Social Media Regulations: A Comparative Analysis of India, Australia and Norway

Ms. Geetanjali Pabreja[1], Harneet Kaur[2], Krish Arora[3], Vandana Kumari[4]
[1]*Assistant Professor, PG Department of Economics, SCD Government College, Ludhiana*
[2]*Student, PG Department of English, SCD Government College, Ludhiana*
[3]*Student, PG Department of Economics, SCD Government College, Ludhiana*
[4]*Student, PG Department of Economics, SCD Government College, Ludhiana*

Abstract - Social media is a digital Internet based platform where people connect , share their views and ideas, information, opinions and multimedia content with others. Social networking platforms such as facebook, WhatsApp, twitter , youtube, instagram, snapchat have become an essential part of our society. People use it for communication, marketing, education, entertainment and networking. However, the rapid increase of false information, cyberbullying, harassment, privacy violation have compelled the government to synchronise usage of social media. This study presents a comparative analysis of various regulatory frameworks adopted by India, Australia, and Norway to regulate social media. These countries have three different regulatory philosophies: India has executive-driven compliance model, Australia has safety-oriented and harm-prevention approach, and Norway's model is driven by rights-based and privacy-centered regulatory system. The findings reveal that India has introduced several judicial measures, including the Information Technology Rules 2021 and the Digital Personal Data Protection Act 2023, but various challenges remain concerning transparency, institutional independence, and protection against the misuse of executive authority. By examining these contrasting regulatory approaches, the study tries to provide a comparative analysis and point out key lessons for social media regulation in India.

Key words: Social media regulation, comparative analysis, online safety, India, Australia, Norway

I. INTRODUCTION

Social media regulation has become one of the most important and debated areas of public law in the 21st century. Different platforms like Instagram, Facebook, and WhatsApp are not mere applications but primary source of news and a medium through which millions experience relationships, form opinions and access news. This penetration of social media in every sphere of life poses complex challenges to the government: how will the government protect it's citizens from misinformation, child exploitation, incitement of violence and data misuse while making sure that the regulatory power isn't turned into a tool of political control?

Different democratic societies have come up with different answers to this question India with approximately 491 million social media users relies on the Ministry of electronics and information technology granting it power to block content and compel platform compliance. Australia has adopted an institutionally independent model, through the eSafety commissioner and the world's first legislative ban on social media for children under 16. Norway follows European Union's regulatory mechanism, treating internet and social media regulation as a matter of protecting people's fundamental rights, such as privacy and freedom of expression. It follows major EU laws like the General Data Protection Regulation (GDPR) and the Digital Services Act. In order to restrict someone speech, a court must approve it through a justifiable and reasonable evidence. This paper undertakes a comparative analysis of these three models.

II. EXTENT OF SOCIAL MEDIA USAGE

According to DataReportal report there are over 5.6 billion social media users as of 2025, a figure that represents nearly two-thirds of the world's population. Asia has the largest number of users with 60% of all the social media users in the world. In high income countries in Northern Europe such as Norway more than 99% of people have internet access. Developing nations like India has 491 million social media users which represent 33.7% of its 1.46 billion people. The 18-34 age group uses social media the most.

Table 1: Social Media Usage — India, Australia, Norway, and Global Comparison (2025)

Country	Users (2025)	% of Population	Avg. Daily Use	Top Platform
India	491 million	33.7%	2h 30m	WhatsApp / YouTube

Australia	~20 million	~73%	1h 47m	Facebook / YouTube
Norway	~4.2 million	~75%	1h 30m	Facebook / Instagram
Global	5.17 billion	~64%	2h 23m	Facebook / YouTube

Compiled by authors. Sources: DataReportal (2025); World Population Review (2025); Statista (2024)

III. NEED FOR GOVERNMENT REGULATION

3.1 Social Harm and Real-World Violence

Social media users frequently face cyber harassment, trolling and internet tracking and sometimes these platforms are used to spread misleading claims by criminals and political parties which lead to catastrophic consequences. Incidents of cyber security in India have arose from 10.29 lakh in 2022 to 22. 68 lakh in 2024. In 2018, 32 people lost their lives in mob lynching after spread of misleading information on WhatsApp, asserting that child kidnappers were wandering in villages. In supreme court this issue was also discussed in case of Tehseen Poonawala versus union of India, which dealt with mob lynching and misleading information. During the same year, another big controversy was the Cambridge analytica scandal. Personal data of many Facebook users was collected without their consent and was used to influence the elections. This poses serious concerns about the privacy and democracy. (Shankar & Ahmad, 2021).

