Analysis of the Social Media Bill, 2081

On 28 January 2025, the Ministry of Communication and Information Technology registered the 'Bill related to Operation, Use, and Regulation of Social Media in Nepal, 2025' (the "**Bill**") at the Upper House of the Federal Parliament (National Assembly). The Bill aims to regulate the use of social platforms and impose accountability primarily on individual users and the platform operators.

As per the Ministry's Concept Paper, the Bill is an outcome of the necessity to regulate social media platforms for their dignified, safe, and orderly use. It cites that the constitutional basis of the Bill lies in safeguarding the right to communication and digital privacy while safeguarding freedom of speech. While the 'Directive on the Use of Social Networks 2023' is already in force, the Paper underscores the policy issues in the Bill and argues for changes in the Bill for a more balanced and comprehensive regulatory framework.

The Bill contains provisions on licensing of the social network platforms, content takedown mandates and criminal liability for non-compliance, among others. However, it lacks important aspects of social media regulation such as, child safety provisions (age verification/age rating of content), platform security standards, data privacy/cybersecurity requirements, reporting obligations in case of cybercrime/data-breach. While the Government advocates that the Bill is essential for online safety of the public, the Bill in its existing form, leans more towards excessive content regulation and government control.

In this analysis, we have identified key issues in the Bill that require revision to achieve effective social media regulation which retains our fundamental right to speech at its heart and balances the public interest of a dignified society.

This analysis covers:

1. EXTRA-TERRITORIAL APPLICATION

Section 1(3) of the Bill provides that the Act shall extend throughout Nepal and shall also apply to any person outside of Nepal (meaning foreign national residing outside of Nepal will also be covered) if such person has committed offence under this Act against Nepal or a Nepali citizen.

Even though the Bill proposes an extra-territorial application jurisdiction, the extra-territorial enforcement jurisdiction of the same is questionable. Refining the scope with clear limits may be required to ensure that the extra-territorial effect of the Bill is fair and practical. An example can be taken from the UK's Online Safety Act, 2023 which applies to services that have significant number of UK users, or if the UK is a target market, or if it is capable of being accessed by UK users and there is a material risk of significant harm to such users.

Generally, the jurisdiction of a state can be established over a criminal offence based on the principles of: (a) territoriality; (b) nationality; (c) universal jurisdiction; and (d) the protective principle. Cybercrimes like online fraud, misinformation, cyberattacks and illegal contents transcend national borders, requiring international cooperation for effective investigation and enforcement.

The extra-territorial effect of the Bill cannot be achieved without the co-operation of other jurisdictions. One of the key issues that foreign jurisdictions will be evaluating while providing mutual legal assistance to Nepal is whether Nepalese legislation ensures sufficient protection of human rights (e.g., freedom of expression, data privacy etc.) and due process (like supervision of courts). An example of this can be taken from the "adequacy decision" requirement for cross-border data transfer under the GDPR, which takes into account the recipient nation's respect for human rights and fundamental freedoms, relevant legislation, judicial redress for the data subject etc. For this reason, it is crucial for the Bill to ensure relevant provisions (discussed in this Paper) that will help Nepalese legislation meet such evaluation criteria.

Another example is the CLOUD Act of the USA which requires a state party seeking assistance in offences like cybercrime, to adhere to International human rights obligations and commitments/ demonstrate respect for international universal human rights such as, privacy, freedom of expression, prohibitions on arbitrary arrest and punishment, among others. As of 2023, Freedom House has ranked Nepal as a 'Partly Free' country under the Global Freedom Score for political rights and civil liberties.

Additional aspect is that it may be a time consuming and burdensome process for a country like Nepal to find resources to negotiate bilateral agreements to obtain electronic data from each country from which it might need assistance. To start, Nepal may benefit from acceding to international frameworks such as the Convention on Cybercrime (Budapest Convention). It provides the most comprehensive guideline on developing domestic legislation on cybercrime, and efficient tools for investigation and prosecution of any crime involving electronic evidence.

Recommendations

a. The Bill needs to strengthen Nepal's democratic credentials and due process protections. Specific provisions addressing these areas (discussed below) should be incorporated into the Bill to meet criteria for international cooperation.

b. Prioritize negotiation and ratification of bilateral treaties on mutual legal assistance with relevant jurisdictions for data exchange, evidence collection and law enforcement cooperation to enhance cybersecurity and facilitate effective law enforcement.

c. Ensuring that the domestic legal frameworks correspond to Budapest Convention on Cybercrime, as well as improving the operation of specialized institutions such as the Cyber Bureau and NP-CERT.

