LexScriptaMagazine.com ISSN: 2583-8725 Vol. 04 - Q1 Jan - Mar, 2026

ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

"Join the League of National & International Scholars"

EDITORIAL TEAM

LEX SCRIPTA MAGAZINE OF LAW AND POLICY (VOL-4, ISSUE-1)

ISSN-2583-8725
Vol - IV, Issue - I
Published by INTEGRITY EDUCATION INDIA

New Delhi
First Floor, 4598/12-B, 1st Floor,
Padam Chand Marg, Daryaganj,
New Delhi, Delhi 110002
Phone: +91 98 11 66 62 16 (M)
Phone: +91 70 11 60 56 18 (M)

Bengaluru
Jallahalli East
Bengaluru, Karnataka. India.
Phone: +91 98 11 66 62 16 (M)
Email: publisher.integrity@gmail.com

USA
New Jersey
14 Grandview Ave, Upper Saddle River,
NJ-07458, USA
Phone: +14805226504 (M)

London
37 Degree Media
64, Hodder Drive, Perivale, London UB68LL.
United Kingdom.
Phone: +44 7950 78 18 17 (M)
Website: integrityeducation.co.in

For any Query / Feedback
Phone: +91 98 11 66 62 16 (Vineet Sharma)

Printed in India @ New Delhi

ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

"Join the League of National and International Scholars"

LEX SCRIPTA MAGAZINE
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

LexScriptaMagazine.com ISSN: 2583-8725 Vol. 04 - Q1 Jan - Mar, 2026

Lex Scripta Journal

The Digital Personal Data Protection Act (2023): A Critique of State Exemptions

Author
Kush Mittal

The Digital Personal Data Protection Act (2023): A Critique of State Exemptions

Kush Mittal
Amity Law School, Amity University, Noida

Protecting User Privacy and Data

In the ***Puttaswamy case***[1], the Indian Supreme Court affirmed that privacy was a fundamental right under Article 21. This abstract examines the influence of contemporary data collection and technology on this right. The proliferation of digital technology has generated an unprecedented amount of personally identifiable information. This has raised concerns regarding the utilization and security of this information. While the Information Technology (IT) Act of 2000 serves as the principal data protection legislation in India, it is becoming challenging to determine its adequacy in safeguarding privacy among rapid technological advancements.

The primary issues include the widespread use of data analytics, governmental surveillance, and biometric data—such as iris scans and fingerprints—in systems like Aadhaar. These technologies jeopardize our personal data, despite their potential to substantially improve our quality of life. Ultimately, privacy is a right that the majority of Indians comprehend. The challenge lies in the necessity for ongoing legislative and regulatory efforts to adapt to evolving data practices and technologies.

Independence, data protection, and the ability to live autonomously without external interference are but a few facets of the right to privacy. Recognized as a fundamental element of human dignity and liberty, numerous nations and cultures have protected the right to privacy through various social and legal frameworks. Individuals possess the right to privacy if they wish to prevent others from intruding into their personal matters or swaying their decisions. Additional essential liberties encompass personal liberty, freedom of expression, and the right to a fair trial, which may intersect with the right to privacy within legal frameworks.

In the digital era, the collection, storage, and utilization of personally identifiable information have evolved. Both public and private enterprises generate and retain substantial quantities of personally identifiable information owing to the heightened utilization of mobile phones, social media, and other internet-connected devices. Financial records, medical records, and biometric identifiers constitute factors that render this data very sensitive. While technology advancements have yielded numerous benefits, like enhanced services and increased connectivity, safeguarding personal data has emerged as a paramount concern. Stringent privacy safeguards are essential due to the frequent occurrence of data breaches, unlawful spying, and the misuse of personal information. Mass data collection projects such as Aadhaar and the rapid digitization of the country have prominently elevated privacy concerns in public discourse in India. The

legal examination of the right to privacy has been comprehensive, and pivotal court decisions have shaped the national viewpoint on privacy rights.
Every individual possesses the freedom and the right to life as provided by Article 21 of the Indian Constitution. The court has expanded the scope of this article to encompass various facets of human dignity and existence; it has increasingly recognized the right to privacy as an essential element of personal liberty. The statute states, "No individual shall be deprived of life or personal liberty except in accordance with a procedure established by law." ***Kharak Singh v. State of Uttar Pradesh***[2](1963) is one of the initial cases concerning privacy under the Indian Constitution, involving a plaintiff subjected to police surveillance. Singh challenged the regulations permitting this form of surveillance. The Supreme Court of India observes that the Indian Constitution does not explicitly guarantee a right to privacy. The court noted that ordered liberty encompasses certain privacy aspects, like the sanctity of one's home. The court determined that some forms of monitoring were forbidden under Article 21 as they violated people' right to personal freedom. Although this ruling did not explicitly recognize a right to privacy, it established a foundation for subsequent discussions over personal liberty.