3.2 Psychological Harm

Social media has emerged as a crucial contributor of psychological harm on younger population by reducing their potency, interrupting their sleep pattern and exposing them to superficial comparisons. The U.S. Surgeon General's advisory encounter that adolescents who spend more than three hours daily on social media face double the risk of depression and anxiety symptoms (HHS, 2023). Pew Research (2024) found that 46% of teenage girls reported that social media developed feeling of inferiority complex in them.

IV. REVIEW OF LITERATURE

1. Klonick (2017) examined the role of social media platforms in regulating online speech and outline as "new governors" of digital Transmission. She underlines that platforms use association's recommendation content moderation policies and algorithmic command to Synchronize user behaviour and online conversation. Klonick assert that although these system help to control destructive content, they elevate concerns about transparency, answerability and freedom of expression. For that reason, she indicate that government intervention is mandatoryto ensure fair and democratic governance of social media platforms.
2. Balkin(2018) emphasized that government regulation in social media usage is must be balanced. He says that excessive regulation can threaten democratic values and civilian autonomy instead no regulation leads misinformation, hate speech and digital harm.
3. Sunstien(2018) point that social media encourage echo chambers and polarization, reduce Republican thought. He advocate that limited and carefully outlined regulatory interventions may be necessary to ensure exposure to sundry view points while safeguarding freedom of expression.
4. Robert Gorwa (2019) emphasized the concept of platform governance in his research and argued that social media platforms are regulated through an amalgamation of government laws, platform self- monitoring and communal norms. Gorwa highlighted that government intervention is essential for digital platform accountability. Regulation should involve multiple stakeholders, not only the state .
5. Shankar and Ahmad (2021) evaluated the information technology Act 2000 and IT rules 2021. They look into how the Indian government monitor social media platforms to control misuse, cybercrime and fraud. They analysed that although the laws exist but enforcement is fragile due to technical intricacy, ignorance and limited organizational capacity.
6. Santos, Cazzamatta, and Napolitano (2025), in a cross-national qualitative comparative analysis of five national platform regulation regimes, found that most jurisdictions adopt vague definitions of misinformation, creating expansive discretionary spaces that risk over-enforcement. They found that only Brazil's framework explicitly addresses AIgenerated content, and that government-controlled fact-checking mechanisms — precisely the model India's 2023 Rules amendment attempted —consistently fail tests of proportionality and democratic legitimacy.

4.1 Research Gap

The subject of social media regulation has become an important one for scholastic inquiry yet,several significant gaps remain.First, most comparative work focuses on the United States, the European Union, and China, neglecting India. Given India's scale of 491 million users, it becomes important subject to study and analyse. Second, there is no existing study that directly compares India, Australia, and Norway. These three countries adopts distinct regulatory philosophies — executive controlled, institutionally independent, and rights-centered. Their comparison yields insights that broader surveys do not. Third, there has been more focus on content moderation and misinformation, with less attention to age-based restrictions, data protection asymmetries, the governance of algorithmic

harm, and the specific risk of political misuse in government-controlled systems. This paper addresses these gaps directly.

V. OBJECTIVES OF THE STUDY

1. To review the regulatory framework governing social media in India
2. To conduct a systematic comparative analysis of regulatory approaches in India, Australia, and Norway across five dimensions: institutional design, content moderation, age-based restrictions, data protection, and traceability and encryption
3. To derive recommendations for India's Regulatory framework

VI. REVIEW OF SOCIAL MEDIA REGULATIONS IN INDIA

6.1 The IT Act, 2000

The Information Technology act 2000, is the primary regulatory mechanism. There are various sections under this act which deal with hacking and computer-related offences; punishment for cheating by impersonating someone; punishment for violation of privacy, cyber-terrorism and publishing or forwarding obscene material in electronic form. The most crucial of all is Section 69 A. This was introduced through a 2008 amendment that empowered the central government to block any content that is a threat to sovereignty, public order, national security or foreign relations and the blocking orders under this sections are kept of confidential from the affected user and general public.