2. DEFINITIONS

2.1. Definition of Social Network Platforms

Section 2(d) of the Bill defines "social network platforms" as app, website, blog, AI tools, or publicly available platform of similar nature created in cyberspace though the medium of electronic technology that allows internet users to exchange ideas and information or to engage in social interaction between individual-individual, individual and groups or institutions, and groups or institutions.

Precise clarification of the scope of this definition is essential, not only for electronic platforms to understand if they need to comply, but more importantly, for the Government to ensure effective implementation and enforcement of the Bill. In its current form, the definition suggests that online presence of a national daily will fall under this definition if it permits comments and interaction among readers which currently is the case for most of the national dailies. However, this is already regulated under the Print and Publication Act, 2048 and Online Media Operation Directives, 2073. E-commerce platforms, which are ordinarily not regarded as forum for exchange of ideas, but the possibility for user interaction via commenting/posting product reviews could bring them under this definition. Likewise, social media platforms as a catch-all category may also cover over-the-top (OTT) services—which are already regulated by the National Broadcasting Act, 2049 and the National Broadcasting Rules, 2052.This overlap raises concerns about multiple regulations and registration requirements.

International institutions listed below provide effective guidelines for defining social media platforms:

a. The UNESCO Guidelines for the Governance of Digital Platforms, 2023 provides that when defining digital platforms that should be in the scope of statutory regulation, the regulatory authorities should identify those platforms that have relevant presence, size, and market share in the jurisdiction, and functionality and features. This is reiterated in the UNESCO Guidelines for Regulating Digital Platforms, 2023 which recommends that the regulatory system should define which digital platform services are in scope, and identify the platforms by their size, reach, services they provide, features, and if they are centrally managed or distributed platforms.
b. As per the ADB Sustainable Development Working Paper Series on Enhancing Policy and Regulatory Approaches to Strengthen Digital, Platform, and Data Economies, 2023 an approach which describes the key characteristics of digital platforms rather than setting out concise definitions is a good practice to adopt, especially when digital platforms are becoming complex, multipurpose systems. This approach reduces the risk of ignoring the interconnected, cross-cutting and evolving nature of digital platforms, and potentially outdating the definition from the outset [for e.g., a hybrid platform that combines elements of social media, e-commerce, and online gaming.] Regulators will have to scramble to update the regulation to include this new type of platform, potentially leaving it unregulated in the meantime.

The current approach to content regulation may have unintended gaps. For a speech to constitute hate speech under the Bill, it must: (a) meet the criteria for hate speech, and (b) be made on a "Social Network Platform". This approach leaves room for individuals to circumvent regulations by creating independent websites that are not classified as social network platforms.

A more effective and practical approach could be to segregate content regulation from the regulation/registration of a Social Network Platform. It is important to distinguish between: (a) registration requirements, and (b) content regulation. For instance, hate speech is a criminal offense regardless of whether the platform involved is subject to a registration requirement. The current draft, by linking these elements too closely, may unintentionally restrict or create regulatory loopholes. A more modern approach is needed to ensure comprehensive and enforceable content regulation. This approach will provide a more flexible regulatory tool by allowing registration requirement linked with the number of subscribers. Other content related crime can still be a crime irrespective of nature of electronic form it has been expressed.

Recommendations

a. The definition should clarify which social media platform services are in scope, identify the platforms by their size, reach, features, and the services they provide. Further, the Bill needs to distinguish between (a) registration requirements and (b) content regulation to ensure that the registration requirement shall trigger to a specific size or feature platforms however, the content regulation shall be applicable to all the platforms irrespective of its registration. Similar approach has been adopted by the EU in the Digital Services Act which defines large online platforms based on active user.

b. The inclusion of "AI tools" within the definition of "Platform" is broad and covers all AI platforms beyond the scope of this Bill. Instead, regulation of "AI tools used by the social network platforms" would be more relevant. This inclusion of "AI tools" within the definition will trigger compliance requirements under the Bill for all AI services which do not characteristically operate as social network platforms. Further, it will be vacant just to add AI tools within the definition of Platform and mandate its registration without considering any other provisions for its regulation . Considering the definition, all AI tools shall be subject to such definition irrespective of its nature. It is also to be considered that jurisdictions like EU has developed separate AI laws to regulate AI. Therefore, considering AI within the Bill is not a good approach given its different nature.

c. The scope of this definition seems to cover any and all kinds of digital intermediaries or content such as online games, or news and journalistic content, news aggregation etc. To address this, the Bill may clarify what kind of intermediaries will/will not be treated as Social Network Platforms. This clarification is important for online businesses that allow registered users to comment or be part of community forums, as well as for service providers who facilitate interaction amongst registered users as one facet of a diverse service offering.

