Section 121 (Obscenity)**, the production, distribution, import, and export of obscene materials are prohibited. Offenders can face imprisonment for up to one year, or a fine up to NRs. 10,000, or both. Notably, this provision includes an exemption for content created from the perspectives of art, literature, education, research, and religion. While the exemption acknowledges the value of creative and intellectual expression, the overall ambiguity in the definition of “obscene materials” may still lead to arbitrary enforcement.

Other crimes enlisted in the Act include unauthorized listening or recording of others’ conversations, taking or distorting another person’s photos without consent, publishing, selling or giving one’s photograph to another without consent, tapping telephone conversations, breaching of privacy through electronic means, making spam calls, etc.

The Code contains provisions that significantly impact freedom of expression by imposing criminal sanctions on certain types of speech. While these measures are ostensibly aimed at maintaining public order, their vague and broadly defined language raises concerns about potential misuse.

This ban on Online Pornography (2018)⁹ is an example of executive overreach based on the Code. On September 21, 2018, the Ministry of Communication and Information Technology directed the Nepal Telecommunication Authority to ban online pornography, citing Article 121 of the National Penal (Code) Act, 2017. The justification provided for this measure was the protection of public morality and decency. The government argued that such content contradicted social norms

⁷ HRW, *Nepal End Attacks Free Expression* (2019) Available at

<https://www.hrw.org/news/2019/04/18/nepal-end-attacks-free-expression>

⁸ Kathmandu Post, *Cybercrime case filed against journalist Dil Bhusan Pathak*, Jul. 17, 2025, Available at

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

⁹ Maharjan Harsha, *Freedom of Expression in Nepal in the Digital World: A Policy Review*, Research Brief No. 31, Martin Chautari (2020).

and contributed to sexual violence. This decision raised concerns regarding the state's broad authority to determine moral standards and its potential encroachment on digital rights.

Directive for Managing the Use of Social Networks, 2023

Clause 3 (Enlistment of Social Network Platform) lays down the process by which persons, companies, institutions can enlist their networks with the Ministry by submitting various documents, including “**Video KYC of authorized representative in case of online application**”.

Clause 4 (Acts prohibited to be committed by Social Network Users) such as:

- Creating anonymous or “disguised” identities or producing and engaging with content using such identities,
- **Targeting protected groups or harming social harmony and tolerance by sharing “word”, audio, visual, picture or by creating, publishing and broadcasting “trolls”,**
- Engaging in “hate speech”,
- Perversely modifying someone’s photograph and publishing or broadcasting it,
- **Editing, publishing and broadcasting, without permission, photographs and videos of private matters other than those of a public nature,**
- **Publish, broadcast or comment “in support of” obscene word, photograph, audio, video animation,**
- Encourage consumption, buying, selling of narcotic drugs,
- Encourage or engage in gambling,
- Publishing or broadcasting content related to terrorism, and
- Encourage content that harms child and promotes prohibited activities such as child sexual exploitation, sexual abuse, prostitution.

Clause 8 (Responsibilities of Social Platform Operator) obliges operators to:

- Develop algorithms to moderate unlawful content,
- Remove content within 24 hours if an affiliated body directs it to do so,
- Publish awareness-related content,
- Abide by the **Santa Clara Principles** to regulate social networks,
- Verify facts of content published or broadcasted on social network platform, and
- To prohibit publication or content that breaches the sovereignty, national integrity, is against social and religious harmony, or outrages social or religious harmony.

Clause 9 (Responsibilities of Social Network Users) obliges users to abide by conditions similar to those imposed by the Constitution in using social networks, in addition to publishing or broadcasting obscene content. It also states that one should not “knowingly” engage with such content.

Clause 13 (Social Networks Management Unit) mandates that a Social Network Management Unit has to be formed within the Ministry to handle grievances received by operator of platform or point of contact or relevant agencies on an appellate basis.

Clause 14 (Special Provision) obliges point of contacts, relevant agencies, social network platforms, and Social Network Management Unit to prioritise grievances related to women, child and minorities.

The mention of the **Santa Clara Principles** in the Directive is disingenuous to say the least. The Principles require explicit compliance with human rights and due process, which includes that the users be informed about every instance of state intervention in content moderation. Neither the provisions of the Directive, nor the Bill include any such provisions. The Directive also imposes greater responsibility on platforms, including the use of algorithms for content moderation and fact-checking content disseminated on said platforms.

