Page 1051 - 1059 **DOI:** *https://doij.org/10.10000/IJLMH.119161*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 2

2025

The Multifaceted Nature of Social Media Laws and their Implications in India

RAJ SANJAY MITRA [1]

ABSTRACT

In the past few years, the regulation of social media platforms in India has become a prominent subject of debate, especially as the digital landscape continues to transform and expand. This issue is both dynamic and multifaceted, reflecting the complex interactions between technology, legal principles, and societal norms. Social media platforms are often viewed as online tools that enhance interpersonal relationships, fostering social connections among users. These platforms primarily consist of resources that facilitate the sharing and dissemination of information via the Internet and mobile devices. Commonly reported incidents on social networking sites include anonymous threats, bullying, harassment, and stalking. A considerable portion of these incidents go unpunished, leading to a lack of recognition of their severity. The Indian government has enacted several measures to address the unique challenges that arise from the rapid growth of social media, including issues related to misinformation, data privacy, and the moderation of online content. This article will investigate the regulatory framework that governs social media platforms in India, along with the broader context of digital platform regulation, internet laws, and online content moderation.

Keywords: *Social Media, Privacy, Information, Regulation.*

I. INTRODUCTION

Corporate We are currently experiencing a remarkable era characterized by social media, advanced technology, and the internet, which have fundamentally altered our daily lives. In the past, where there were no mobile phones or internet access, our primary sources of information were print media such as newspapers, radio, and television. Today, however, anyone can create their own content on social media platforms. Today, social media platforms have the potential for this content to reach thousands of users. Social media serves as a significant forum for interaction, for personal or professional purposes, as well as for entertainment or academic endeavours. But it also encompasses our personal information, which necessitates proper legal governance and regulation by the government to safeguard individuals against online

[1] Author is a Student at Law Centre-II, Faculty of Law, University of Delhi, India.

 [ISSN 2581-5369]

cybercrime.[2]

The realm of social media law is undergoing significant transformation. In recent years, there has been a remarkable increase in internet usage in India, with a substantial portion of the population now classified as active internet users. Like many other nations, India is grappling with the legal implications arising from the internet's expansion, often finding existing laws inadequate or, in some instances, being utilized as instruments of state control. Social media law is a dynamic field that encompasses both criminal and civil dimensions. It primarily addresses legal issues related to user-generated content and the online platforms that facilitate its hosting or transmission. Key legal challenges associated with social media include the *privacy of content*, which involves the rights of both users and third parties—such as instances where images are shared without the consent of the individuals depicted—alongside concerns regarding *defamation, advertising regulations, and intellectual property rights*. Additionally, content shared on social media may sometimes infringe upon *copyrights, trademarks, or other forms of intellectual property*.[3]

II. WHAT IS SOCIAL MEDIA?

The designation of "social" in the context of media implies that these platforms prioritize user engagement and serve as arenas for collective interaction. Thus, social media can be perceived as online facilitators or enhancers of interpersonal networks, promoting social connectivity among individuals. The majority of social media consists of tools that enable the sharing and exchange of information through the Internet and mobile technology. It merges technology, communication, and social interaction, creating a platform for the exchange of ideas through written content, images, videos, and music. People of all ages are attracted to social media, with a notable inclination among the youth, as it provides an outlet for expressing their views and engaging in discussions on various topics. Different categories of social media exist, including social networking sites like Facebook, WhatsApp, Instagram, and Twitter.

III. THE DETRIMENTAL EFFECTS OF SOCIAL MEDIA

Defamation and Hate Speech

The most frequently reported and observed offenses on social networking platforms include individuals making anonymous threats, engaging in bullying, harassing, and stalking others. A

[2] Kanak Shakya, Mechanisation of Social Network on Modern Era, Manupatra Articles (Dec 11, 2023, 10:04 AM) [https://articles.manupatra.com/article-details/Mechanisation-of-Social-Network-on-Modern-Era]
[3] Ayush Chandra, Laws regulating social media in an Indian Context 1(2) LLJ (2024)

significant number of these offenses remain unpunished and are consequently not regarded with the seriousness they warrant. Defamation on social media can be characterized as the act of compromising someone's social media accounts to disseminate indecent or inappropriate messages to their friends and followers, which may include vulgar language and obscene content, or by posting such material through that individual's account on social networking platforms. Hate speech is defined as aggressive communication that includes derogatory statements and messages that convey prejudice against an individual or group based on specific characteristics. These characteristics may encompass ethnicity, religious beliefs, sexual orientation, caste, national origin, sex, race, gender, and significant disabilities or illnesses.

