International Journal of Engineering Research and Development
e- ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 21, Issue 11 (November 2025), PP 94-102

Legal Frameworks Governing Social Media in India

V.Angelin Subiksha
LLM student at SRM School of Law, Chennai

ABSTRACT
Social media's explosive growth has changed public debate, communication, and connectivity, but it has also brought unprecedented legal issues. The study examines the development of India's legal framework governing social media, examining statutory provisions such as the Information Technology Act, 2000, the IT Rules, 2021, the Digital Personal Data Protection Act, 2023, and the Bharatiya Nyaya Sanhita, 2023, along with significant judicial pronouncement.
In India, social media regulation entails striking a balance between constitutional freedoms and the need to prevent cyber crime, disinformation, and privacy violations. The research analyses how India is dealing with issues of privacy, defamation, content regulation, and intermediary liability in a fast-changing digital world. The study concludes that although there has been notable progress, gaps in enforcement and constitutional issues still exist. This situation calls for a balanced approach that respects rights in digital governance.
KEY WORDS
Cyber crime, Social media intermediaries, Intermediary liability, Information Technology Act,2000, Information Technology (Intermediary Guidelines and Digital Media Ethics) Code, Privacy, Freedom of speech.

Date of Submission: 02-11-2025 Date of acceptance: 11-11-2025

I. INTRODUCTION

The emergence of social media has completely changed how people interact, communicate, and share information in today's world. We can now quickly share our information with others using electronic means. It has the power to unite people worldwide. Facebook, Instagram, Twitter (X), WhatsApp, and other platforms have become essential to both personal and professional life because they provide previously unheard-of access to information and encourage novel forms of public conversation. With its varied network, this platform almost reaches every home on the planet. For it to have a positive impact on society, each user should use it sensibly and constructively. The majority of social media users are young people. Social media can also have unintended consequences for users. They distanced themselves from loved ones due to their excessive reliance on social media.

Simultaneously, the swift growth of social media has brought about formidable legal obstacles, specifically concerning privacy, data security, disinformation, hate speech, cybercrime, and online content regulation. Users are given total freedom to voice their opinions, but everything has advantages and disadvantages. Numerous crimes, such as cyber-bullying, cyber-defamation, email phishing, and creating false profiles, are associated with social media. In order to guarantee responsible use of digital platforms while respecting constitutional freedoms, these issues have made the creation of comprehensive legal frameworks necessary.

Social media crimes are addressed by laws such as the Indian Penal Code 1860, now, Bharatiya Nyaya Sanhita, 2023 and the Information Technology Act 2000, which also protect women's modesty and other related offenses. A balance between individual liberties and the interests of society as a whole is sought by the provisions of these Acts, which attempt to balance the constitutional guarantee of freedom of speech and expression under Article 19(1)(a) with the reasonable restrictions allowed under Article 19(2). This field has been further enhanced by judicial interpretation, as courts have addressed matters ranging from intermediary liability to the acceptable bounds of online expression.

This study seeks to understand the legal framework that governs social media in India by examining statutory provisions, regulatory guidelines, and court rulings. It also aims to draw attention to the real-world difficulties in policing a changing digital environment while defending fundamental rights. The project's goal is to give readers a thorough grasp of India's changing social media regulations and their wider ramifications for civil liberties, governance, and democratic engagement in the digital age. The project aims to offer a thorough grasp of India's changing social media regulation strategy and its wider ramifications for civil liberties, governance, and democratic engagement in the digital era.

SOCIAL MEDIA LAW

Social media law is a growing area of the law that encompasses both criminal and civil aspects[1]. Two important areas—privacy and free speech—are the main lenses through which social media regulation is viewed. Because of the extraordinary potential of asymmetrical information dissemination, there is a good chance that powerful individuals are abusing digital media platforms to further their political and commercial agendas. Because technology is developing so quickly, the state is faced with the difficult task of balancing people's rights against society, one another, and occasionally even with itself.