The Directive was clearly a foreshadowing of the impending criminalization of anonymity and pseudonymity online. Although the intent to criminalize “obscene” content online is clear, **Clause 4** leaves room for some hope when it prohibits “editing, publishing and broadcasting, **without permission**, photographs and videos of private matters other than those of a public nature”. This could mean that the Directive did not prohibit content shared in private conversations, including sexual content shared consensually. In any case, the absence of definitions of “public” or “private” nature leaves much to be desired in the regulation of content shared via social networks.

Information Technology and Cyber Security Bill, 2082 (2025)

Section 88 (Production, Publication, Dissemination, Buying or Selling of Obscene Content) criminalizes the production, publication, dissemination, buying or selling of obscene content online. An exception has been included for sexual content produced or used for research, education, legal, and medical purposes. The punishment for such use is upto 2 years of imprisonment and Rs. 200,000.

The Information Technology and Cyber Security Bill (ITCS) Bill contains various crimes enlisted in the SNB, and will repeal the ETA if it comes into force.

In the absence of any definitions or elements that constitute “obscene” materials, blanket bans on any and all forms of “sexual” content either private or personal is indicative of a regressive and protectionist legal approach. There are no subjective or objective tests determining which purpose is legal and which is not, and consent, which is the foundation of all lawful interactions both online and offline has been completely disregarded. If passed without amendments, the Bill will lead to criminalization both consensual exchanges and victims of online sexual violence - ultimately causing a chilling effect on freedom of expression.

This disruption of safe and just use of digital space will be exacerbated by the element of surveillance that will accompany this provision. If sharing of obscene material is criminalized, state authorities will have to surveil online platforms to “prevent” these “crimes” from happening. This will again push vulnerable communities further to the margins, with no legal protection or remedy.

Policies & Guidelines

Science, Technology and Innovation Policy, 2075 (2019)

Digital Nepal Framework, 2075 (2019)

National Cyber Security Policy, 2080 (2023)

National Information and Communication Technology Policy, 2072 (2015)

Draft Policies

AI Policy, 2081 (2024)

Personal Data Protection Policy, 2082 (2025)

Other

[Repealed] Information Technology Bill, 2019

How can we critically engage with the Bill?

PROVISIONAL ANALYSIS

This section contains an analysis of selected provisions of the Bill against Nepal's obligations under the International Covenant of Civil and Political Rights (ICCPR) and applicable law and principles.

A. Legal Foundation and Selective Reform

The Bill cites the precedent¹⁰ set in *Baburam Aryal et.al. v. Government of Nepal*,¹¹ as one of the core legal reasons for its conception. The petitioners relied on a Kantipur Daily article published in 2069 B.S. that reported on the investigation related to the murder of Justice Ran Bahadur Bam to make their case for the right to freedom of expression, right to information, right to privacy, and protection of human rights. **Kathmandu Daily reported that the investigating police officers accessed the call records and SMS details of over 5 lakh phones, particularly treating text exchanges between partners as a source of entertainment.** The petitioners claimed that this was made possible by the policy vacuum that persists in the digital sphere.

In the absence of dedicated legislation, the Government claimed that the right to privacy is not absolute, and interventions are justified in the context of a criminal investigation. The precedent affirms the right to privacy as an inalienable right. **The Court said that the right can be restricted during emergency conditions, criminal investigations cannot be used to intervene into the private lives of citizens by accessing and storing personal information arbitrarily. The responsibility of online platforms and service providers is also upheld, with the Court stating that they should not give up protected information without due process even to national authorities. State authorities handling criminal investigations and service providers were held to have special responsibilities to maintain the confidentiality and security of personal information by drawing a nexus between individual privacy and national interest.**

The provisions related to platform and user liability is evidence of *some* attention of the legislators towards the decision. However, designation of arbitrary and overbroad powers to state authorities, overlapping jurisdictions ascribed to state bodies, the use of vague terms such as “national interest” and “harmony”, and criminalization of anonymity indicate intentions to exempt the state from responsibility and democratic criticism. **The SNB is yet another example in the Government's long-standing pattern of selective reform.**

¹⁰ SNB, Theoretical Background, No.1.

¹¹ *Baburam Aryal et.al. v. Government of Nepal*, Writ No. 069-WO-0268.

B. Overbroad Non-Definitions and Arbitrary Powers

The Bill uses various phrases such as national interest, national integrity, sovereignty, territorial integrity, and national security to criminalize acts that go against it. Although fundamental freedoms—including those related to communication, press operations, and media registrations—can be suspended in the state of emergency to preserve national security and order during crises, they also open the door to potential overreach, wherein the suspension of freedoms could be exploited to silence dissent or control the flow of information during politically sensitive periods.

