



# The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2024

Editor-in-Chief – Prof. (Dr.) Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

---

"Social Media is a catalyst for the advancement of everyone's rights. It's where we're reminded that we're all human and all equal. It's where people can find and fight for a cause, global or local, popular or specialized, even when there are hundreds of miles between them. " Rania Al-Yassin<sup>1</sup>

Social media was primarily designed to be a platform for storing memories, learning and discovering new information, advertising and self-promotion, and connecting with others. This has aided many people in establishing businesses, connecting with family and friends, and becoming acquainted with new ideas from around the world, among other things. However, because of limited physical space and the growing popularity of social media, the issue of data uploaded on social media has arisen. The social media regulatory component comes in to define the users' Right to Free Expression, ensuring that the right does not infringe on the privacy of others, violate their rights, or enable the commission of Cyber Crimes through the use of platforms.

Section 2(w) of the Intermediary Guidelines and Digital Media Ethics Code Rules-2021 defines social media as an intermediary that primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify, or access information through its services.<sup>2</sup> Social media is a virtual platform that allows businesses and government agencies to interact and communicate with the general public. This is a concise description of Social Media, which is constantly evolving due to technological innovation and the term's inclusive nature. If we were to identify the most

---

<sup>1</sup> Rania Al-Abdullah is the Queen of Jordan as the wife of King Abdullah II. Rania was born in Kuwait to Palestinian parents. She received her bachelor's degree in business at The American University in Cairo. Rania championed an array of causes, including the rights of women and children, access to education, environmental concerns, and the development of strong Jordanian communities.

<sup>2</sup> Intermediary Guidelines and Digital Media Ethics Code Rules-2021, 2(w).

'social media intermediary' means an intermediary which primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services;

common characteristics shared by modern social media services, we would notice the following: user-generated, content-based profiles; and use-specific profiles created for apps or websites.

The Information Technology Act of 2000 was enacted in response to a resolution passed by the United Nations General Assembly in 1997.<sup>3</sup> The Act is the first and only Act that addresses the legal aspect of electronic advances, and it recognises e-Signatures, e-Records, and e-Evidence in legal proceedings under the Act. The IT Act also addresses the regulatory aspects of these Internet services as well as cybercrime. Chapter XI deals with cyber crimes; it is not an exhaustive list of offences because there is a daily increase in a new variety of cyber crimes and new methods to commit them. Because any crime committed on the Internet differs significantly from traditional crimes, specific Cyber Crime Cells and units have been established.<sup>4</sup>

Social media, being the most famous medium for disseminating information worldwide, has also become the hub for cyber crimes. Under section 2(w), "intermediary", with respect to any particular electronic record, means any person who, on behalf of another person, receives, stores, or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, web-hosting service providers, search engines, online payment sites, online auction sites, online marketplaces, and cyber cafes.<sup>5</sup> In the capacity of this definition, the government includes social networking websites such as Facebook, Twitter, LinkedIn, Instagram, etc. Under the scope of this Act, the government has tried to camouflage any other similar wrongs occurring through these websites.

Despite the fact that the Act covers major cyber crimes committed via social media, the law has become out of date due to the rapid development of social media in recent years. Some of the gaps include: This section of the Information Technology Act was enacted to penalise internet communication that is excessively insulting and menacing and causes annoyance, inconvenience, injury, intimidation, or hostility

---

<sup>3</sup><https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdclswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbfgGhdfgFHtyhRtMjk4NzY=> (last visited Jun 26, 2022).

<sup>4</sup> Information technology act, 2000, CHAPTER XI .

<sup>5</sup> Information Technology Act 2000, 2(w) .

[(w) —intermediary], with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes;]

and hatred. Sending an electronic mail message with the intent to annoy, inconvenience, defraud, or mislead the addressee became a crime under Section 66 A.<sup>6</sup>

The Supreme Court's decision to strike down Section 66 A of the Information Technology Act is a significant step toward preserving online free speech.<sup>7</sup> Six years after the decision, the Act is still used to punish citizens. The Supreme Court expressed dismay that more than 745 cases brought under Section 66A of the Information Technology (IT) Act are still pending in 11 states, despite the fact that it was ruled illegal six years ago and all pending cases filed under it were ordered to be dismissed.

Cyber lynching is a form of mob lynching that takes place online. Trolling on social media platforms by members of the virtual society stems from the same mindset. It is a growing trend in which ordinary people get involved in organised virtual crime against someone who is either a literal minority or has a marginalised mass-base. Both Facebook and Twitter are two-way interactive media platforms where users can comment, like, dislike, share, respond, and even slam one another. This mode of self-expression has resulted in a distinct user behaviour pattern. Based on the level of hostility, language, intimidation, and degree of harm inflicted on the other person, this procedure can be classified into three to four categories, including cyberbullying, trolling, lashing, and, ultimately, social media trial.<sup>8</sup> As a result of the onslaught of such crimes, these individuals frequently abandon social media, deactivate their accounts, become inactive, suffer from depression, and, in some cases, commit suicide. Before being murdered, some people were targeted and intimidated on social media.<sup>9</sup>

---

<sup>6</sup>Information Technology Act 2000, 66A .