The circumstances surrounding R. India ultimately recognized privacy as a fundamental human right in the landmark 1994 case ***Rajagopal v. State of Tamil Nadu***[3], sometimes referred to as the "Auto Shankar Case." This is the autobiography of the convicted criminal Auto Shankar. His purported associations with various police personnel are meticulously documented throughout. The government attempted to prevent the publication of the book, citing privacy concerns. The Supreme Court ruled, to the publisher's relief, that Article 21 of the Constitution fundamentally protects private speech. The court's ruling asserts that individuals possess the right to prohibit the disclosure of their personal information without their agreement, unless a greater public interest in the publication exists. This case established, for the first time, that privacy is an inherent right within the context of personal liberty under Article 21, so altering Indian law.

The various types of data collected, managed, and utilized in the contemporary digital era raise specific privacy issues. Personal data encompasses information such as name, address, phone number, email address, and photos that may be utilized to identify an individual. Despite its significance for transactions and services, such data necessitates stringent security procedures to prevent misuse. Metadata comprises information regarding devices, time stamps, and geolocation, essentially representing data about data. Metadata's camera offers extensive insights into an individual's interests and behaviors, despite its inability to provide identification.[4]

Financial data encompasses details regarding credit cards, banking institutions, investments, and monetary transactions. This information is essential to ensure financial stability and avert fraud. Health data encompasses medical records, pharmaceutical details, biometric information, and data collected from health monitoring devices. Ensuring confidentiality and preventing bias based on medical history relies on the

safeguarding of health data. Data collection and processing constitute a significant endeavor for numerous Indian businesses, collectively contributing to the delineation of technological progress. The Unique Identification Authority of India (UIDAI) exemplifies a public sector organization by administering the Aadhaar program, which collects and records biometric and demographic data from all Indian citizens. Other branches of government also collect information for public safety, law enforcement, and intelligence purposes.[5]

To provide online services like as telephone and digital payments, Indian IT giants like Reliance Jio and Paytm manage vast quantities of data. These enterprises enhance their offerings, broaden their operations, and provide an improved client experience through data utilization. Online Social Networks: India possesses substantial user populations for Facebook and WhatsApp. To achieve targeted advertising and other corporate goals, these sites collect user interactions, usage trends, and personal data. The various methodologies employed for data collection in India reflect the diverse goals and applications for which data is obtained. Aadhaar is a prominent effort that aggregates biometric data, including fingerprints, iris scans, and facial photographs. In addition to identity verification and improving access to government and financial services, biometric data fulfills other roles.

Mobile tracking enables application developers and telecommunications firms to aggregate data on user location, call history, and application usage habits. This knowledge enables us to deliver location- based services, customize user experiences, and enhance network efficiency. Numerous government agencies and Internet Service Providers monitor user activity online for purposes of public safety and legal adherence. To detect and prevent cyberthreats and illicit activities, internet surveillance monitors users' online behaviors, encompassing search histories, email communications, and social media engagement. In recent years, science and technology have progressed significantly. Collecting extensive data from consumers is crucial for providing enhanced services that align with their requirements and preferences. The government has enacted legislation designed to protect the personal data that individuals in India provide with various online enterprises. The two paramount legislations are the Digital Personal Data Protection Act of 2023 and the Information Technology Act of 2000.
The recently enacted Digital Personal Data Protection Act, 2023 signifies a pivotal moment in the advocacy for individuals' privacy rights. It protects the data of users from many websites that share it.