Nepal, as a signatory to the International Covenant on Civil and Political Rights (ICCPR)¹², is obligated to uphold freedom of expression as per Article 19, which guarantees the right to "seek, receive, and impart information and ideas of all kinds." The freedom of expression can not be limited by media type, as the covenant envisions future technological advances¹³. Restrictions on this freedom must pass a three-part test¹⁴.

- Prescribed by Law: The restriction must be clearly defined, not be ambiguous and not grant excessive discretion to authorities.
- Legitimate Aim: Restrictions must protect specific interests such as national security, public order, or the rights of others. 1) Restrictions must be applied only for those purposes for which they were prescribed and must be directly related to the specific need on which they are predicated. 2) the restriction must be primarily directed at one of the legitimate aims and serve it in both purpose and effect. For example, a restriction that has a purpose directed at one of the legitimate aims listed but has a merely incidental effect on that aim cannot be justified.
- Necessity and Proportionality: The restriction must be necessary for achieving a legitimate aim and must be the least restrictive means available. The restriction must be necessary for the protection or promotion of the legitimate aim. The necessity element of the test presents a high standard to be overcome by the State seeking to justify the interference.

Freedom of expression, as enshrined in Article 10, is subject to several exceptions which, however, must be narrowly interpreted and the necessity for any restrictions must be convincingly established. When examining the laws related to freedom of speech and opinions in Nepal, there is use of vague terminologies and unclear definitions of acts prevented under the freedom of speech and opinion. The law and constitutional provisions fail to meet these standards, raising concerns about arbitrary enforcement.

¹² A STUDY OF THE DOMESTICATION STATUS OF INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS IN NEPAL, National Human Rights Commission (2007) Available at https://nhrcnepal.org/uploads/publication/ICCPR_Study_Report.pdf

¹³ United Nations, General Assembly, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, A/HRC/17/27

¹⁴ Expert Meeting on the Links Between Article 19 and 20 of the ICCPR: Freedom of Expression and Advocacy of the Religious Hatred that Constitutes Incitement to Discrimination, Hostility or Violence, UNHCR (2008) Available at <https://www.law-democracy.org/live/wp-content/uploads/2015/02/foe-briefingnotes-2.pdf>

Overbroad and Vague Laws was evenly acknowledged across young women and men, and also consistently flagged by non-binary, queer, and transgender participants. The current SNB has multiple definitions, posing the following problems:

- **Broad Grounds for Restriction:**

- The extensive list of restrictions, though partly aligned with international standards, risks undermining the democratic process by allowing the state to limit dissent and critical debate.
- The low thresholds—especially regarding “harmonious relations”—could easily be used to marginalize voices that challenge entrenched power structures.

- **National Interest as a Catch-All:**

- Granting the legislature the power to define “national interest” provides a wide latitude that may result in arbitrary or politically motivated censorship.
- The precedent set by the National Broadcasting Act shows how vague criteria can lead to significant constraints on media freedom and public discourse.

- **Need for Clear Definitions:**

- The lack of precise definitions for what constitutes protected expression versus prohibited speech creates legal uncertainty.
- Establishing clearer standards would help ensure that restrictions are applied in a manner consistent with both domestic principles and international norms.

- **Emergency Powers and Risks:**

- While the suspension of freedoms during emergencies can be necessary, it also poses risks if not strictly regulated.
- Without robust safeguards, such powers might be exploited to maintain control even when the emergency has passed, further eroding democratic freedoms.

C. Impossibly Burdening the Business Ecosystem

The SNB requires pre-registered companies, firms and institutions, with PAN certification to register to operate platforms and social networks. While the Bill allows online registration under **Section 3**, the Department has the power to request “additional” documents if need be. The Ministry has been enlisting social networks since 2023, meaning it has had several references as to the complications related to the process of registration and regulation. Granting discretions in application, review, and renewal processes without explicit grounds for rejections and compliance enumerated in the Bill has shrouded it with further confusion.