*[66A. Punishment for sending offensive messages through communication service, etc.—Any person who sends, by means of a computer resource or a communication device,—*

*(a) any information that is grossly offensive or has menacing character; or*

*(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device;*

*(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages,*

*shall be punishable with imprisonment for a term which may extend to three years and with fine.]*

<sup>7</sup> Shreya Singhal v. Union of India, AIR 2015 SC 1523; Writ Petition (Criminal) No. 167 OF 2012

<sup>8</sup> Swati Arjun & Shikha Rai, *Crime by the Commons, Emerging Trend in Social Media*, 4 Journal of Content, Community and Communication 35-41 (2018).

<sup>9</sup> The killing of Gauri Lankesh, Columbia Journalism Review, [https://www.cjr.org/special\\_report/gauri-lankesh-](https://www.cjr.org/special_report/gauri-lankesh-killing.php#:~:text=By%20Siddhartha%20Deb&text=Last%20September%2C%20as%20the,before%20sh)

[killing.php#:~:text=By%20Siddhartha%20Deb&text=Last%20September%2C%20as%20the,before%20sh](https://www.cjr.org/special_report/gauri-lankesh-killing.php#:~:text=By%20Siddhartha%20Deb&text=Last%20September%2C%20as%20the,before%20sh)  
[e%20made%20it%20inside.](https://www.cjr.org/special_report/gauri-lankesh-killing.php#:~:text=By%20Siddhartha%20Deb&text=Last%20September%2C%20as%20the,before%20sh) (last visited Jun 26, 2022).

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 were drafted in the exercise of powers under Section 87 (2) of the Information Technology Act, 2000, and supersede the earlier Information Technology (Intermediary Guidelines) Rules 2011. The Code 2021 requires social media platforms to establish a redressal mechanism for users to voice their grievances and to provide users with the right to be heard. The Code also divides intermediaries, including social media, into two categories: significant intermediaries, which are mostly messaging apps, and intermediaries.<sup>10</sup>

In the case of substantial intermediaries, the government may order the intermediary to provide the first generator of any information only in the case of sovereign threats or serious offences. Intermediaries should also not publish or cease publishing information that is prohibited by a court order or an order issued by the appropriate government agency or its Redressal Officer.<sup>11</sup> Social media platforms are also liable if they do not remove false content after becoming aware of it. The Code also requires social media platforms to have a permanent Legal Compliance Officer who is an Indian citizen as well as a Nodal Contact Person.

The Rules require intermediaries to provide information under their control or possession upon request from a government agency. Any government agency authorised by law to conduct investigative, protective, or cybersecurity activities may make such a request. The request may be made to verify an individual's identity, to prevent, detect, investigate, or prosecute violations of any law, or to respond to cybersecurity incidents. The Rules, on the other hand, make no provision for procedural safeguards or procedures in connection with such activities.

Another gap is identifying the first originator of information on a messaging platform, which will necessitate the service provider permanently storing certain additional information: (i) who all exchanged a message, and (ii) the exact message or certain details that uniquely describe a message so that

---

[Such as Gauri Lankesh, a Bengaluru-based Vernacular journalist who was first threatened on Facebook and subsequently murdered for her anti-establishment beliefs, and who was subjected to social media lynching even after her death. Where she was abused by being called (Qaumi & Bitch) and subjected to slut shaming.]

<sup>10</sup> The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, PRS Legislative Research, <https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021> (last visited Jun 26, 2022).

<sup>11</sup> Supra note 10

information in question can be matched against it. This will be required for every message exchanged across the service provider's platform in order to track the first originator of any communication. It should be noted that permanently retaining such details about a message is not a technological requirement for providing messaging services via the internet. The Rules also do not establish a timetable for how far back in time the messaging provider must search to determine the first originator. Overall, this rule will result in messaging services retaining more personal data, which contradicts the concept of data minimization.<sup>12</sup>

In times of crisis, free expression is critical for emerging economies. In democratic countries, the availability of an open media allows the government to face opposition, public pressure, and criticism, and to prevent crises from escalating. Undemocratic conditions and press restrictions lead to a lack of public discourse and, eventually, a lack of necessary policy decisions. Attempts to control digital media or social media spaces make the population vulnerable and may result in the denial of critical socio economic rights. When human rights are violated, disinformation thrives. Journalists and civil society may be the best equipped to confront falsehoods and present opposing viewpoints in order to reduce this "information disorder."

When discussing territorial regulation of social media, we must recognise that it should be regulated only when the country understands what to regulate and the consequences of regulation, as well as the fact that regulation does not imply control of social media, i.e., regulation is not synonymous with control. There is no freedom under control; however, there is freedom under regulation; however, it is subject to reasonable constraints in the public interest."

Can social media, on the other hand, be limited to a geographical zone where anyone from anywhere in the world can commit a crime against someone on the other side of the world? This question is primarily concerned with country-specific private international law, but can such a significant conflict be left to the variety of country-specific private international law? These investigations point to the creation of a Globally Coordinated Regulatory Body.<sup>13</sup> From this vantage point, all parties are increasingly aware of

---

<sup>12</sup> White Paper of the Committee of Experts on Data Protection Framework for India, MyGov.in, <https://www.mygov.in/task/white-paper-committee-experts-data-protection-framework-india/> (last visited Jun 26, 2022).

<sup>13</sup> DORNALA SAI MAHITHA, *Social Media and Its Regulations in India*, 4 INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES.

the need for a mechanism capable of ensuring effective public oversight of content moderation on social media platforms.