Cyber Harassment and Online Stalking

"Cyberstalking" refers to a criminal act in which perpetrators utilize the Internet and various electronic devices to pursue individuals. Online harassment, bullying, and abuse on social media platforms are often associated with cyberstalking. This behaviour typically involves repeated acts of harassment or threats directed at a specific person. Cyberbullying and harassment may manifest through threatening or abusive emails, text messages, or the dissemination of personal information online. The intent is to target an individual, either by attempting direct communication or by sharing their private and sensitive data, thereby inducing feelings of distress, fear, and anger. A significant advantage for cyber stalkers is the anonymity provided by social media and the Internet, which enables them to monitor their victims' activities without the risk of being identified. Various psychological factors may contribute to stalking behaviour, including extreme narcissism, hatred, anger, a desire for revenge, jealousy, obsession, mental health issues, a need for power and control, deviant sexual desires, and an addiction to the Internet.

The Influence of Social Media on Privacy Rights

Social media serves as a platform for communication over the internet, originally designed to foster global connections among individuals. Prominent social networking platforms include Instagram, Facebook, and WhatsApp. Users of these platforms experienced a sense of security until the emergence of the 1990s, which marked the onset of cybercrime. It is important to recognize that individuals often disclose their personal information online, whether intentionally or inadvertently. This occurs through activities such as registering for services like Amazon Prime or social media accounts. Alarmingly, approximately one-third of internet users report being unaware of the extent of their personal information available online. The vast amount of data circulating on the internet has led to new legal challenges, for which

 [ISSN 2581-5369]

comprehensive regulations have yet to be established.

Moreover, the risks extend beyond merely safeguarding passwords or refraining from sharing personal details. A wealth of information is accessible online, including social connections, purchasing habits, and frequently visited websites. Failure to secure personal information from cybercriminals can result in significant harm, including the theft of social security benefits, fraudulent claims using one's identity, and the creation of counterfeit documents such as passports and identification cards. Additionally, issues such as sexual predation, cyberstalking, defamation, and identity theft have gained prominence. Research indicates that younger individuals are particularly vulnerable to these cybercrimes, often due to their lack of awareness regarding the potential dangers of sharing personal information. This susceptibility is frequently attributed to their immaturity, which can be easily exploited by malicious actors.

IV. REGULATION OF SOCIAL MEDIA - A LEGAL PERSPECTIVE

The Information Technology Act of 2000 [4] (IT Act) serves as the cornerstone for the regulation of online activities in India, establishing a legal framework to tackle issues related to cybercrime, electronic commerce, and data protection. The Act has undergone amendments to encompass various dimensions of online interactions, particularly concerning social media. It plays a crucial role in addressing the challenges posed by social media, including provisions aimed at combating online harassment and cyberbullying. Notable sections of the Act include **Section 79**, which provides exemptions from liability for intermediaries in specific circumstances, and **Section 66A**, which prescribed penalties for sending offensive messages via communication services. However, Section 66A, previously utilized to combat online offenses such as cyberbullying and harassment, was declared unconstitutional by the Supreme Court in 2015 [5] due to its ambiguous definitions and potential for misuse.

Section 69A grants the government the authority to restrict public access to various types of content for multiple reasons. Should an intermediary neglect to comply with directives to censor such content, they could face imprisonment for a term of up to seven years. This provision allows the government to potentially block any content it considers to meet the broadly defined criteria, and its application has yielded mixed outcomes. There are instances where censorship is warranted, such as in the case of a fake video circulated on Facebook that incited recent communal violence in Uttar Pradesh by falsely depicting violence against the majority community. However, the implementation of government directives is not consistently adhered

[4] The Information Technology Act, 2000
[5] *Shrey Singhal v. Union of India* AIR 2015 SC 1523

 [ISSN 2581-5369]

to, and there is a notable absence of adequate oversight and accountability mechanisms.

Additionally, the vague and expansive nature of the criteria required to invoke this power raises significant concerns. To avoid liability under **Section 79** of the IT Act, intermediaries must adhere to specific regulations. These guidelines, established in 2011, mandate the removal of any information that is deemed grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, paedophilic, libelous, invasive of privacy, hateful, or racially and ethnically objectionable, as well as content that promotes money laundering or gambling, harms minors, or is otherwise unlawful. Sections 69A and 79 have attracted considerably less public scrutiny, likely due to their substantive nature as opposed to the punitive focus of Section 66A. Nevertheless, these regulations create a framework for censorship that may be constitutionally questionable. [6]