6.2 Shreya Singhal v. Union of India (2015)

Under this case the Supreme Court struck down section 66A of the IT act that was used to arrest individuals for online posts that were deemed offensive on the grounds that its language was unconstitutionally vague and that it affects the right to freedom of expression.

6.3 IT Rules 2021:

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, represent the most significant expansion of India's social media regulatory framework.Platforms with over five million users were designated 'Significant Social Media Intermediaries'. These were required to appoint a Resident Grievance Officer, Chief Compliance
Officer, and Nodal Contact Person in India, making executives personally reachable by Indian law enforcement. Furthermore, under these rules, content must be removed within 36 hours of a government or court order; non-consensual intimate images within 24 hours.

Rule 4(2) the traceability mandate requires significant platforms to identify the 'first originator' of any message. WhatsApp challenged this provision in the Madras High Court, arguing that compliance would require breaking end-to-end encryption and creating mass surveillance infrastructure. The provision remains in litigation. The 2023 Amendment gave government notified fact checking units to label content as 'false or misleading', after which platforms would lose safe harbour for leaving it up. The Supreme Court stayed this amendment, recognising the profound democratic risk of a government-controlled arbiter of truth. By 2026, the takedown timeline for government orders had been further compressed to three hours — the shortest in the world (Drishti IAS, 2025).

6.4 Digital Personal Data Protection Act, 2023

The DPDP Act 2023, is India's landmark legislation regulating the processing of digital personal data. With emergence of this act consent of the user is required to process his/her data, individuals have the right to access information, correct, update, or erase their data, and nominate someone to exercise rights in case of death or incapacity. Moreover, to process data of children (under 18) parental consent is required. The government has imposed strict ban on tracking, behavioral monitoring, or targeted advertising. Data fiduciaries must implement security safeguards, and delete data once its purpose is met. Non-compliance can lead to massive fines (e.g., up to ₹250 crore for failing to prevent a data breach). However, the technical mechanism for age verification are loosely unspecified in pending rules as of 2026 and the other rules are poorly implemented.

VII. COMPARATIVE ANALYSIS: INDIA, AUSTRALIA, AND NORWAY

7.1 Institutional Design and Independence

India across the years has maintained a rigid stance over a coercive oversight across social media platforms, though it ensures a temperate reconciliation with privacy protection through its DPDPA (Digital Personal Data Protection) regulations providing a consent based mechanism of digital privacy and personal data security however the government and other departmental bodies have an overruling authority under section 17 of the constitution to take necessary action against any perceived threat to sovereignty ,territorial integrity ,and public order .The government does have the right to intervene and access the personal data and digital activity record of an individual or an organization without any prior notice or consent . This approach contrasts against the Puttaswamy (2017) decision of the Supreme Court of India which inclines towards a policy of protection of digital privacy against state interception and infringement through non consensual access and espionage. One of the major issue that lies at the foundation of government controls that separates India from Norway and Australia is that the ministry has the complete authority of

discretion and there is no independent authority of oversight that can monitor the activity of the executive based ministry that at times can infringe on the right of people to freedom of speech and expression .

Norway takes upon an entirely opposite approach towards social media and digital surveillance under the provisions of GDPR (General Data Protection Regulation) as formulated by joint EU committee. Any intervention by the governmental authorities requires judicial permissions and there are provisions for legal protection and appropriate safeguards to protect privacy.
Individuals possess the right to seek redressal against any act of erasure, interception, access and portability. It also ensures that government agencies remain accountable to independent statutory EU bodies which gives Norway an advantage which India should adopt through a stronger institutional compartmentalization rather than through external leverage .The privacy of people and organizations is considered as a fundamental right and this spirit also needs to be impersonated across Indian political diasporas.