A fine of Rs. 55,00,000 has been decided upon platform operators that run their platforms without registration and licensing in **Section 17**. Mandatory registration provision of social networks means prior censorship, surveillance, and interference on the right to freedom of expression given the chances of procedure being tedious, costly and arbitrary. In the present case, fees under

Companies Act, 2063 (2006) along with relevant Acts, and applicable fees under SNB and the impossible burden of compliance will actively stunt the budding startup ecosystem in Nepal

D. Ignorance of Technology Facilitated Violence

The prevalence of specific forms of **Technology-Facilitated Violence (TFV)** such as **Technology-Facilitated Gender Based Violence (TFGBV)**, **Image-Based Abuse**, **Online Intimate Partner Violence (IPV)**, etc often inspires the creation of Bills that regulate interactions over social networks. However, in a country where 1 in 4 young people experience IPV via text and video calls via social networks,¹⁵ the SNB fails to so much as even acknowledge it directly.



Terms associated with online IPV

Note: The bigger the size of the terms, the more they were cited by participants

Source: Child SafeNet & SVRI's Research on Online OPV in Young People in Nepal

The SNB sparingly states in **Section 28** that if someone uses social networks to commit a crime in accordance with any law, 1 year will be added to their final punishment. However, this omission of TFV and the proposed *indirect* workaround is likely to increase complications and impede justice for TFV victims. Together with the ITCS Bill which proposes to criminalise all non-educational forms of online sexual expression, victims of IPV and TFGBV could potentially be identified as criminals from the outset- depriving them from even the inkling of justice.

E. Non-consideration of Marginalised Identities

In our survey, when respondents were asked about the actions being taken by the government to regulate social networks, most young women (18–34) and marginalised genders cited “increasing surveillance without accountability”, and the theme of surveillance was unanimously mentioned by all queer, trans, and non-binary respondents.¹⁶ Marginalized persons were generally more critical of

¹⁵ Child SafeNet & SVRI, *From Romance to Risks: Online Intimate Partner Violence Against Teens and Young People in Nepal*, 13 (2024), Available at [From romance to risks: Online intimate partner violence against teens and young people in Nepal - SVRI](#)

¹⁶ Body & Data, SNB Survey, See “Government Actions”.

the Social Network Bill. However, the Bill fails to establish safeguards for the protection of these communities or impose additional punishment for online activities that target marginalized communities.

Roughly 4 in 10 users maintain multiple accounts on the same platform, with **younger users and gender minorities** using multiple accounts as a form of **identity management or safety**. **Section 27** criminalizes the use of anonymity and pseudonymity, especially when it is against national integrity. Generally, two-thirds of internet users do not use their legal name because it allows them to express themselves and interact with other people more freely,¹⁷ i.e. to protect themselves against censorship and surveillance. In the survey, non-binary and trans users favor pen names or contextual identities, meaning that marginalized persons are more likely to use these accounts as precautionary measures. Criminalization in the absence of special protection substantially increases the threat these communities are under for their online presence, especially if they are vocal against systemic injustices.

F. Over-criminalisation and Crushing Fines

Criminal sanctions can be excessive for speech-related offences, especially when alternatives exist. Civil measures, such as fines or retractions, focus on rectifying harm rather than imposing harsh penalties. They ensure accountability without burdening the justice system and disrupting civic discourse. However, the bill criminalises acts of opinion and expression, through imprisonment and uses vague wording granting authorities excessive discretion. The fear of criminal penalties can discourage people from speaking at all, even when they have legitimate opinions or criticisms. This threatens marginalised communities like LGBTQIA+, women, activists, and journalists in the online space.

1. Arbitrary/Over-criminalisation

The bill's non-existent definitions of national interest, national integrity, sovereignty, territorial integrity, and national security already imposes arbitrary regulatory mechanisms. The crushing sentences and fines of these crimes are violative of Nepal's supposed rehabilitative approach. Ambiguous definitions of "hate speech," "obscene" and "gruesome" allow selective enforcement.

- Hate Speech and Defamation (**Section 16(1)(a)**): Prohibits content deemed as "trolling," "hateful expressions," "insults," or "hate speech" that or "harms" a person's reputation- leading to a fine of upto Rs. 500,000.
 - ICCPR's definition of "Hate Speech": International law imposes one clear positive duty upon states as far as restrictions of freedom of expression are concerned, as stated in ICCPR Article 20, "the prohibition on war propaganda and hate speech"¹⁸. There is, however, no agreed definition of propaganda or hate speech in international law.