The Act possesses numerous notable characteristics. The primary objective of the Digital Personal Data Protection Act is to facilitate the processing of digital personal data for legitimate reasons while simultaneously protecting individuals' rights to the security of their personal information. The personal information of data principals is subject to a duty of care, permitting its use solely for purposes authorized by the principal. This ensures, in accordance with the data principle, that the data will not be utilized for unlawful reasons. The data fiduciary managing the principal's information must first obtain the

principal's consent and provide a valid justification. It will implement all requisite measures to ensure the confidentiality of the principal's personal data. It is necessary to inform the affected parties and the Board of the infraction. Their responsibility is to ensure that issues are addressed in accordance with established protocols.6
When a data principal allows the processing of personal data, the Act confers special rights upon them. One such privilege is the capacity to grant, oversee, evaluate, and rescind authorization as required. Any personal information collected by the data fiduciary may be updated, removed, or contributed to in accordance with the data principle. Upon responding to a complaint, a data principal is able to request grievance resolution from the Board. In the event of a data principal infringement or other grievance, the following factors may be considered under the Act to determine the penalty: the nature, severity, and extent of the breach; the types and classifications of personal data affected; the recurrence of the breach; whether the individual incurred any losses or derived any benefits; and whether the individual undertook any measures to mitigate the breach's impact, as well as the timeliness and effectiveness of those measures. The Digital Personal Data Protection Act of 2023—a pivotal advancement in the protection of privacy rights in India—must address various outstanding difficulties and deficiencies to ensure its effective implementation and the realization of its objectives.

The federal government, possessing unfettered discretionary power, is not accountable for the actions of the states. The state possesses limitless authority. This implies they may have access to a plethora of public data, which they could utilize for their own political or national security objectives. The Act exempts many "instrumentalities of the State" from its regulations, thereby augmenting governmental authority. The Act encompasses both digital and non-digital data, including data generated by conversion into digital format. How can a Chinese individual ascertain whether the data custodian has digitized the paper records? Despite the Act's deviation from international standards, especially regarding "data anonymization" and "sensitive personal data," the Central Government maintains complete authority over the Data Protection Board of India, which is regarded as a premier and independent entity responsible for protecting individual privacy. This is regrettable.

The Supreme Court asserts that personal privacy is one of the most essential human rights. In August 2017, the Supreme Court of India delivered a ruling in ***Puttaswamy (Retd.) v. Union of India***[7]. K.S., Justice delivered a seminal ruling recognizing, pursuant to the Indian Constitution, a fundamental liberty protected by the right to privacy. Article 21 of the Constitution guarantees, as determined by the court, both the right to life and personal liberty, in addition to the right to privacy. This ruling renders enhanced privacy rights under Indian law viable, hence influencing overall privacy safeguards in India.
Founded in 2025 by the Indian government to supervise the execution of the Digital Personal Data Protection (DPDP) Act, 2023 and ensure digital personal data security, the Data Protection Board of India (DPBI) will have the authority to review complaints, impose penalties, and issue directives to ensure compliance with regulations. The Indian

government prohibited several Chinese smartphone applications in 2020 because to apprehensions around data privacy and national shortages. Among the prohibited applications, UC Browser, TikHub, and WeChat were particularly prevalent. The prohibition emphasized the importance of safeguarding personal information and ensuring its appropriate management and storage. It also emphasized India's necessity for enacting more rigorous data privacy regulations.

The COVID-19 pandemic has underscored the importance of privacy and data protection, as governments worldwide have implemented contact tracing and surveillance initiatives to monitor the virus's spread. The Indian government's digital measures to monitor COVID-19 cases and facilitate vaccinations have prompted concerns over privacy and security. The outbreak has demonstrated the necessity for more stringent legislative frameworks to protect personal data and ensure its secure handling and preservation.

The Indian Supreme Court, in a landmark decision, upheld in Justice ***K.S. Puttaswamy (Retd.) v. Union of India*** [8](2017) that Article 21 of the Indian Constitution ensures a fundamental right to privacy. The ruling recognized that privacy is essential to human rights and dignity in the digital era, and that safeguarding these rights primarily relies on preserving confidentiality. This decision in the struggle against increasing digitization and surveillance has significant implications for data protection and privacy.