   The similar approach was considered in the EU Digital Service Act, where the Act does not automatically categorize all interactive online services as social networks rather it distinguishes between different types of online services based on their primary function. For instance, comments section in an online newspaper is considered ancillary to its main service (publishing news under the editorial responsibility of the publisher) and is therefore not classified as an online platform. In contrast, a social network that stores and disseminates user comments is classified as an online platform service, as user interaction is a core feature rather than a minor aspect of the service. Similarly, cloud computing and web-hosting services are not considered online platforms if public dissemination of information is only a minor or secondary function.

2.2. Definition of Hate Speech

The definition of "hate speech" under Section 16(1)(a) of the Bill encompasses activities related to posting, sharing, commenting, live streaming, reposting, tagging, hash-tagging, or mentioning any content or doing any other activity of similar nature on a social network to incite violence or hatred against an individual, group, or community, or disrupt social harmony. The Bill imposes a fine of up to NPR 5,00,000 for making hate speech.

The following list contains international principles and jurisprudences that should be reflected in the domestic laws on incitement to hatred:

- The Johannesburg Principles of National Security, Freedom of Expression and Access to Information recognizes criticism of (i) government policy or the government itself, (ii) the nation, or its symbol, public officials etc. as protected expressions, and it should not be subject to punishment unless the criticism or insult was intended and likely to incite imminent violence.

- The Rabat Plan of Action outlines a six-part threshold ("Rabat Test") for defining hate speech that incites to discrimination, hostility or violence. This includes the assessment of context, speaker's position/status in the society, intent, content and form (e.g., provocative and direct), extent of the speech act (public, magnitude and size of audience), reasonable probability of incitement.

- Likewise, state should ensure that the three-part test under the ICCPR – legality, proportionality and necessity – for restrictions to freedom of expression also applies to cases of incitement to hatred.

- The approach recommended by UN Strategy and Plan of Action on Hate Speech may further be adopted to make a distinction on the expression to ensure only rigorous criminal expression (like hate speech inciting violence) are criminally punished and civil suit or administrative penalties are levied for speech that may not be criminal but are socially inappropriate (for example -harming a person's reputation, misleading advertisements).

- The Camden Principles on Freedom of Expression and Equality requires that restrictions on free speech in the law (relating to hate speech) are clearly and narrowly defined and respond to a pressing social need; are the least intrusive measure available; are not overly broad, so that they do not restrict speech in a wide or untargeted way; and are proportionate so that the benefit to the protected interest outweighs the harm to freedom of expression, including with respect to the sanctions they authorize.

- In the landmark judgement of Shreya Singhal vs Union of India (2015), the Indian Supreme Court has interpreted that mere discussion or even advocacy of a particular cause howsoever unpopular is at the heart of freedom of expression. It is only when such discussion or advocacy reaches the level of incitement that law may be made curtailing the speech or expression that leads or causes public disorder.

Including activities such as "posting, sharing, commenting, live streaming, reposting" as hate speech could criminalize a wide range of online interactions even those that may not directly intended to incite violence or hatred. For instance, as per the Bill, the simple act of tagging or mentioning someone in a discussion deemed controversial, even without endorsing the content, could be interpreted as hate speech. This not only creates a chilling effect on free speech but risks imposing sanctions against legitimate speech including journalistic reporting or satire.

International principles recommend formulation of a narrow definition of hate speech, as broad definitions leave room for arbitrary application of the law. The definition under the Bill is excessively broad and the provision does not factor in any kind of threshold applicable for a speech to constitute as hate speech. This will create unpredictability in the enforcement of the law and can lead to abuse, as regulatory authorities may have significant discretion in deciding what constitutes hate speech. The Bill gives exclusive power to the governmental authority to punish any individual who unknowingly share or engage with content deemed as hate speech.