¹⁷ ChildNet, Global perspectives On Online Anonymity, Available at [Global survey about online anonymity](#)

¹⁸ Article 19, *ICCPR Links Between Articles 19 and 20*, Available at <https://www.article19.org/data/files/pdfs/conferences/iccpr-links-between-articles-19-and-20.pdf>

- Content with Malicious Intent (**Section 16(1)(b)**): Bans sharing “myth”, “misinformation” and “disinformation” without any subjective elements to establish intent or objective elements to establish harm. The punishment is a fine of upto Rs. 500,000.
- Threats to Sovereignty and Social Cohesion (**Section 18**): Prohibits content that “undermines national sovereignty, geographical integrity, national security, or social harmony”, with vague criteria allowing selective enforcement.
- Gruesome (or graphic) Content (**Section 24**): Prohibits sharing “gruesome” images or videos without defining the term with upto 3 months and fine of Rs. 50,000.
- Indecent, False, Misleading Content (**Section 25**): Bans sharing “indecent” images or videos or “false” or “misleading” information with penalties of up to 2 years in prison, a fine of Rs. 200,000, or both.

Criminalising these broad categories disproportionately impacts journalists, activists, and marginalised communities, creating a chilling effect on free speech and discouraging public discourse.

2. Restrictions on Anonymity

Section 27 prohibits the creation and use of anonymous and pseudonymous accounts. While creation warrants a punishment of 3 months of imprisonment and upto Rs. 50,000 in fines. If such accounts are used to publish content against national sovereignty, territorial integrity or national interest, a fine of upto Rs. 15,00,000 and a term of upto 5 years.

In Body & Data’s survey, it was found that non-binary and trans users favor pen names or contextual identities. Anonymity is rare overall, though slightly more common among non-binary and female users. This provision disproportionately affects marginalised groups, survivors of violence, and LGBTQ+ individuals who rely on anonymity for safety. Restricting anonymity also discourages whistleblowing, investigative journalism, and online activism, limiting the voices of those who fear persecution.

3. Metered Punishment

Section 28(2) imposes double penalties for repeat offences, mirroring the **Electronic Transaction Act’s Section 47(2)**, which allows disproportionate punishment and legal harassment of activists and dissenters. This raises concerns about legal overreach and potential misuse of punitive measures to silence opposition voices.

How and where do we lead the Bill?

POTENTIAL FOR VALUE CREATION

Despite the overwhelming discontent against the Bill, the Bill has immense potential for value creation through critical feminist and marginalised approaches and synthesis of regulatory aspects mechanisms in the Nepalese legal landscape. In this section, we imagine the values this Bill has the potential to enshrine through our collective effort and advocacy.

A. Envisioning a Feminist Internet

1. Special Protections for Marginalised Identities

The Bill wholly disregards the existence and experiences of marginalised communities online. If passed without amendments, the Bill would adversely impact marginalised communities and identities that opt for pseudonyms and anonymous identities online to express discontent against national policies and predominant socio-political norms. Nearly half (43%) of respondents believe their identity affects their online experience, while language and identity exclusion was frequently cited as a primary concern regarding the Bill by young women participating in our survey.

Clause 14 of the Social Network Directive obliges point of contacts, relevant agencies, social network platforms, and Social Network Management Unit to prioritise grievances related to women, child and minorities. However, the current SNB includes no such consideration in grievance handling or RRT mechanisms.

To rectify this, we propose that the Bill preliminarily include a chapter on guiding/general principles akin to the **National Penal Code, 2074 (2017)**.¹⁹ Such a chapter could create a framework from which to approach the Bill. In said chapter, a **provision related to special protection for marginalised identities could be included**. Such inclusion could subsequently oblige:

- Platform operators under **Section 12** to enforce such special protections,
- The Department to enforce content moderation in the interest of marginalised groups under **Section 13** and **Section 36**,
- The Grievance Handling Rapid Response Teams created by Platform Operators to duly take experiences of and protections for marginalised identities under **Section 15**,
- Platform users to refrain from furthering hate speech, mis/disinformation, superstition, etc., particularly against or targeting marginalised per **Section 16**, and
- Adoption of contextualised investigations of victims and accused persons belonging to marginalised communities under **Chapter 5**.

¹⁹ See Chapter 2, National Penal Code, 2074 (2017).

2. Safeguards for Consensual Online Sexual Expression

Together, the ITCS Bill and the SNB force us to imagine a future where consensual sexual expression will be illegal, if not heavily surveilled. Such legal regimes undermine the very foundations of inalienable human rights to freedom of expression and bodily autonomy. While protectionist approaches to inhibit harmful online sexual content, such as child pornography and technology-facilitated violence are necessary, blanket bans on all forms of online sexual expression are counterintuitive.