The efficient operation of AI systems necessitates the collection and analysis of vast amounts of data. The collection of this data may involve personal information, raising significant privacy concerns. By analyzing data trends, AI may predict individuals' preferences and behaviors, hence facilitating intrusive profiling and violations of privacy. The automated decision-making capabilities of AI systems in areas such as employment, credit assessment, and law enforcement can profoundly impact human quality of life. These systems may exhibit deficiencies in transparency, accountability, and restitution for affected individuals.[9]

The Internet of Things (IoT) instantly generates a surge of data. Wearable health monitors and smart home appliances, like IoT devices, continuously collect data on the health, behavior, and activities of their users. potential risk exposures: Numerous IoT devices exhibit inadequate security measures, rendering them susceptible to hacking and unauthorized data access, both of which jeopardize personal privacy. Given the proliferation of technologies in contemporary society, it is possible to create a pervasive surveillance environment in which every individual's actions are monitored and recorded.

The real-time surveillance of individuals in both public and private settings facilitated by face recognition technology raises concerns about the erosion of anonymity and pervasive surveillance. Face recognition systems exhibit varying degrees of accuracy, leading to false positives and negatives that might result in bias or unwarranted charges. Facial recognition is frequently utilized without the knowledge or consent of persons

being monitored, who may not even be aware of its implementation.
Contemporary legislation requires revisions to privacy regulations to keep pace with technological changes. Comprehensive: New legislation must encompass all aspects of data collection, processing, storage, and distribution to protect individuals from intrusive technologies. Legislation must ensure that individuals are informed about data collection methods and need to provide explicit consent prior to data usage. Every individual possesses the right to access and manage their own data; they also have the right to rectify inaccuracies and eliminate superfluous items.[10]

A just society devoid of bias and errors relies on transparency in AI decision-making and the establishment of accountability frameworks. Protocols in connected device security: Regulation establishing stringent security standards for various devices should aid in mitigating data breaches and unauthorized access. To prevent abuse and protect individual rights, explicit regulations and limitations on the use of facial recognition technology are essential. Legislation governing surveillance must delineate the bounds of governmental oversight to ensure its legality and reasonableness. Companies should undergo regular audits, impact assessments, and compliance with privacy laws as part of their corporate data responsibilities.[11]

Educating the public on the necessity of enhanced data security and the benefits of digital literacy can be advantageous. Education and expertise: Promote digital literacy programs that educate individuals on the secure utilization of emerging technologies, the protection of personal information, and the implications of data collection. Instruct users to exercise caution while utilizing the internet; recommend the use of complex passwords, enable two-factor authentication, and be judicious regarding the content they share. Engagement of Civil Society Assist civil society organizations that seek to hold governments and corporations accountable while advocating for stronger privacy safeguards. Promoting transparent discourse on privacy issues will enhance understanding, inform the public, and foster solidarity in support of robust privacy legislation and policies.

Hate Speech

Social media has revolutionized global knowledge exchange and interpersonal interaction. Individuals globally can now interact through simple clicks on their phones or laptops, facilitated by the expansion of platforms such as Facebook, Instagram, and Twitter. Conversely, the proliferation of simplistic communication—capable of significant repercussions—has facilitated the growth of disinformation and hate speech. The pursuit of a solution to the problem of regulating hate speech on social media encounters significant obstacles within the Indian legal framework. The legislation pertaining to hate speech on social media platforms in India comprises the Indian Penal Code (IPC) of 1860 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules of 2021.[12]
The Indian Penal Code prohibits and penalizes communication that incites violence, hatred, or discord among various communities based on religion, ethnicity, place of birth, language, domicile, and other factors. The specific regulations on this matter are

delineated in sections 153A, 295A, 298, and 505. Under the IT Rules, 2021, intermediaries jeopardize their safe harbour status if they fail to erase or disable access to any information within 36 hours of receiving a complaint. Despite the legislative framework, Indian courts have numerous challenges in regulating hate speech on social media platforms.

India has a longstanding history of regulating hate speech, originating from the independence movement when freedom of expression was deemed fundamental. Nevertheless, regulations prohibiting hate speech and imposing restrictions were enacted due to the belief that the primary source of social discord was the freedom to free expression. Section 153A of the Indian Penal Code, instituted during the colonial period to mitigate escalating intercommunal violence, was the initial legal framework for regulating hate speech. Under Section 153A, which prohibits the promotion of communal discord and the inciting of hostility among various religious groups, the perpetrator was under suspicion. The Constitution of India was enacted in 1950 after the declaration of independence and sovereignty in 1947. Article 19 of the Constitution protected the right to free expression, subject to reasonable restrictions.