It is also to be noted that the act of inciting violence or hatred against an individual, group, or community, or disrupt social harmony has already been captured in existing laws of Nepal (Section 47 of the Electronic Transaction Act (2008), Section 49, 65 of the National Penal Code 2017) which impose imprisonment and/or fine for violation of the same. Overlapping provisions on the same offence may lead to legal uncertainty and inconsistent application of the law.

Further reference can be made to Section 66A of the Information Technology Act 2000 of India (one of the references undertaken by Nepalese Government to draft the Bill) which was considered unconstitutional due to its vague and open-ended definition which made it arbitrary. Despite being declared unconstitutional, there has not been any amendments made to Section 66A however, the takeaway from the decision is that the limitation imposed on a person in enjoyment of the right should not be arbitrary or of an excessive nature, beyond what is required in the interests of the public (*A test also laid down in the case of Chintaman Rao vs. State of Madhya Pradesh*).

Recommendations

a. The "posting, sharing, commenting, live streaming, reposting, tagging, hash-tagging, or mentioning any content or doing any other activity of similar nature" aspect of the definition should be removed to mitigate legislative ambiguity and arbitrary enforcement.
b. It's important to note that hate speech can only be directed at individuals or groups of individuals. It does not include criticism of government policy or the government itself.
c. The definition should be narrowed to maintain alignment with international law. Further, the mere act of sharing/commenting/mentioning or doing any other activity of similar nature on a social network without the intent to incite violence should not be an offences especially in a country like Nepal, that has a low digital literacy rate (31%) with a lot of users who often engage with content without fully understanding its implications.
d. The Bill should not rely on government authority's decision to impose sanctions on a person for making hate speech and should ensure the right to a fair and public hearing by a competent, independent and impartial tribunal or a judicial body. The right of correction and right of reply should be ensured during the enforcement of the provision.

e. While legislating it should also be kept in mind that criminal proceedings have been initiated and fine has been imposed on a "stand-up comedian" for making jokes, which is unlikely to be considered so in other jurisdictions that adhere to freedom of expression. It adds another responsibility on our lawmakers to ensure that there is no risk of misuse and provide for clear guidance and strict standards on which hate speech will be evaluated.
f. In addition to the above, government should build the capacity to train and sensitize security forces, law enforcement agents and those involved in the administration of justice on issues concerning the prohibition of incitement to hatred.

Likewise**,** Misuse of Social Network under the Bill includes any act of posting, sharing, commenting, live streaming, reposting, tagging, using hashtags, mentioning, or any other similar activity on social media that is against this Act or prevailing laws. The definition of "misuse of social network" should be removed as this becomes redundant when the Bill already provides the list of restricted activities and applicable punishment/remedy mechanisms. The Bill also should focus on preventing harm through clear content moderation rules, risk assessment and enforcement mechanisms rather arbitrarily restricting lawful online behavior.

3. CONTENT TAKEDOWN

Section 13 of the Bill allows the Department to order the removal of unlawful content from social media platforms. The Bill provides power to the Department to issue necessary orders to the concerned licensed institutions or the point of contacts based in Nepal, to remove the content temporarily or permanently or in partial or fully. The Department on its own or upon examining the complaints received on the content being against the Bill or prevailing laws of Nepal, can issue such orders. The concerned institutions or point of contact must immediately remove such content upon receiving of such order. If the platform fails to comply, it faces a fine of five lakhs to fifteen lakhs rupees and may need to compensate the victim. A rapid response team, under Section 36, can also take immediate action to remove or block access to content to protect the victim's rights. The Bill further provides for the requirement to provide user details to investigate crime as per the Bill to the concerned authorities, when requested.

Content takedown has been a debatable issue as it has a direct link with the freedom of speech and restrictions of such needs to follow due process. Due process refers to fair, transparent, and just legal procedures that ensure individuals or entities are not deprived of their rights arbitrarily. In the context of content takedown, it means that any removal of speech should adhere to legal standards, provide opportunities for appeal, and be subject to judicial or independent oversight. The similar principle of due process has been provided by various international documents, i.e.:

a. The Johannesburg Principles of National Security, Freedom of Expression and Access to Information provides that there should be full and effective judicial scrutiny of the validity of the restriction on expression by an independent court or tribunal.
b. Manila Principles on Intermediary Liability provides that Content must not be required to be restricted without an order by judicial authority and further provides that such request for restriction of content must be clear, be unambiguous, and follow the due process.
c. Under international human rights standards, legitimate restrictions on freedom of expression should conform to the strict threshold of the Three-Part Test under Article 19(3) of the ICCPR.Under the test, decision about legality of a specific piece of content should follow due process and be open to review by a judicial body, following the three-part test on legitimate restrictions to freedom of expression wherein the restriction should have: (i) a basis in law, (ii) have a legitimate aim, and (iii) be necessary and proportional.
d. The Digital Service Act issued by the European Union has adopted the transparency principle on social media, which requires social media platforms to be transparent in content moderation. The act requires platforms to have mandatory procedures in place for removing illegal content, inform user when account gets restricted and further should provide right to appeal such decisions.

The Bill does not meet the standard of (a) judicial review and (b) takedowns request should be necessary and proportional. The Bill lacks a judicial review mechanism and grants authority to the Department to issue takedown notice of any such content which they deem unlawful. Neither the Bill provides for the appeal mechanism to the social media platforms nor to the user to challenge decision of the Department. Section 13 of the Bill provides power to the Department to issue necessary orders

to the concerned licensed institutions or the point of contacts based in Nepal, to remove the content temporarily or permanently or in partial or fully. The Department on its own or upon examining the complaints received on the content being against the Bill or prevailing laws of Nepal, can issue such orders. To vest all power within the executive is against the notion of separation of power. Determining any content as unlawful need to undergo rational test as also advocated by ICCPR, which hence is required to be accessed by the judicial review.

The Bill also lacks provisions in relation to transparency and accountability of the government and social media platforms. As provided by the Manila Principles on Intermediary Liability, any notice for take down of the content must be clear and unambiguous, the content takedown request to be issued by the Department must amongst others, disclose (i) the legal basis on which the take down request was issued, (ii) the law which was violated (iii) timeline for removal of content and right to appeal such notice etc. Furthermore, it is highly recommended that the Bill incorporate principles similar to those in the EU's Digital Services Act, which mandate transparency in content moderation. These include mandatory procedures for removing illegal content, notifying users when their accounts are restricted, and providing them with the right to appeal such decisions.

Due to lack of due process, it is likely that there may be arbitrary power grantedto the government leading to controversies. Therefore, complying with the international principles, the due process and transparency must be abided to ensure legitimate restrictions to freedom of expression.

Recommendations

a. The Bill should focus on the systems and processes used by platforms, rather than allowing discretion to the Department to judge the appropriateness or legality of unitary pieces of content. The Bill should also mandate the platforms to develop risk mitigation mechanisms to prevent the spread of illegal content. Like Digital Service Act, requires platforms to conduct system risk assessments to detect and reduce potential harm through moderation tools, user report systems and transparency requirement.
b. The decision on limitations or take down of specific types of content should be allowed to be reviewed by an independent judicial system/court, following a due process of law and in compliance with the three-part test. This test should be specifically provided in the law.
c. The Bill should require platforms to be transparent in their content moderation including but not limited to requiring platforms to disclose their moderation policies and its implemented, notify user for their content being restricted, right to appeal for such decision amongst others.
d. The Bill should explicitly require the authority to conduct a thorough internal assessment before issuing a takedown notice, ensuring:
   (a) **Legality and Justification** – Aligning with the Manila Principles on Intermediary Liability to confirm that the content violates applicable laws.
   (b) **Impact on Freedom of Expression** – Assessing proportionality in line with the UN Special Rapporteur on Freedom of Expression to prevent undue restrictions.
   (c) **Transparency and Accountability** – Following the EU Digital Services Act by notifying users and providing appeal mechanisms.
   (d) **Necessity and Proportionality** – Ensuring compliance with Article 19 of the ICCPR, requiring restrictions to be lawful, necessary, and proportionate.

4. LICENSING

Traditionally, business registration requirements are based on where businesses physically operate, i.e., where goods are sold or where services are provided. With the digital economy, for digital platforms and service providers, registration models are shifting instead to where consumers reside. This requirement is costly and burdensome for service providers, which is made even harder by complex business registration processes. The difficulty increases as digital platforms and service providers span multiple sectors.