In general, it addresses legal concerns about user-generated content and the websites that host or distribute it. Among the special legal issues brought up by social media are defamation, advertising law, intellectual property (IP) law, privacy, including the rights of social media users and third parties, and others. Social media content occasionally violates trademarks, copyrights, and other intellectual property rights. Social media use is covered by both criminal and civil laws at the federal and state levels. Regulations pertaining to social media can be used to protect or prohibit the publication of content in order to strengthen or restrict the privacy rights of stake holders. The legal concerns surrounding user-generated content and the websites that host it are covered by social media law.

BACKGROUND OF MAJOR STATUTES GOVERNING SOCIAL MEDIA RELATED OFFENCES

Commonly known as the IPC, the Indian Penal Code is a significant piece of legislation and arguably the most frequently applied in criminal law, acting as India's primary criminal code. Initially enacted in 1860 and revised multiple times since then, it encompasses nearly all substantive elements of criminal law and is complemented by other criminal provisions.

The Information Technology Act 2000[2] has modified the sections related to records and documents in the IPC by adding the term 'electronic,' thereby equating electronic records and documents with their physical counterparts. Following this, several amendments have been introduced to incorporate cyber offences into the IPC.

The Bharatiya Nyaya Sanhita, which took the place of the IPC, also addresses cyber crimes. Under the BNS, cyber crimes are defined as unlawful actions that involve computers, the internet, or digital devices. The BNS, effective from July 1, 2024, tackles cyber crime by incorporating it within larger categories such as organized crime and theft.

In the early days of the internet, the lack of specific regulations for social media resulted in a fairly unregulated online environment. Governments around the globe struggled to modify existing legal structures to accommodate the quickly evolving digital landscape. In India, recognizing the importance of a more refined approach, the initial movements towards establishing social media laws began to take shape. During this time, lawmakers built the groundwork for the Information Technology Act of 2000, which was the first legislation that paved the way for the extensive legal frameworks we encounter today. The primary objective was to grant legal acknowledgment to electronic documents and promote e-commerce, with wider ramifications for the digital space.

In October 2000, the Information Technology Act 2000 (IT Act) was enacted by the Indian Parliament. Due to the fact that it was the first substantive law addressing electronic commerce and cybercrimes, it marked a turning point in the development of digital media regulation in India. The law was enacted based on the United Nations' recommendations to adopt United Nations Model Law on Electronic Commerce,1996, popularly known as UNCITRAL Model[3]. The Act, primarily, lays down the legal framework for e-commerce and the prevention of cybercrimes in India. It primarily tackled cybercrimes, although the term "cybercrime" itself was not defined in the Act, and only covered some examples of computer-related crimes. It did not define sensitive issues like free speech, privacy, data protection, and other crucial aspects related to online discourse. The boundaries of due diligence for social media entities were not defined under the Act. The legislation was not well suited to deal with social media and internet related other issues. An expert committee was thus established by the government in January 2005 to examine the IT Act. Because of the advancements, particularly in the fields of data protection and privacy, the committee recommended a number of changes in its report, which found significant gaps in the current Act. Subsequently, Parliament introduced the Information Technology (Amendment) Bill 2006. Passed in December 2008, the Amendment Act went into force in October 2009. The IT Act, 2000 framework underwent significant changes with the Amendment Act, 2008, which added new express provisions to include more cyber offenses under the original Act's jurisdiction. A number of provisions pertaining to privacy and individual data

[1] **Winston & Strawn**, ***Social Media Law***, Winston & Strawn Legal Glossary, https://www.winston.com/en/legal-glossary/social-media-law

[2] The Information Technology Act, 2000 (No. 21 of 2000)

[3] ***Ravi Shankar & Tabrez Ahmad, Information Technology Laws: Mapping the Evolution and Impact of Social Media Regulation in India***, 41 DESIDOC J. Libr. & Info. Tech. 295 (2021), [*https://doi.org/10.14429/djlit.41.4.16966](https://doi.org/10.14429/djlit.41.4.16966)*.

protection were included in the new amendment, along with measures to prevent child pornography, voyeurism, and cyber-terrorism through the use of electronic and digital media. As social media in India grew quickly, the Act incorporated a few sections that will be covered later.

In an effort to expand the definition of "due diligence" for intermediaries, the government established detailed guidelines named Information Technology (Intermediaries Guidelines) Rules in April 2011. These regulations were created under the authority granted by Section 87(2) in conjunction with Section 79 of the IT Act.