Blanket bans on sexual expression offline, such as sex work, have demonstrated time and again to not only be ineffective but also to adversely impact the very communities they intend to protect.²⁰ Online sexual expression is common in private interactions and public domains, and more often than not, cannot be prevented through deterrence measures. **In the chapter containing “guiding principles” as proposed previously, the Bill could include a provision that protects consensual exchanges, including sexual exchanges, through the use of social networks and platforms** against surveillance and criminalisation. This would, again, create a framework from which to approach the subsequent provisions of the Bill.

3. Protections Against Technology-Facilitated Violence

The Bill proposes to criminalize specific forms of TFV such as bullying, stalking, hacking, phishing, sextortion, extortion, deepfakes, etc in **Chapter 5**. The Bill leaves out doxxing, cybermobs, image-based abuse, shallowfakes, online impersonation (catfishing).²¹ Young women participating in our survey highly reported online harassment as a primary concern regarding the Bill. Similarly, 2 out of 5 respondents (40%) say they have experienced harm or discrimination online, while over 1 in 10 prefer not to say - potentially indicating distress or uncertainty. While women aged 18-24 had the highest reports of harm.

As we have seen in case of abortion, sparing mentions and indirect legal recourse is wholly insufficient to do justice by victims. After a case was brought by a marginalized person against the state for inadequate legal framework regarding reproductive and resulting inaccessible services, the Court ordered the state to make sufficient arrangements.²² Eventually, a separate chapter on abortion was included in the **National Civil Code** and a new Act to ensure safe motherhood was introduced.²³

Given the prevalence of online violence, a dedicated policy, let alone provision is necessary to address TFV. **This could be done by adding a provision that clubs together digital crimes (doxxing, online impersonation) with crimes whose nature is transformed by the use of technology (sextortion, TFGBV).** This would allow for specific legal elements to emerge,

²⁰ Human Rights Watch, *Why Sex Work Should be Decriminalized* (2019) Available at <https://www.hrw.org/news/2019/08/07/why-sex-work-should-be-decriminalized>.

²¹ See UNFPA's Glossary on Digital Violence Terms for definitions, Available at [16 DAYS OF ACTIVISM AGAINST GENDER-BASED VIOLENCE | United Nations Population Fund](#)

²² **Laxmidevi Dhikta et.al. v. Government of Nepal et.al.**, NKP 2067 B.S., Vol. 9, Decision No. 8464.

²³ See Safe Motherhood and Reproductive Health Rights Act, 2075 (2018).

allowing direct regulation and deterrence. Crimes under the **National Penal Code** could also be integrated into the Act to avoid double criminalization.

Such a provision would also specify admissible digital evidences, allowing the effective application of **Section 34** and the integration of the SNB with **Evidence Act, 2031 (1994)**. Victims of TFFV would also know to preserve digital evidences in the forms of video screen recording, screenshots, video recording, audio recording, websites, emails, etc.²⁴

4. Ensuring Accessibility for Disabled Persons

Disabled persons are generally excluded from social, political, and economic facets of participation. The digital space is one of the few places where disabled persons are able to freely express themselves, access their communities, and join support networks. To ascertain accessibility and meaningful participation of disabled persons, **platforms must be made to conduct annual disability audits and held liable** if their platforms and network fail to comply through amendments.

5. Approaching a Pleasure-Centric Internet

A pleasure-centric approach to the internet means embracing and encouraging pleasure and enjoyment associated with the use of the internet through informed and safe use. This includes ensuring that protective mechanisms against harm and repression are in place to allow users to fully indulge in the benefits of technology.

Protections for the online presence of marginalized persons, alternative forms of expression, online sexual expression, effective and delimited delegation of power, along with protections against surveillance and violence would lead us to a pleasure-centric internet. **For this, we propose that legislators (and civil society) begin from the intention of maximizing pleasure and not deterrence against harm.** This begins from the very name of the Act- the names **Online Safety Act** and **Online Harms Act** induce varied reactions, with one instilling comfort and trust, while the other incites caution and vigilance. Even if we are not able to change the name of the Act, it would benefit the cause of good governance to amend the SNB in a manner that first and foremost, pushes free and safe online presence.

For this, we can cautiously borrow from South Asian legislations (Sri Lanka, Malaysia, etc) and laws like those of Australia, such as the **Online Safety Act (2021)**, which introduces a **Cyber Abuse Scheme and Image-based Abuse Scheme for children** and empowers an Online Ombudsman and independent regulator- the **eSafety Commissioner** to regulate platform moderation by imposing liabilities on platforms and internet service providers.