The Bill mandates obtaining license by the social media platforms for providing its services in Nepal and further requires that such license be renewed every two years, with the government holding exclusive authority over the process. The Bill further grants the Department the exclusive authority to decline license renewal at its discretion. An appeal against such a decision may be made to the Ministry, whose decision shall be final. This concentration of power grants the government substantial

control over social media regulation, without checks and balances, as the licensing system is managed solely by the government rather than an independent regulator. The Bill also fails to provide for any pre-defined and limited ground for de-registration. Licensing in itself brings any institutions within the larger control of the government and further providing renewal requirement without predefined ground allow arbitrary power to the government to reject renewal of the platforms. Further, no judicial oversight/review mechanism to such arbitrary power is a bigger threat to social media and freedom of expression.

It is essential for the government to clearly justify the rationale behind requiring social media platforms to obtain a license to operate in Nepal. Nepal has already implemented a digital service tax for foreign service providers earning revenue from Nepali users, ensuring compliance with tax obligations. If the government's objective is to hold social media companies accountable and improve access, this can be done without a strict licensing requirement. Instead, platforms could be required to appoint points of contact or legal representatives who are easily accessible through digital means, even if not based in Nepal.

Another significant issue with the Bill is the requirement for all foreign social media platforms used in Nepal to obtain a license and establish a point of contact, even if they have just one user in Nepal. This provision seems impractical, imposing strict obligations on platforms regardless of their size or engagement.

To provide with some of reference on how licenses requirement is dealt internationally:

1. The EU Digital Service Act does not mandate a licensing requirement for providers that do not have an establishment in the EU but offer services, but requires they have a point of contact, and where necessary a legal representative, allowing for communication with member states authorities.
2. Singapore can be seen as one of the examples of jurisdictions where the has no requirements for registration of foreign service providers, applications, pre-approvals, or local presence. It has developed a Content Code for OTT, video on demand, and niche services for content providers to comply with and reserves the right of authority to reach out to providers regarding the code.
3. A similar licensing requirement recently adopted by Malaysia has been criticized for providing government with largely unrestricted power to control the operation and use of nearly all media in Malaysia.

Recommendations

a. Remove the additional licensing requirement only for the purpose of content regulation (for example to collect tax on the revenue earned from Nepal, the social media platforms having certain revenue threshold are already required to get registered as per Digital Service Tax). A dedicated point of contact readily accessible to regulators at all times shall fulfill the intent of the government and further will not create additional burden to the foreign social media.

b. As provided by the UNESCO Guideline the definition should clarify which social media platform services are in scope, identify the platforms by their size, reach, features, and the services they provide. Further, the Bill needs to distinguish between (a) registration requirements and (b) content regulation to ensure that the registration requirement shall trigger to a specific size or feature platforms however, the content regulation shall be applicable to all the platforms irrespective of its registration. Similar approach has been adopted by the EU in the Digital Services Act which defines large online platforms based on active user.

5. ESTABLISHING POINT OF CONTACT

The Bill mandates establishing a point of contact within Nepal by foreign social media platforms having its user in Nepal. The Bill provides flexibility that such point of contact can be any entity or organization established in Nepal and the foreign social media platforms need not necessarily establish their separate contact office in Nepal. However, it is Prima facia in this global age that local presence requirements should not be necessary for legitimate market participation. Such a requirement increases business costs and regulatory hurdles, and disincentivizes investment by digital platforms.

Regulators can retain oversight and authority without requiring businesses to establish permanent presence in the country. This should be done by creating clear and open communication channels with the service providers. The providers should appoint point(s) of contact or legal representative(s) who need not be based in-country, but with the aid of technological advancements, are immediately available if the need arises.

Singapore can be seen as one of the examples where there is requirement for registration of foreign service providers, applications, pre-approvals, or local presence. It has developed a Content Code for OTT, video on demand, and niche services for content providers to comply with and reserves the right of authority to reach out to providers regarding the code.

Recommendation

a. Flexibility to appoint point(s) of contact or legal representative(s) who need not be based in-country, but with the aid of technological advancements, are immediately available if the need arises. Over time, clear and transparent communication will build trust between service providers and regulators

6. OFFENCES RELATED TO THE USE OF SOCIAL MEDIA

It is to be understood that social media is merely a platform for humans. Harmful acts on social media can be seen in two ways: as entirely new offences or as existing crimes committed in a digital space. Usually, it's the latter case where the acts are already prohibited by the existing laws but committed in new forum (in this social media). The issue lies in the behaviour, not the platform. Crimes like harassment, defamation, incitement, threatening are all crimes and have been for a long time.