In April 2018, the Indian government acknowledged through an order that there were "no norms or guidelines in place for online media websites and news portals," and it intended to regulate digital media to address issues such as fake news and other matters not directly addressed by the IT Act. Following this, the government submitted an affidavit to the Supreme Court in October 2019, recognizing the necessity to regulate content on social media. The affidavit indicated that the Indian government was concerned about social media and noted that "it has become a powerful tool capable of causing immense disruption to the democratic framework due to unregulated social media content." On February 25, 2021, India announced the "Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021", aiming to mainly oversee social media platforms and also apply to OTT services.

The Digital Personal Data Protection Act, 2023 (DPDP Act)[4] marks India's inaugural comprehensive regulation aimed specifically at protecting personal data in the digital realm. Established to tackle the rising issues of privacy, security, and accountability within the digital landscape, this Act offers a systematic approach to the lawful handling of personal data while acknowledging individuals' rights over their information. It is relevant to the processing of digital personal data occurring within India, as well as to any processing carried out outside India if it pertains to providing goods and services to individuals in the country.

COMMON SOCIAL MEDIA CRIMES

An increasing number of individuals, irrespective of their age or gender, are signing up for accounts on online social media platforms to interact with one another in this digital environment. Some users maintain hundreds or even thousands of friends and followers across various accounts. However, there is also a rise in the number of fraudulent profiles. These fake accounts frequently bombard genuine users with spam, sharing inappropriate or illegal material. Additionally, fake profiles can be created to impersonate well-known individuals, leading to harassment directed at them.

The most commonly targeted websites and applications for establishing 'Fake Profiles' include:

1. Facebook
2. Instagram
3. Twitter
4. LinkedIn

The following are the typical offenses occurring on or as a consequence of social media[5]:

a) Online Threats, Stalking, Cyber bullying

The crimes most frequently observed and reported on social media include making threats, bullying, harassing, and stalking others in the digital space. Although a significant portion of this behavior often goes unpunished or is not treated with the seriousness it deserves, victims of such crimes often find themselves unsure about when to involve law enforcement.

b) Hacking and Fraud

While it might seem like a harmless joke to log into a friend's social media account and share an embarrassing status message amongst friends, it can actually be considered a serious offense. Furthermore, establishing fake or impersonation accounts to deceive others (rather than simply being anonymous) can be classified as fraud, particularly based on the actions performed by the individual operating the fake or impersonation account.

c) Buying Illegal Things

Engaging through social media for business networking or purchasing lawful goods or services can be entirely acceptable. Conversely, using social media to acquire drugs or other regulated, controlled, or prohibited items is likely against the law.

d) Vacation Robberies

Unfortunately, a prevalent tactic among thieves is to utilize social media to determine when someone is away on vacation. If your travel updates are visible to the public instead of being limited to friends, burglars can easily find out when you will be gone for a long time.

e) Creation of fake profile

[4] The Digital Personal Data Protection Act, 2023, (NO. 22 OF 2023)

[5] **Delhi Police**, ***Social Media Crimes***, Cyber Crime Unit, *(https://cyber.delhipolice.gov.in/socialmediacrimes.html*)

Fabrication of a false identity for an individual and sharing insulting material, including altered images, on that false identity is a crime.

f) Fake online friendship

Cultivating virtual friendships through social media (without any actual in-person acquaintance and leveraging emotional ties to manipulate people into sending money under various pretenses like medical emergencies, legal issues, difficulties abroad, etc.).

g) Cerebral property crimes

It involves the theft of copyrighted materials, the misappropriation of trade secrets, and violations of trademarks, among other offenses. Copyright refers to the legal entitlement of an author, publisher, composer, or any other creator of a work.

h) Cyber Crouching[6]

It refers to the practice of obtaining, trading, or utilizing an Internet domain name with the intention of profiting from a trademark owned by another party. The individuals engaging in this activity then propose to sell the domain to the rightful trademark owner at an exorbitant price.

i) Cyber terrorism

It is a highly perilous type of cybercrime, involves executing violent acts via the internet, including slow or extensive disruptive operations. Cyber terrorism can be defined as the intentional engagement in disruptive actions. Currently, this phenomenon has evolved, with terrorist organizations delving into cyber psychological warfare and employing brain computing techniques to sway human behavior for their objectives.