Australia defines its position as a middle path between the methodology of India and Norway it's a deliberate institutional counter design. Its e-safety commissioner is appointed for a fixed term and is supposed to remain non affiliated to political zeitgeist. It also defines roles of intervention for separate agencies like ACCC for completion concerns, OAIC for privacy, ACMA for broadcasting reducing chances of political overreach which is evident in India. While it allows its authorities to take action it curbs arbitration of both public and private actors through their act of Telecommunication (interception and Access). Its Privacy retention laws though allow for state access and intervention in matters of serious concern generating a debate on its stance on privacy protection.

7.2 Content Moderation and Free Expression

India's legislation of traceability as per IT rules (2021) section 4(2) makes it mandatory for platforms to furbish details about the origins of messages that brings the government into a conflict with many digital platforms end to end encryption that protects individual privacy. The government arduously stands its ground to be given access so as to curb chances of mob violence, terrorism, minors exploitation , though it remains a matter of serious debate as such a mechanism stands as symbolic to the creation of an infrastructure of internal state espionage reminiscent of the cold war era. The rules continue to prohibit the use of 15 types of content languages terming them as harmful, disrespectful, and patently false. The result of such overruling authority of the government authorities is that they can even access and remove content that under their perception is harmful or uncomfortable rather than being unlawful.

Australia with its Online Safety Act 2021 defines specific categories of content that is considered to be unlawful and is mentioned in its criminal law jurisdictions which consists of action being taken against minor exploitation, terror content, Extreme violence, serious hate speech, cyber bullying of children, and nonconsensual intimate images. All of this stands as a testament to State's commitment of proportionate action and not arbitrary intervention these regulations ensure public safety from specified harms and aren't built to regulate the general public discourse. The framework stands in support of legitimate content regulations like clear definitions, procedural safeguards, and independent oversight.

Norway follows EU patterns of welfare orientation under the Digital Services Act ensures that platforms act against content that is illegal under law the platforms have to explain the reasons of removal of content and are supposed to maintain appeal mechanisms , every restriction must satisfy judicial proportionality, Algorithmic transparency and systemic risk assessment. This approach marks the case for modifying the structure of social media platforms and engagements and not specific individual content instances.

7.3 Age-Based Restrictions and Child Protection

Australia in 2024 enacted the first law (Online Safety Amendment Act) that refrained minors under the age of 16 from using social media platforms this came as the first hard legislation where compliance and consequence of offence were non-negotiable and penalties of 50 million Australian dollars are imposed in case of offence

Norway's approach is less rigorous its age limit is till 15 years and it ensures that platforms maintain a revised data set regarding information of its users age and holds the platforms accountable for systemic errors this framework coupled with digital ID verification and parental consent makes minimum age enforcement under its GDPR act more pragmatic and effective

India's stance on minimum age laws is the weakest of all three nations. The DPDPA Act of 2023 requires parental consent for operating social media platforms but has no verification authorities or specific digital ID's that ensure its effective enforcement. The honorable Supreme court in its ruling refused a ban for social media claiming it to be a Legislature matter however even till this day the legislature hasn't reached any consensus for regulation of social media usage by minors.

7.4 Data Protection and Surveillance

On paper India's DPDPA legislation is a consent based rule however in practice under its section 4(2) the government agencies are given overriding authority of surveillance and traceability which stands as an infringement to the right to privacy of people howsoever the government continues to operate with arbitration and the legislature has turned a blind eye towards the issue

Australia's recent amendments to the privacy act 1988 have increased the leverage of the government to intervene into platforms workings and seek a compelled technical assistance from the platforms in matters of legal concerns regarding its content now this overriding mechanism has drawn some sharp criticism from many spheres of Australian community like in case of India though a safe guard is in place in Australia's case that is it requires authorization to act upon any content and to access personal information of users.

Norway under its GDPR considers privacy of its people as a fundamental right which cannot be infringed upon. Any intervention by the state can only happen after judicial clearance and is monitored by independent authorities, even platforms like Meta have been charged with penalties for infringing on the privacy rights this is a completely different take than India's regulations where there is judicial oversight but government and other executive bodies are safeguarded by contrasting overlapping and ambiguously defined regulations and rights.