²⁴ See Tech Safety Canada's Toolkit on Preserving and Storing Evidence of TFFBV: Best Practices, Available at [3.05 Preserving and Storing Evidence of TFFBV: Best Practices – Tech Safety Canada](#)

B. Adopting Rehabilitation and Facilitation

1. Human Rights-Based Legislation

As elaborated above, restrictions to freedom of expression must be in compliance with permissible restrictions under Article 19(3) of ICCPR. The three-part test requires that restrictions be prescribed by law, and necessary and proportionate to pursue a legitimate aim. **Adding provision that states that all restrictions on online expression shall be subject to the three-part test prescribed by the ICCPR would ensure compliance.** Combined with clear definitions in the Bill, such an approach would warrant a just and lawful regulation regime to manage interactions taking place over social networks.

Further, when interpreted in conjunction, the right to freedom of expression and the right to privacy converge to provide users with the right to anonymity. Anonymity on the internet is already relative, with constant surveillance and inevitable data trails. However, internet users have consistently stated that anonymity allows them to safely engage in online spaces by creating a space for self-representation, even enabling discussion of taboo topics²⁵. In case of crimes requiring identification of anonymous users, criminal investigations have been known to use service providers and platform services to track accused/offending persons. **Therefore, anonymity and pseudonymity must be accepted as tools for online safety while authorities must only be allowed to identify users using such identities exceptionally allowing,** In any case, decriminalizing the use of such identities online and acts relying on arbitrary and highly volatile definitions would ascertain compliance with human rights.

2. Teachability over Disproportionate Fines

The tech-startup industry is a budding sector in Nepal, currently in need of reinforcement through simpler compliance measures and substantial investment. Fines under **Section 17** of upto Rs. 55,00,000 assume that all operators of social networks and platforms make disproportionate profits through unlicensed platforms. However, that is not the case for startups or small businesses. Instead of imposing such fines, the following measures can be adopted:

- Prescribing a **cut-off date** for registration of **existing platforms**, allowing them to stabilize and attract investments without the burden of compliance of upto **1 year**,
- Allowing **test periods** to **new platforms** upon commencement of the Act for upto **6 months**, after which they will be required to apply for licensing, and
- Imposing **fines proportionate to the net profits** of the platforms that do not register after aforementioned periods.

We propose that all fines in the SNB should be revised in consideration of the economic burden it places on the accused persons. Intention and action in online spaces are extremely nuanced, warranting individualized legal responses to each case. However, given the lack of institutional

²⁵ Sarah Stummer, *A Right to Anonymity in the Digital Age: A Discussion of the Opportunities, Risks and Limitations*, Verfassungsblog (2024) Available at [A Right to Anonymity in the Digital Age](#)

resources required to provide such tailored responses, arbitrarily accused individuals will have little to no recourse if an accusation is made under the Bill and the fine will only make matters worse.

C. Simplifying Compliance for Businesses

While the Bill allows online registration under **Section 3**, the Department has the power to request “additional” documents if need be. The Ministry has been enlisting social networks since 2023, meaning it has had several references as to the complications related to the process of registration and regulation. Granting discretions in application, review, and renewal processes without explicit grounds for rejections has shrouded the Bill in confusion.

Overlapping regimes for company registration, tax compliance, closure, and electronic transactions among others creates higher barriers to entry for emerging and small businesses. **This can be resolved by developing compliance manuals and handbooks along with accessible online portals or websites to simplify bureaucratic compliance.**

D. Strengthening Digital Infrastructures

1. Independent Regulatory Bodies

The Bill states that no further institutional arrangements are required to execute the Bill. However the current form of the Bill and existing institutional resources do not inspire confidence. On account of the increasing data surveillance and storage in the state through digitization and digitalization, it has become critical to develop competent bodies to manage the storage, use, and processing of data. Coincidentally, data misuse was the most frequently cited concern of respondents vis-a-vis their use of social networks.

We therefore propose that **independent bodies be established for the management of sensitive information, platform regulation, content moderation, and grievance handling.** The current designation of all powers to the Department will increase the chances of data leakage, data misuse, and structural biases (such as vetting and profiling).