MAJOR ISSUES IN THE REALM OF CYBERSPACE

I.PRIVACY RELATED CONCERNS

In the digital era, privacy has emerged as a significant concern. Social media companies regularly gather extensive amounts of personal information, including user profiles, online behaviour, location data, and private messages. This information is frequently utilized for targeted advertising, leading to worries about surveillance capitalism[7]. The issue is compounded by regular data breaches and unauthorized sharing of information. For example, repeated leaks of databases from Facebook and WhatsApp have revealed sensitive personal information.

In India, the right to privacy was established as a fundamental right under Article 21 in the case of *Justice K.S. Puttaswamy v. Union of India*, which highlighted the importance of informational privacy as part of the right to life and personal liberty. Nonetheless, real-world protection of privacy remains inadequate. The DPDP Act of 2023 addresses some of these issues by mandating informed consent, granting individuals the right to access and delete their data, and instituting penalties for companies that misuse or breach data. However, challenges persist in terms of enforcement, particularly regarding large international tech companies, as well as ensuring that data localization or government surveillance does not encroach upon individual freedoms.

II.DEFAMATION IN CYBERSPACE

The distinction between private and public expression has become less clear due to social media, leading to frequent cases of defamation online. A single defamatory tweet, post, or video can quickly disseminate, inflicting lasting damage on a person's reputation[8]. According to Indian law, defamation constitutes both a civil and criminal offense. The Indian Penal Code, 1860 (Sections 499–500) addresses defamation as a criminal act, while civil recourse is available through tort law. The recent Bharatiya Nyaya Sanhita, 2023 Section 356 continues to include provisions related to defamation.

The challenge in the digital realm lies in reconciling defamation laws with the constitutional right to free speech protected by Article 19(1)(a). Courts have consistently pointed out that the right to free speech is not unlimited and can be constrained under Article 19(2) to safeguard individual reputation. Intermediaries are tasked with the complex responsibility of handling requests to remove content deemed defamatory. In the Supreme Court case *Shreya Singhal v. Union of India*, it was clarified that platforms are required to take action against content only when instructed by a court or government authority, thus preventing arbitrary censorship. However, the rapid pace in which online materials are shared render traditional defamation remedies slow and often ineffective.

III.CONTENT CONTROL IN CYBERSPACE

[6] **Swati Sharma & Vikash Kumar Sharma**, ***Cyber Crime Analysis on Social Media***, 11 BSSS J. Comput. 1 (2020), [*https://doi.org/10.51767/jc1104](https://doi.org/10.51767/jc1104*).

[7] **Electronic Privacy Information Center (EPIC**), ***Social Media Privacy***, (https://epic.org/issues/consumer-privacy/social-media-privacy/)

[8] **IIPRD**, ***Defamation in the Digital Age: Navigating Social Media, Blogs, and Legal Consequences***, (https://www.iiprd.com/defamation-in-the-digital-age-navigating-social-media-blogs-and-legal-consequences/)

The most complicated problem in the online world is probably content regulation. The billions of user-generated posts on social media platforms serve as middlemen and contain damaging content such as fake news, hate speech, child sex abuse, and terrorist propaganda. Strict regulations have been implemented by governments worldwide, including India, to guarantee accountability[9]. The IT Act's Section 69A gives the government the authority to censor internet content for reasons of public order, security, or sovereignty. This provision has been frequently used to block apps and social media accounts.

Additionally, platforms must designate compliance officers, enable message traceability, and remove illegal content within 36 hours of notice, according to the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Concerns about over-censorship, privacy invasion, and other issues have been raised by these regulations, which on the one hand seek to prevent harmful content and false information.