Table 2: Comparative Regulatory Framework — India, Australia, and Norway

Dimension	India	Australia	Norway
Governing Law	IT Act 2000 + IT Rules 2021 + DPDPA 2023	Online Safety Act 2021 + Privacy Act 1988	GDPR + EU Digital Services Act (via EEA)
Regulatory Body	MeitY (executive ministry)	eSafety Commissioner (independent statutory officer)	Datatilsynet (independent; reports to EU bodies)
Regulatory Philosophy	Security-first; executive control	Harm-based; institutional independence	Rights-centered; systemic reform
Content Categories Regulated	15 categories — vague terms ('grossly harmful', 'patently false')	8 narrowly defined categories (child exploitation, terrorism, NCII, etc.)	Illegal content only under existing law; platforms explain every removal
Takedown Timeline	3 hours (govt order); 24 hours (NCII)	24 hours (NCII); 72 hours (other defined harms)	No fixed timeline; due process & appeal rights required
Transparency of Orders	Blocking orders confidential under S.69A	Annual public reports; reasons required; court-reviewable	Full transparency; all actions publicly reasoned
Minimum Age for Social Media	No hard ban; 18+ requires parental consent (DPDPA 2023)	16 years — world's first hard ban (2024)	15 years; parental consent below threshold
Age Verification Method	Aadhaar-linked (rules pending, 2026)	Mandatory tech verification; no self-declaration	Digital ID systems; government-issued verification
Traceability / Encryption	Traceability mandatory (Rule 4(2)) — conflicts with E2E encryption	Not required; Assistance & Access Act for targeted warrants	E2E encryption protected; judicial order required for access
Data Protection Standard	DPDPA 2023 (consent-based; broad govt exemption, S.17)	Privacy Act 1988 + 2024 reforms (judicial oversight for state access)	GDPR — strictest global standard; no state override
Platform Penalty	Loss of safe harbour + imprisonment of officers	Up to AU$50 million (age ban); AU$10 million (content)	Up to 4% of global annual turnover (GDPR / DSA)

Notable Case / Outcome	Reuters & 2,000+ accounts suspended under S.69A (2025); SC stayed fact-check amendment	eSafety v. X Corp (2024): public proceedings, Commissioner withdrew — shows institutional limits	Meta fined by Datatilsynet for data misuse; Norway benefits from EU collective enforcement leverage
Independent Oversight	None — Ministry issues and reviews its own orders	Yes — eSafety Commissioner + ACCC + OAIC (distributed)	Yes — Datatilsynet + EU DSA supervisory bodies

Compiled by authors. Sources: DataReportal (2025); Drishti IAS (2025); Doon Law Mentor (2025); Laws Study (2025); Santos et al. (2025)

VIII. KEY FINDINGS

This comparison brings us across several key findings that are of analytical significance:

1. **Institutional independence and regulation quality :** When we consider various parameters of social media regulations of all three nations the most standalone variable of distinction is the oversight of an independent authority over government activities to curb arbitration and authoritarian behavior which attempts to suppress the voice of people and their freedom of expression. The presence of independent authorities with fixed terms and repeal mechanisms present in both Australia and Norway gives them an edge against India in terms of regulatory quality and democratic accountability.
2. **Ambiguous Measures are unacceptable for Democratic Governance :** The regulations in India consist of vaguely defined content like 'grossly harmful' , 'disrespectful and more the terminologies remain unclear and are under discretion of ministry rather than embedded in acts of regulations this again undermines the democratic ideals and infringes on the rights of people and this is something at which both Nations of Norway and Australia hold an upper hand.
3. **Protection of Children and Minors:** This category is where the legislations of India are the most inadequate even though the DPDPA act defines clearly about child safety and its regulatory mechanism and redressal systems are inefficient. India has more than 398 million young users under the age of 18 and still adequate machinery hasn't been developed that can match the prowess of Norwegian grievance redressal or Australian oversight regarding digital ID's of minors and a ban on their usage.
4. **Indian Model is based on Concentration rather than Decentralization:** In a democracy concentration of all power vestiges arbitration and authoritarianism while Australia provides a failsafe against such action through defined roles and mandates to multiple associations like E-safety commissioner , OAIC , ACMA ,And Norway ensures a decentralized network through EU authorities India fails on that democratic principle as overriding authority remains in the hands of ministry of communication and overhauling authority at times also leads to decisions that come under the purview of democratic ideals but are abandoned and left without action of accountability.