Section 67B of the Information Technology Act, 2000 is a recent addition introduced by the Amendment Act of 2008. This provision specifically targets offenses where a stalker preys on minors under the age of 18, disseminating content that depicts these children in intimate situations to instil fear in them. Also, **Section 66E** of the Information Technology Act, 2000, along with Section 354C of the Indian Penal Code [7], addresses the issue of "voyeurism." This term refers to the deliberate act of capturing, publishing, or transmitting images of an individual's private areas without their consent, thereby infringing upon the individual's right to privacy.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[8], introduced in February 2021, mark a significant evolution in the regulation of social media platforms. These rules categorize platforms into three distinct groups: social media intermediaries, significant social media intermediaries, and publishers of news and current affairs content. Key provisions include the establishment of a grievance redressal mechanism, which mandates that users can file complaints regarding content moderation. Additionally, platforms are required to appoint a Chief Compliance Officer, a Nodal Contact Person, and a Resident Grievance Officer in India to ensure that user complaints are addressed within designated timelines. Social media intermediaries must also implement a system for the prompt removal of harmful content, including hate speech, misinformation, and explicit material, within specified timeframes while addressing grievances efficiently.

[6] Kanak Shakya, Mechanisation of Social Network on Modern Era, Manupatra Articles (Dec 11, 2023, 10:04 AM) [https://articles.manupatra.com/article-details/Mechanisation-of-Social-Network-on-Modern-Era]
[7] Indian Penal Code, 1860
[8] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

The Digital Personal Data Protection Act of 2023 sets forth extensive regulations aimed at safeguarding user data on social media platforms. This legislation enforces a principle of purpose limitation in data collection, obligating platforms to explicitly outline the reasons for which user data is gathered and utilized. It introduces stringent consent requirements, ensuring that users maintain significant control over their personal information. Additionally, the Act addresses the issue of cross-border data transfers, stipulating the need for adequate protective measures and explicit consent for the processing of data internationally. The Act confers important rights upon data principals (users), including the right to access their personal data, rectify inaccuracies, and request deletion under certain conditions. It also imposes considerable penalties for non-compliance, with fines potentially reaching up to four percent of global revenue for serious infractions. Furthermore, the legislation enforces data localization mandates, requiring that specific categories of sensitive personal data be stored within the geographical confines of India.

The legal framework delineates comprehensive regulations for content management on social media platforms. The **IT Rules of 2021** mandate that these platforms prohibit certain types of content, such as that which endangers national security, incites terrorism, or infringes upon individual privacy rights. Additionally, the rules require platforms to actively monitor content and promptly remove any that is deemed prohibited, while also obligating them to retain pertinent records for investigative purposes. This framework also encompasses specific regulations concerning political content on social media, especially during election periods. The Election Commission of India has issued guidelines that necessitate the pre-certification of political advertisements and the maintenance of transparency in political communications across social media platforms. These stipulations are designed to avert the misuse of social media for electoral manipulation and to promote equitable practices in digital campaigning.

The implementation of social media regulations involves various agencies and mechanisms. The Ministry of Electronics and Information Technology (MeitY) acts as the principal regulatory body, endowed with the authority to issue directives to social media platforms and ensure adherence to legal standards. The Computer Emergency Response Team (CERT-In) is integral to addressing cybersecurity issues, while dedicated cyber cells are responsible for the investigation and prosecution of offenses related to social media. [9]

Any individual who contravened the aforementioned laws was earlier subject to the provisions

[9] Sommya Kashyap, Legal Framework of Social Media in India, Law Article (12 March 2025, 9:00 pm) [https://lawarticle.in/legal-framework-of-social-media-in-india/]

outlined in the **Indian Penal Code** [10] (IPC).

- **Section 295A** addresses the intentional defamation of religion or religious beliefs.
- **Section 153A** pertains to the promotion of animosity between groups based on race, religion, and similar factors.
- **Section 499** concerns defamation, stipulating that anyone who makes a defamatory statement, whether in writing or verbally, with the intent to harm another's reputation, will face legal repercussions. Sections 499 and 500 serve as the primary protections against misuse on social media platforms.
- **Section 505** relates to statements that provoke public unrest.
- **Section 509** addresses the disrespect of women's dignity.
- **Section 124A** pertains to sedition, which refers to actions that incite opposition with the potential to undermine the government.

Bharathiya Nyaya Sanhita 2023 [11]

- **Section 152** of the BNS introduces the concepts of "electronic communication" and "fiscal means" as instruments that may be employed to facilitate secession, organized rebellion, or racial discrimination, thereby rendering such actions punishable.
- **Section 299** of the BNS Act, which replaces Section 295A of the IPC, addresses malicious acts intended to provoke religious sentiments, imposing more stringent penalties for such offenses.
- **Section 356** of the BNS encompasses vilification, which was previously addressed in Section 499 of the IPC.