KEY PROVISIONS IN THE STATUTES OF INDIA

A. INFORMATION TECHNOLOGY ACT, 2000

Section 66C	Anyone who fraudulently or dishonestly utilizes the electronic signature, password, or any other unique identification characteristic belonging to another individual shall face imprisonment of either kind for a duration that may extend up to three years and shall also be subject to a fine that may reach up to one lakh rupees.
Section 66D	Any individual who uses a communication device or computer resource to commit fraud through impersonation will face imprisonment of any kind for a period that may last up to three years, along with a fine that could reach one lakh rupees.
Section 66E	Anyone who intentionally or knowingly captures, distributes, or shares an image of another person's private area without their consent, in a manner that infringes on that person's privacy, shall face imprisonment for up to three years, or a fine that may reach two lakh rupees, or both.
Section 67	Anyone who publishes, transmits, or facilitates the publication or transmission of any material in electronic form that is sexually suggestive or appeals to unhealthy sexual interests, or that is likely to deprave and corrupt individuals who are expected to read, view, or listen to the content, will face punishment. Upon a first conviction, the penalty may include imprisonment for up to three years and a fine of up to five lakh rupees. In the case of a second or subsequent conviction, the punishment may be extended to imprisonment for up to five years, along with a fine of up to ten lakh rupees.
Section 67A	Anyone who publishes, distributes, or facilitates the publication or distribution of any material in electronic form that depicts sexually explicit acts or behavior shall face a punishment of imprisonment for up to five years and a fine that may reach ten lakh rupees upon the first conviction. In the case of a second or subsequent conviction, the punishment will increase to imprisonment for a term of up to seven years as well as a fine that may also be up to ten lakh rupees.
Section 67B	Child porn
Section 69A	Power of government to block public access to a content
Section 72	If any individual, acting in accordance with the powers granted by this Act, rules, or regulations established under it, gains access to any electronic record, book, registry, correspondence, information, document, or other material without obtaining the consent of the relevant individual, and subsequently discloses such electronic record, book, registry, correspondence, information, document, or

[9] **Bhatt & Joshi Associates**, ***Regulation of Social Media and Online Content: Legal Frameworks, Case Laws, and Judgments***,(https://bhattandjoshiassociates.com/regulation-of-social-media-and-online-content-legal-frameworks-case-laws-and-judgments/)

	other material to another person, they shall be subject to a penalty that may reach up to five lakh rupees.

One of the most important provisions of The Information Technology Act of, 2000 is the safe harbor provision within Section 79, which protects intermediaries like social media platforms, search engines, and messaging applications from liability for user-generated content. Essentially, intermediaries are considered neutral conduits; they are not accountable for third-party information that is shared or transmitted via their platforms, as long as they do not originate, choose, or alter the transmission. This protection is vital because it prevents platforms from facing lawsuits for every unlawful or offensive post made by their vast user base, thereby facilitating the operation of large-scale social media services.

However, the protection is not absolute. To qualify for safe harbor, intermediaries must adhere to the due diligence requirements set forth by the IT Act and the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. This involves notifying users against posting illegal content, creating a mechanism for grievance redressal, and following takedown orders issued by courts or government bodies. If an intermediary neglects these responsibilities, it risks forfeiting the protections of Section 79 and could be held directly accountable for any unlawful content present on its platform.

The *Avnish Bajaj v. State (200)5* case, commonly referred to as the Bazee.com case, represents a significant milestone in Indian cyber law related to intermediary liability. This case emerged following the listing for sale of a pornographic MMS clip involving two minors (the DPS MMS scandal) on Bazee.com, an online auction site managed by Avnish Bajaj. Despite the listing being taken down quickly upon discovery, the Delhi Police apprehended Bajaj and accused him under Section 67 of the IT Act, 2000 for electronically distributing obscene content, along with applicable sections of the IPC concerning obscenity. The primary question before the Delhi High Court was whether the Managing Director of an intermediary platform could be held personally liable for content posted by users who are not connected to the platform.

The Court determined that Avnish Bajaj could not be held criminally liable under Section 67 of the IT Act in his individual capacity, as the legislation did not include provisions for vicarious liability of directors. While the company could have faced prosecution had it knowingly allowed the transmission of obscene content, its director could not be held accountable without a specific statutory provision stating so. Nonetheless, the Court permitted proceedings to continue under IPC clauses, such as Section 292 (regarding the sale of obscene content), since individual criminal liability under the IPC can apply to those directly involved in or negligent towards the offense.