Table 3: Summary of Findings — India, Australia, and Norway

Finding	India	Australia	Norway
Institutional Independence	Absent — MeitY controls and reviews its own orders	Strong — eSafety Commissioner has fixed tenure and public mandate	Strong — Datatilsynet operates under EU supervision, no govt override
Transparency & Accountability	Low — blocking orders secret; RTI denied on security grounds	High — annual public reports, parliamentary hearings, court review	Highest — all decisions publicly reasoned; GDPR audit trails
Free Speech Protection	Weak — broad vague categories; chilling effect documented	Moderate — narrow categories; court review; but age ban raises concerns	Strongest — every restriction must meet constitutional + judicial test

Child Protection Effectiveness	Inadequate — no hard age limit; verification rules still pending (2026)	World-leading — first country with hard age ban at 16 + tech verification	Robust — age 15 minimum + digital ID verification + consent framework
Data Protection Adequacy	Weak — DPDPA 2023 has broad S.17 state exemptions; no judicial check on govt access	Moderate — Privacy Act 1988 reformed 2024; some state access allowed	Gold standard — GDPR; no state override; individual rights fully enforceable
Risk of Political Misuse	High — executive controls platforms, journalists, and opposition content	Low — distributed authority; multiple agencies; ministerial direction excluded	Lowest — independent of any political branch; EU oversight layer adds protection
Platform Accountability	Safe harbour loss + imprisonment — coercive but opaque	Civil penalties up to AU$50M — proportionate and transparent	Up to 4% global turnover — most credible deterrent for large platforms
Regulatory Model	Command and control (stateled)	Co-regulatory (independent body + industry codes)	Rights-based co-regulation (EU framework + independent supervisors)

Compiled by authors. Source: Author's analysis based on comparative review of regulatory frameworks

IX. RECOMMENDATIONS

India's digital population is growing significantly with around 490 million social media users which necessitates media literacy across the population. Social media is not a passing phenomenon, it is there to stay and people who lack guidance on its use will inevitably misuse it. In order to use it effectively awareness campaigns must be designed to reach different demographics. Children can be educated through structured school curriculum, while working- age adults can be reached through targeted advertisements on social media platforms themselves—much like how the Reserve Bank of India disseminates fraud alerts via SMS directly to users' mobile phones.

1. Following Australia's ban on social media for children under sixteen, few Indian states have also adopted the same model. Karnataka has banned it for children under 16 and Andhra Pradesh has also decided to ban it for children under 13. But, India should consider a more nuanced approach. It should restrict harmful content within platforms for users under sixteen or eighteen, such as algorithmically-driven short video content that diminishes attention spans rather than denying platform access entirely. To enforce such age-based restrictions credibly, the government should mandate Aadhaar verification while creating account on any social media platforms. However, few state governments have decided to follow Australia's path of banning social media for teenagers. The Karnataka Government has introduced a ban on social media for teenagers below 16, following the suit Andhra Government has also decided to ban it for children below 13.

3.India's existing regulatory framework suffers from a fundamental problem of ambiguity. The Broad and subjective nature of current provisions creates room for governmental misuse, which threatens the very freedoms of expression and speech that a democratic society is built to protect. Hence, it's important to develop clearly defined regulations so that these are interpreted correctly and are not misused by those in power.

4.Finally, and perhaps most critically, India needs an independent statutory body that handles social media regulations. It should function entirely outside the influence of any ruling government or ministry, just as Australia has eSafetycomissioner. Social media is one of the most powerful tools that can be used for manipulating political opinion. Allowing the ruling party any degree of control over its regulation is a threat to democracy.

IX. CONCLUSION

India, Australia, and Norway represent three fundamentally different approaches to regulate social media, India's model prioritizes state security and executive efficiency. It has succeeded in building a legal infrastructure capable of rapid response to defined threats, but at the cost of transparency, proportionality, and democratic accountability. Australia's model prioritizes institutional independence and defined harm categories. It has demonstrated that a democratic government can govern social media effectively without concentrating regulatory power in the executive but its hard age ban raises unresolved questions about exclusion and paternalism. Norway's model treats digital governance as a fundamental rights matter, building regulation on proportionality, judicial oversight, and systemic platform accountability. It is the most principled of the three frameworks, and also the one most dependent on external institutional architecture, the EU regulatory umbrella that India cannot simply import. What the comparison ultimately demonstrates is that the choice of regulatory philosophy is not merely technical. It is a statement about what kind of democracy India intends to remain. A state that governs social media through confidential ministerial orders, with no independent oversight and broad exemptions for its own surveillance or a democratic mechanism that protects citizen’s privacy and ensures digital security.