S.N.	Crime	Punishment as per existing laws	
		Laws	**Punishment**
1.	*Prohibition of undermining sovereignty, integrity or national unity*	Section 49 (4) of National Penal Code 2017	Imprisonment- Up to 5 years and, Fines- up to NPR 50,000
2.	*Prohibition of Committing Libel*	Section 306 of National Penal Code 2017	Imprisonment- Up to 2 years or, Fines- up to NPR 20,000 or, Both
		Section 47 of Electronic Transaction Act 2008	Imprisonment- Up to 5 years or, Fines- up to NPR 1,00,000 or, Both
3.	*Prohibition of breaching privacy through electronic means:*	Section 298 of National Penal Code 2017	Imprisonment- Up to 2 years or, Fines- up to NPR 20,000 or, Both
		Section 45 of Electronic Transaction Act 2008	Imprisonment- Up to 3 years or, Fines- up to NPR 2,00,000 or, Both
		Section 29 (1) (o) of The Individual Privacy Act 2018	Imprisonment- Up to 3 years or, Fines- up to NPR 30,000 or,

			Both
4.	*Prohibition of Extortion*	Section 253 of National Penal Code 2017	Imprisonment- Up to 3 to 7 years or, Fines- up to NPR 70,000 or, Both
5.	*Prohibition of producing or selling obscene materials*	Section 121 of National Penal Code 2017	Imprisonment- Up to 1 year or, Fines- up to NPR 10,000 or, Both
		Section 47 of Electronic Transaction Act 2008	Imprisonment- Up to 5 years or, Fines- up to NPR 1,00,000 or, Both
6.	*writing letters with dishonest intention of causing annoyance*	Section 300 of National Penal Code 2017	Imprisonment- Up to 1 year or, Fines- up to NPR 10,000 or, Both

The table illustrates that existing laws already cover the crimes further penalized by the Bill. While adjustments to current laws or addressing certain gaps may be necessary, there is no compelling justification for introducing a separate set of offences solely for acts committed on social media or digital platforms. Crimes should be addressed based on their nature rather than the medium through which they are committed.

7. RESTRICTIONS ON ANNONIMITY

Section 27 of the Bill prohibits operation of any social media pages, groups or profiles under a name other than the user's legal name. Such action may lead to imprisonment and fines. While the intent may be to discourage dissemination of unlawful content or criminal activities from such accounts, the outright banning of pseudonymous accounts is not a preferrable solution. The outright ban on the pseudonymous accounts is against the principles laid down by UN Special Rapporteur on Freedom of Expression, which advocates that the anonymity is pre-requisite for democratic participation. Many users rely on pseudonyms to discuss sensitive topics such as political dissent, LGBTQ+ rights, and whistleblowing. It is needless to say the importance of anonymity, especially for activist, journalist and marginalized communities etc. to express and enhance information and ideas. The similar anonymity still exists in in real life case, where individuals can send anonymous letter or make anonymous calls in several instances including reporting of crime to some authorities (Like corruption, sexual harassment).

Further, the Bill mandates social media platforms to identify users prior to allowing them to use the platforms. This is one of the mechanisms used to verify age of the user in order to ensure that the platforms (mostly with adult contents) are not accessible to children. For instance, the Online Safety Act of UK requires platform (specially dealing with pornography and certain other types of harmful content) to introduce age assurances to ensure that the children are not normally able to encounter it. While the mandate to disclose the identity in our Bill may be considered valid, it is also proportionate to allow people thereafter to use websites using pseudonyms or anonymously. However, the platforms must ensure the privacy and security of the data. Likewise, the Section 12(J) of the Bill requires providing of user details to the concerned authorities for the investigation of crime as per the Bill, however, fails to provide for the requirement of judicial order prior to requesting such user details.

The EU Digital Service Act can be taken as reference where the law does not impose, the Digital Service Act does not impose an obligation for users to use real names. It focuses more on platform responsibility for content moderation rather than mandating the identification of each user. Platforms can still allow pseudonymity or anonymous participation while ensuring the removal of harmful content. Furthermore, it is important to note that in the digital age, the identity of a user is often linked to their IP address, and any action performed by that address can be traceable, enabling platforms and authorities to trace activities, when necessary, without compromising the user's anonymity by requiring real names.

Recommendation:

1. The provision to restrict anonymity should be removed and emphasis on platform-based accountability (as also adapted by EU Digital Service Act), where platforms are obliged to take responsibility for the content and services they offer and rather relying on government-mandated identity disclosure.