This ruling was crucial as it highlighted the deficiencies in the IT Act concerning intermediary liability. It illustrated the necessity for online platforms to have a well-defined legal framework outlining their responsibilities related to user-generated content. The case ultimately played a role in influencing the 2008 amendment to the IT Act, which introduced a more robust safe harbour provision in Section 79 and mandated due diligence responsibilities for intermediaries. Consequently, the Avnish Bajaj case became a critical point in defining India's regulatory approach towards social media and online platforms, striking a balance between ensuring accountability and shielding intermediaries from liability for every action taken by their users.

The case of *Shreya Singhal v. Union of India*[10] (2015) represents a significant ruling by the Supreme Court of India concerning free speech and online expression. This case emerged when the constitutionality of Section 66A of the IT Act, 2000 was contested. Section 66A made it a criminal offense to send any information via a computer or communication device that was deemed "grossly offensive," "annoying," or of a "menacing character." This provision was criticized for its vagueness and potential for misuse, resulting in the arrest of individuals for posting innocuous or critical remarks on social media platforms like Facebook and Twitter. The petitioner, Shreya Singhal, contended that the section infringed upon the fundamental right to freedom of speech and expression guaranteed by Article 19(1)(a) of the Constitution.

The Supreme Court declared Section 66A of the IT Act entirely unconstitutional, citing vagueness and overreach as its basis. The Court noted that terms like "grossly offensive" or "annoying" were subjective, allowing for arbitrary enforcement by the authorities. This led to a chilling effect on free speech, as individuals might avoid expressing their views online due to the fear of legal action. The Court stressed that any limitations on speech must adhere to the criteria explicitly stated in Article 19(2) of the Constitution, such as sovereignty, national security, public order, decency, or defamation, and Section 66A failed to satisfy these conditions.

Additionally, the judgment addressed Section 79 of the IT Act, which grants safe harbour protections to intermediaries. The Court clarified that these intermediaries are only obligated to eliminate content when instructed by a court order or government authority, rather than simply upon receiving private complaints. This interpretation ensured that platforms were not compelled to engage in arbitrary censorship and that the content removal process was subject to judicial or governmental review.

[10] Shreya Singhal vs U.O.I, AIR 2015 SUPREME COURT 1523

The Shreya Singhal case is seen as a pivotal moment in Indian internet law, as it not only protected the right to free speech in the digital realm but also delineated the boundaries of intermediary liability. By nullifying Section 66A and refining aspects of Section 79, the Court affirmed that the governance of online content must align with constitutional protections, establishing a robust precedent for safeguarding digital expression in India.

B. IT (INTERMEDIARY GUIDELINES AND DIGITAL MEDIA ETHICS CODE) RULES, 2021

The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 create a structure for managing content on social media platforms and digital intermediaries. The main concept is that intermediaries should not simply act as inactive hosts of content but have to exercise due diligence and take appropriate measures to stop the spread of illegal and harmful content.

Rule 3 mandates that all intermediaries notify users that they should not host or share content that is defamatory, obscene, pornographic, infringes on privacy, hateful, or otherwise illegal. Intermediaries are also required to implement a grievance redressal system, designate a Grievance Officer, and guarantee that complaints are acknowledged within 24 hours and resolved within 15 days. This provision is intended to provide users with a direct means to report harmful or unlawful content posted online.

For Significant Social Media Intermediaries (SSMIs), identified as platforms having over 5 million registered users in India, Rule 4 imposes more rigorous obligations. These platforms must designate key personnel located in India: a Chief Compliance Officer who oversees legal adherence, a Nodal Contact Person to liaise with law enforcement, and a Resident Grievance Officer to handle user complaints. Moreover, SSMIs are mandated to facilitate the traceability of the original sender of a message when instructed by a court or the government, a contentious requirement that messaging services such as WhatsApp have vocally opposed due to concerns over privacy and end-to-end encryption.

The regulations also mandate that these platforms utilize automated systems to actively monitor harmful content, particularly material related to child sexual abuse, rape, and deepfakes. Platforms are obligated to respond to takedown requests from the government or courts within 36 hours and eliminate content that breaches legal requirements or individual rights. Additionally, in situations concerning sexual content or impersonation, platforms are required to respond within 24 hours of receiving a complaint to mitigate further harm.