The Constitution of India [12] guarantees fundamental rights to its citizens, safeguarding their essential life interests and providing remedies in cases of violations. Article 19 addresses the Right to Freedom, and while it does not explicitly mention the freedom of the press or media, this right is encompassed within Article 19(a), which pertains to the freedom of speech and expression. Dr. Ambedkar stated, “Freedom of the press is vital for political liberty. When individuals are unable to communicate their thoughts freely, true freedom is unattainable; where freedom of expression is upheld, the foundation of a free society is established, and the means to preserve liberty are inherently present.”

[10] Supra 6
[11] Bharathiya Nyaya Sanhita, 2023
[12] The Constitution of India

 [ISSN 2581-5369]

V. PERTINENT CASE LAWS

Shreya Singhal v. Union of India [13]

In this instance, sections 66(a) and 69(a) of the Information Technology Act were contested on the grounds that they infringe upon Article 19(1)(a) and Article 14 of the Indian Constitution. The court remarked that there exists no intelligible differentia, meaning no discernible distinction. It noted that there is no significant difference between the internet and other mediums in the dissemination of information. In this pivotal ruling, the Supreme Court concluded that section 66(a) of the IT Act should be annulled, as it contravenes the freedom of speech and expression guaranteed by Article 19(1)(a) of the Constitution and is not justified under Article 19(2), which allows for reasonable restrictions. The court emphasized that section 66(a) is overly broad, ambiguous, and constitutionally vague due to the terminology employed in the statute. This provision encroaches upon the rights to free speech, dissent, and access to information. Additionally, the court noted that this statute bears no direct relation to public order and does not satisfy the "clear and present danger" test, a principle derived from U.S. law that assesses whether the language used poses a genuine threat that the government is entitled to mitigate. This assessment involves considerations of proximity and degree.

Tehseen S. Poonewala v. Union of India [14]

An issue arose regarding the government's responsibility to provide additional guidance for the removal of violent content from social media platforms. The court determined that the public should not assume the role of enforcers of justice and emphasized the importance of every citizen adhering to the rule of law. Furthermore, the court issued directives to halt the spread of information and to prevent the circulation of harmful and reckless messages on social media.

Karmanya Singh v. Union of India (WhatsApp-Facebook Privacy Case)[15]

In the current case, WhatsApp asserts that Facebook is its parent company, thereby justifying the transfer of user data to Facebook. The types of data involved include names, phone numbers, credentials, location, and status, among others. This sensitive information could be utilized for various purposes, many of which users may remain unaware of, with the most concerning being the potential for unwarranted surveillance. It has been observed that this update from WhatsApp will impact a broad spectrum of users, most of whom may not recognize the potential risks they

[13] *Shreya Singhal v. Union of India* AIR 2015 SC 1523
[14] *Tehseen S. Poonewala v. Union of India* (2018) 9 SCC 501
[15] *Karmanya Singh v. Union of India* MANU/DE/2607/2016

face.

This matter is currently before the Supreme Court of India, where the issue of privacy as a fundamental right has been escalated to a larger constitutional bench. This bench determined that privacy consists of three distinct categories: intimate, public, and private zones. The intimate zone pertains to physical and sexual privacy, while the private zone includes sensitive information such as ATM and PAN numbers. The Supreme Court has indicated that these two zones are not directly relevant to the current case. Instead, the public privacy zone must be evaluated on an individual basis. The present case falls within this category and remains under consideration by the Supreme Court.

VI. CONCLUSION

In India, the media is considered the fourth pillar of democracy, complementing the legislative, executive, and judicial branches of government, which operate within a similar regulatory framework. While certain controls on the press are essential, there are currently no explicit regulations governing media practices in India. The constitution does not contain a specific article dedicated to media; rather, it encompasses media under Article 19(1)(a), which guarantees the freedom of speech and expression. In an era characterized by rapid technological advancement and instantaneous information dissemination, the media is tasked with a vital role. A single erroneous or misleading report can have detrimental effects on society, potentially inciting riots or fostering animosity among different groups. In a nation where diverse cultures and religions coexist, it is imperative for the media to uphold the truth while refraining from disseminating falsehoods or sensationalizing stories for the sake of popularity. The swift advancement of social media technologies continues to pose significant challenges for legal regulation. Matters such as deepfakes, cryptocurrency marketing, and content moderation powered by artificial intelligence demand a continual adjustment of the legal framework. Furthermore, the merging of social media with various digital services, such as over-the-top (OTT) platforms and digital payment systems, calls for cohesive regulatory strategies. It is crucial to implement reasonable restrictions that prevent media personnel from inciting hatred or communal discord, while simultaneously protecting their freedom of speech and expression.

*****

 [ISSN 2581-5369]