8. ADDITIONAL ISSUES TO BE INCLUDED IN THE BILL

8.1. Provisions in relation to Child Protection

Children can be one of the vulnerable groups in internet crime and further it has rigorous effect to children. The Bill needs to ensure safe internet use to efficiently combat violations of children right online. Different international institutions like Organisation for Economic Co-operation and Development (OECD), UNICEF, International Telecommunication Union has issued numerous guidelines for policy makers to implement policies and strategies that will protect children in cyberspace and promote their safer access to all the extraordinary opportunities online resources can provide.

Recommendations

To sum of all the recommendations made by such reports, the Bill amongst other needs to have at least provision for:

a. The online platforms should develop mechanisms to assess the reliability of age verification tools based on content and the child's age. \
b. The online platform should create online tools for easy reporting of online violence and providing help and support.
c. A dedicated point of contact for communication and take down of abusive content within 2 hours of a judicial removal order is predetermined.
d. Rating of the content and only display the appropriate content to ensure children are safe online.
e. Develop parental control/access tool.

8.2. Data Privacy

The Bil lacks strict provision on data privacy and security. There have been past instances of data breaches in Nepal, but no significant investigations were conducted, nor were there any substantial legal discussions or developments to address the issue. This highlights a critical gap in the country's approach to data security.

Various international guidelines are in existence which provides for fundamental principles to be adopted by any jurisdiction to ensure that data privacy laws are consistent and compatible across borders, facilitating the flow of information and commerce between countries. Documents like Universal Declaration of Human Rights 1948, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980, Convention 108 + (Convention for the Protection of Individuals about the Processing of Personal Data), Fair Information Practice Principles, 1973 lays down principles for data privacy which deals with principle of security, integrity, access, accountability amongst others which are to be undertaken as baseline of developing laws and policies by any nations.

The Bill needs to establish clear guidelines for data collection, storage, transfer and usage while ensuring accountability for breaches. It should also outline penalties for violations, require

organizations to implement strong security measures, and grant individuals' greater control over their personal data. Without proper legal frameworks, the risk of data misuse, identity theft, and cyber threats will continue to rise. Developing a well-defined data protection law will enhance privacy, boost public trust in digital platforms, and align Nepal with global standards on data security.

Recommendations

a. Minimum security standard to be maintained by the platforms
b. Make arrangement for the audit of the security system
c. Reporting of the breaches to the authorities
d. Creation of a separate data protection authority which shall oversee the data privacy issues
e. Mechanism for cross border transfer of data including security of data
f. Right of the data subject (right to rectify, right to erasure etc)

Conclusion

The government should move beyond traditional regulatory approaches (such as licensing or outright shutdowns for non-compliance) and adhere to standards of international law. Such shutdowns not only restrict global access to information but also impact fundamental rights, including those related to work, health, and education, while imposing significant economic costs and hindering development. There exists an opportunity for the regulators to dive deeper into meaningful areas of intervention such as market interventions (taxes, competition, e-commerce) or design regulations (product features/product safety), rather than direct speech/content regulation. It is high time that these opportunities are realized and effectively implemented.

To address the significant gaps in Nepal's digital legal regime, we recommend bridging these gaps through the formation of new laws or amendments to existing ones. To highlight some; (i) Nepal will require a comprehensive law regulating digital privacy, which can be achieved through amendments in the existing Privacy Act 2018 (2075) (ii), the duplication of laws like requirement of licensing of social media in Cybersecurity and IT Bill 2024 must be removed and further Cybersecurity and IT Bill 2024 be developed as a comprehensive cybersecurity laws for the cross-border cooperation against technology-facilitated crimes. Further, the government must also ensure that cybersecurity bill also aligns with international standards like the Budapest Convention to ensure effective cross-border cooperation. As cybersecurity bill will be the comprehensive law for regulating the techno crime, the existing Electronic Transaction Act 2008 (2063) shall be replaced (to remove the duplicity of law) where the provisions relating digital signature may be incorporated in the E-commerce Bill.

Lastly, in shaping our digital regulation, we must not formulate digital laws in isolation from international principles, nor should we repeat past actions of arbitrarily banning and unbanning apps without valid legal grounds. A well-structured legal framework should be rooted in due process, transparency, and judicial oversight ensuring that regulatory actions are clearly justified, proportionate and legally sound by adhering to the global best practices.