X. REFERENCES

[1]. Balkin, J. M. (2018). Free speech in the algorithmic society: Big data, private governance, and the future of democracy. UC Davis Law Review, 51(3), 1149–1210.

[2]. DataReportal. (2025). Digital 2025: India. https://datareportal.com/reports/digital-2025-india Doon Law Mentor. (2025). Legal issues and challenges of social media in India. https://doonlawmentor.com/legal-issues-and-challenges-of-social-media-in-india/

[3]. Drishti IAS. (2025). Changing architecture of social media regulation in India. https://www.drishtiias.com/daily-updates/daily-news-editorials/changing-architecture-of-socialmedia-regulation-in-india

[4]. Flew, T., Martin, F., & Suzor, N. (2019). Internet regulation as media policy: Rethinking the question of digital communication platform governance. Journal of Digital Media & Policy, 10(1), 33–50.

[5]. Gorwa, R. (2019). What is platform governance? Information, Communication & Society, 22(6), 854–871.

[6]. Gorwa, R. (2024). The politics of platform regulation: How governments shape online content moderation. Oxford University Press.

[7]. GrabOn. (2025). Social media statistics in India 2025. https://www.grabon.in/indulge/tech/socialmedia-statistics/

[8]. Information Technology Act, 2000. Ministry of Law and Justice, Government of India.

[9]. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Ministry of Electronics and Information Technology, Government of India.

[10]. Klonick, K. (2017). The new governors: The people, rules, and processes governing online speech. Harvard Law Review, 131(6), 1598–1670.

[11]. Laws Study. (2025). Section 69A of the IT Act and online censorship in India. https://lawsstudy.com/section-69a/

[12]. Online Safety Act 2021 (Australia). Federal Register of Legislation.

[13]. Online Safety Amendment (Social Media Minimum Age) Act 2024 (Australia). Federal Register of Legislation.

[14]. Pew Research Center. (2024). Teens, social media and mental health.

[15]. https://www.pewresearch.org/internet/2025/04/22/teens-social-media-and-mental-health/ Puttaswamy (K.S.) v. Union of India, (2017) 10 SCC 1, Supreme Court of India.

[16]. Santos, A., Cazzamatta, R., & Napolitano, C. J. (2025). Holding platforms accountable in the fight against misinformation: A cross-national analysis of state-established content moderation regulations. Journalism Practice. https://doi.org/10.1177/17480485251348550

[17]. Shankar, A., & Ahmad, T. (2021). Social media regulation in India: An analysis of the IT Act 2000 and IT Rules 2021. Journal of Cyber Policy, 6(2), 189–205.

[18]. Shreya Singhal v. Union of India, (2015) 5 SCC 1, Supreme Court of India.

[19]. Statista. (2024). Internet penetration rate in Norway. https://www.statista.com/statistics/

[20]. Sunstein, C. R. (2018). #Republic: Divided democracy in the age of social media. Princeton University Press.

[21]. Tehseen Poonawalla v. Union of India, (2018) 9 SCC 501, Supreme Court of India.

[22]. United Nations Special Adviser on the Prevention of Genocide. (2018). Report on Myanmar. United Nations.

[23]. United States Department of Health and Human Services. (2023). Social media and youth mental health: The Surgeon General's advisory. https://www.hhs.gov/surgeongeneral/reports-andpublications/youth-mental-health/social-media/index.html

[24]. World Health Organization Europe. (2024). Teens, screens and mental health. https://www.who.int/europe/news/item/25-09-2024-teens--screens-and-mental-health

[25]. World Population Review. (2025). Social media users by country 2025.

[26]. https://worldpopulationreview.com/country-rankings/social-media-users-by-country