2. Establishing Federal Bodies

Since the establishment of federalism in 2015, discontent regarding improper devolution of power and resources between Federal, Provincial, and Local bodies has been persistent. If this Bill passes, users and platforms will be required to report to the Department or submit complaints to the Cyber Bureau in the capital of the country. This will reinforce existing attitudes towards federalism, further deepening the divide between all levels. The Bill should include provisions that imagine provincial and local structures that handle data storage and grievance handling respectively. Completely digitizing registration procedures and maintaining federal bodies that oversee provincial and local management would create effective and decentralized digital infrastructures.

3. Delimiting and Strengthening the “Department”

The Bill grants overbroad and arbitrary power to the Department regarding all matters related to social network bills. Together with the myriad of undefined grounds for restriction of freedom of expression, the Department would have uninhibited powers. Delimitation of power by establishing or retaining existing structures such as the **Social Network Management Unit** for grievance handling could be a solution.

The **Social Networks Directive** established a **Social Network Management Unit**, which had similar powers to that of the Department as enlisted in the SNB. **We propose that human resources from the Unit be transferred or the Unit itself be relocated into the Department. Contract-based appointments to special taskforces for platform accountability, user compliance, content moderation, etc** can also increase the competency of the Department.

4. Duly and Equitably Established Rapid Response Team

The Bill contains no qualifications, composition or working procedures related to the Rapid Response Team (RRT) entrusted as the first reporters to scenes of vulnerability. This opens the RRT to abuse of power, nepotism, discrimination, and overall ineffectiveness. **The solution is simple- adding a provision including clear qualifications and composition of the RRT would ensure transparency and accountability of the Department and the Ministry.**

E. Synthesising Legal Regimes

1. Bracing for Emerging Technologies

The scope of the Bill is limited primarily to networks and platforms that are social in nature, allowing communication and dissemination of content between individuals, computers, and institutions over the internet as signified by the name and objectives of the Bill. This excludes **service-oriented online platforms and online broadcasting services among others.** Confusion around platforms such as ChatGPT looms large, with upto 70 respondents enlisting it as a platform they regularly used in our survey. The Large Language Model (LLM) is not a “social network” within the scope of the Act but needs regulation. In recognition of the prominence of AI-based applications, the government has proposed draft policies related to AI and personal data protection. These policies are indicative of prospective legal directions.

The current **SNB excludes key aspects such as use of AI in content generation and even moderation** all the while intending to regulate user behavior and platform accountability on social networks. It also wholly disregards regulatory aspects related to **storage and use of the data** collected by these platforms in the process of operation. We propose that **the Bill pave way for emerging legislations and policies regarding AI and Data Protection by enlisting general principles such as those included in Santa Clara Principles and Guiding Principles on Business and Human Rights in Chapter-2.** This would reflect transparency on part of the government- an open acknowledgement of the ever-expanding gap between policy and technology and a public commitment to compliance with human rights and international legal principles.

2. Furthering Private International Law

The Bill allows the operation of platforms run by foreign-registered companies, firms, and institutions. If held liable for not registering or failing to comply with relevant guidelines under the Bill, it will open the state, relevant individuals, and platforms up to lawsuits. Since most popularly used platforms are run by foreign companies, specific private international law-related provisions will be required to lawfully resolve said cases. We propose that **a provision either extending the scope of private international law under the National Civil (Code) Act, 2074 (2017) to include social network related issues be added or that a provision laying specific grounds under which relevant provisions of the private international law will be applicable.**

3. Defining Criminal Jurisdictions

Section 1(3) of the Bill clearly states that the Bill applies to crimes committed against Nepalese nationals abroad, proposing extra-territorial criminal jurisdiction. In the absence of binding treaties or regional laws that regulate activities on the internet, it is almost impossible to actually prosecute transnational crimes committed via the use of social networks. To rectify this, the **Bill must supplement the Mutual Legal Assistance Act, 2070 (2014) by extending its scope to include crimes committed through the use of social networks and other electronic means.**

The regulation of digital spaces is already convoluted with multiple routes to justice- from filing complaints to either the Cyber Bureau or divisions within Nepal Police to adjudication by the District Court. Adding a provision that clearly mentions the application of the **ETA, National Penal Code**, and applicable criminal laws to the offences enlisted in the Act would ease investigation and prosecution.



Body & Data

www.bodyanddata.org

[@bodyanddata](https://www.instagram.com/bodyanddata)



Facebook



Instagram



Bluesky



X

Author: Monisha Choudhary

Editor: Monika

Layout: Monisha Choudhary

Published By: Body & Data

Support: Vision for Change