Significantly, Rule 7 states that if intermediaries do not adhere to these requirements, they will forfeit the "safe harbor" protection granted by Section 79 of the IT Act. Consequently, they may be held directly responsible for illegal content posted by users, which they are usually protected against.

The case *Kunal Kamra v. Union of India* presents a constitutional challenge initiated by comedian Kunal Kamra, accompanied by various media organizations, editors, and journalists, within the Bombay High Court. The petitioners contested the amendments made in 2023 to the Information Technology (Intermediary Guidelines & Digital Media Ethics Code) Rules, 2021, which established a Fact-Checking Unit (FCU)[11] by the central government. According to the amendment, social media intermediaries are required to flag or remove content about the "business of the Central Government" identified as "fake, false, or misleading" by this FCU; noncompliance could lead to the loss of their safe harbour protections under Section 79 of the IT Act.

On January 31, 2024, a split verdict was issued by a two-judge bench (Justices G.S. Patel and Neela Gokhale), where Justice Patel declared that the amended rules, particularly Rule 3(1)(b)(v) (as amended), were unconstitutional on multiple grounds: they infringed upon Articles 14 (equality), 19(1)(a) (freedom of speech & expression), and 19(1)(g) (right to practice a profession), due to their over-broad and vague nature, thus creating a chilling effect. He concluded that the powers of the FCU were poorly defined, granting government authorities excessive discretion without procedural safeguards, essentially allowing them to act as judge, jury, and executioner regarding what qualifies as "fake or misleading" content. Conversely, Justice Gokhale supported the amendments, asserting they provide a proportional limitation on speech to address misinformation, claiming there are adequate safeguards in place.

Due to the divided opinion, a third judge, Justice A. S. Chandurkar, was designated to resolve the impasse. In his ruling, delivered on September 26, 2024, Justice Chandurkar sided with Justice Patel, agreeing that the amendments, particularly the rule granting authority to the FCU in its current form, were unconstitutional. He stated that Rule 3(1)(b)(v) of the Rules, as amended, overstepped the limits set by the IT Act, 2000, and breached Articles 14, 19(1)(a), and 19(1)(g). Major criticisms pointed out included the ambiguity surrounding phrases like "business of Central Government," "fake/false/misleading," and the absence of due process or natural justice in the moderation or removal of content based on the FCU's assessments.

This ruling is notable as it reaffirms the constitutional boundaries regarding government oversight of online expression: any regulation that endangers freedom of expression must be adequately defined, must not exhibit arbitrary or vague characteristics, must adhere to safe harbour requirements, and must guarantee

[11] **Government of India Press Information Bureau**, ***PIB Fact Check Unit***, (https://www.pib.gov.in/aboutfactchecke.aspx)

procedural fairness. The decision challenges overly expansive content moderation policies that could compel intermediaries to engage in pre-emptive censorship. This remains a significant aspect of ongoing legal discussions, particularly as the Supreme Court has been approached for appeals and interim orders concerning the enforcement of the FCU in relation to these regulations.

C. DIGITAL PERSONAL DATA PROTECTION ACT, 2023

In India, the first all-encompassing framework for controlling the gathering and use of personal data is established by the Digital Personal Data Protection Act, 2023. Social media companies are among the biggest processors of personal data in the nation, so its provisions are directly applicable to them.

Social media companies are only permitted to process personal data for legitimate purposes and in compliance with the Act under Section 4. The processing needs to be supported by legitimate user consent.

According to Section 5, this consent must be given in a clear affirmative action and be free, specific, informed, and unconditional. This stops platforms from depending on ambiguous consent clauses that are frequently hidden in terms and conditions. Furthermore, platforms must offer an easy-to-use method for users to revoke their consent at any time in accordance with Section 6. In actuality, this implies that a user may choose not to see tailored ads or withdraw consent for a platform to monitor their online activities.

While consent is fundamental, Section 7 allows for specific "legitimate uses" where data can be processed without obtaining consent, including fulfilling a legal duty or addressing medical emergencies. Nevertheless, these exceptions are restrictive and cannot be misused by platforms for commercial profiling or advertising purposes.

The privacy of children is specifically safeguarded by Section 9. Social media platforms are restricted from monitoring, profiling, or directing advertisements toward users under 18 years old. Additionally, they must secure verified parental consent prior to handling children's personal information. This is especially important for platforms such as Instagram, YouTube, and gaming applications, which often have underage users, and it reflects worldwide worries about the exploitation of minors on the internet.

The Act also grants authority to individuals known as Data Principals by providing them with rights as outlined in Section 11. These rights encompass the ability to access details on the usage of their data, the power to amend any inaccuracies, and the option to request the deletion of their data. For users of social media platforms, this means enhanced control over their online presence, which includes the capacity to ask for the removal of old posts or even the total deletion of their accounts.

A strong focus is placed on accountability regarding data breaches. Section 16 mandates that platforms must notify both the Data Protection Board of India and the individuals affected in the event of any personal data breach. This guarantees that users are quickly informed if their personal information is compromised through hacking, leaks, or carelessness.

Lastly, the Act establishes a rigorous penalty structure to encourage adherence. According to Section 33, social media companies could incur fines of up to 250 crore for infractions such as neglecting to protect user data or processing it without obtaining consent. Section 34 also outlines increased penalties for improperly handling children's data, acknowledging the greater risks that minors face online.

D. BHARATIYA NYAYA SANHITA, 2023

Section 356	Creating or distributing false information that damages someone's reputation remains punishable under the BNS. On social media, this encompasses defamatory tweets, posts, videos, or memes that negatively affect a person's public image. Both the originator and the distributor of defamatory material may be held responsible.
Section 294	Distributing or sharing obscene material is considered a crime. If vulgar videos, images, or inappropriate posts are posted or circulated on platforms such as Instagram, Facebook, or WhatsApp, the individual accountable could face legal consequences under this provision.
Section 77	Specifically addresses "voyeurism," which is the taking or publishing of images of a woman's private areas or behaviors without her consent.
Section 78	Addresses the offence of stalking in both physical and cyber forms. Imposes imprisonment and fines for monitoring or bothering a woman through physical or electronic means.
Section 353	Makes it illegal to make statements that instill fear, cause alarm, or provoke actions against the State. Online posts that create panic, pose a threat to national security, or disrupt public order are included under this regulation.

Section 319	Addresses impersonation including electronic methods. Creating false social media profiles, engaging in phishing scams, or committing fraud by masquerading as another individual on platforms is subject to penalties under this section.

II. CONCLUSION

The regulation of social media in India illustrates the intricate balance between technological advances, fundamental rights, and the government's duty to uphold law and order. Social media platforms have become essential for communication, commerce, and participation in democracy, yet they also provide a breeding ground for various crimes, including cyberstalking, defamation, data theft, and the spread of inappropriate or harmful content. The Information Technology Act of 2000, the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules of 2021, the Digital Personal Data Protection Act of 2023, and the newly enacted Bharatiya Nyaya Sanhita of 2023 collectively establish a comprehensive framework designed to tackle these issues. These laws impose responsibilities on intermediaries, protect user privacy, and penalize the misuse of digital platforms while seeking to balance freedom of expression with reasonable limitations under Article 19(2) of the Constitution.

Judicial rulings, such as those in Avnish Bajaj v. State, Shreya Singhal v. Union of India, and Kunal Kamra v. Union of India, have been crucial in defining the limits of intermediary liability, invalidating ambiguous and unconstitutional provisions, and reinforcing the priority of constitutional rights in the online environment. However, gaps in enforcement, challenges related to jurisdiction, and the swift evolution of technology continue to challenge the effectiveness of the current laws.

Moving forward, India must work towards achieving a balance where laws enforce accountability without hindering innovation or restricting legitimate expression. An approach that emphasizes transparency and rights, along with strong institutional frameworks, is vital to ensure that social media serves as a means of empowerment rather than exploitation. Ultimately, the progression of social media legislation in India is not only legally essential but also a democratic necessity, protecting individual freedoms while fostering responsible engagement with digital platforms in an interconnected environment.