Restrictions on the right to free speech and expression have contributed to the prevention of crimes such as initiating illegal actions, contempt of court, and defamation. The landmark ruling in 1969, ***Kedar Nath Singh v. State of Bihar***[13], examined the dilemma of reconciling the basic right to free expression with necessary governmental restrictions. The Supreme Court of India ruled that a communication can only be prohibited if it incites violence or public disorder; derogatory or offensive comments alone do not constitute hate speech. The government has implemented measures inside the IPC to regulate hate speech online to align with contemporary standards. Section 505 was instituted to prohibit communication that incites public unrest; Section 295A criminalizes statements that intentionally denigrates a specific religious community. Subsequently, the government promulgated regulations in 2021 for Information Technology (Intermediary Guidelines and Digital Media Ethics Code) aimed at mitigating hate speech online.

India has historically struggled to regulate hate speech due to its extensive and diverse population. Historically, hate speech has been propagated through several channels, with social media being just one of them. The Indian government consequently enacted restrictions restricting such expression. The Indian Penal Code (IPC), enacted in 1860, prohibits communication that incites enmity, violence, or hostility among groups identified by religion, race, nationality, language, domicile, and other criteria. One of the objectives of the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 is the regulation of social media material. Despite these standards, regulating online hate speech poses significant challenges for Indian courts.

It is inherently challenging to hold intermediaries like Instagram, Twitter, and Facebook accountable for content generated on their platforms, given they possess legal immunity from accountability. Secondly, due to the number and rapidity of social media posts, law enforcement encounters significant challenges in identifying and apprehending offenders. The word "hate speech" is ambiguous, as free expression sometimes includes subjective criteria. The nation's linguistic and ethnic diversity complicates law enforcement efforts. Certain individuals contend that hate speech occurs when an individual intentionally targets another person or group based on their gender, sexual orientation, race, religion, ethnicity, or political ideas. While there are reasonable limitations on free speech in India, especially concerning hate speech, it remains a fundamental right.[14] Despite being fundamentally different, defamation and hate speech can both inflict harm on individuals and communities.

The latest regulations intended to regulate digital media and social media are the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, introduced by the Government of India. Social media firms must appoint grievance officers, a nodal officer, and a compliance officer to oversee adherence to legal requirements. Moreover, these sites must remove or restrict access to content deemed illegal under Indian law within a specified timeframe. A multitude of individuals are rejecting the standards, asserting that they infringe upon their rights to free expression and privacy. Critics argue that the government exerts excessive control over this content and that the legislation grants intermediaries excessive power to remove any material from social media platforms.

As a result, there have been widely reported instances of social media companies like Facebook and Twitter violating the new restrictions, leading to confrontations with the government. Additionally, the Indian government has recently instructed social media companies to comply with regulations or face legal repercussions. India continues to grapple with the issue of hate speech on social media. Social media platforms have disseminated hate speech and misinformation, resulting in religious discord and violent assaults. These facilities are subject to stringent government and law enforcement surveillance to facilitate the identification and apprehension of perpetrators.[15]

Regulating hate speech in Indian internet forums presents a complex challenge that necessitates a multifaceted approach. The government, social media companies, law enforcement agencies, and groups can together devise a solution that safeguards free expression while mitigating the adverse effects of hate speech. Employing machine learning algorithms, artificial intelligence, and natural language processing techniques will enable corporations operating social media platforms to proactively discover and eradicate harmful information. This strategy may facilitate the automation of the content moderation process, hence alleviating the workload of human moderators. A comprehensive examination of these aspects mitigates false positives and ensures transparent decision-making. The government should educate individuals on civility and the diversity of viewpoints present on social media. Targeted awareness initiatives that

inform individuals about how hate speech fractures communities, diminishes discourse, and fosters animosity will aid in achieving this objective.
The government must ensure the rigorous enforcement of existing laws and regulations to prevent the proliferation of hate speech on social media. Law enforcement officials should have adequate training to identify and investigate cases of hate speech on social media and to penalize persons who incite hatred or infringe upon the rights of others. While individuals possess the right to self-expression, it is imperative to recognize that this liberty has specific responsibilities. Exercising freedom of expression to propagate hate speech or infringe upon another's rights is fundamentally erroneous. The right to free expression is not an unlimited privilege; it is subject to valid constraints, especially where those limitations involve infringing upon the rights of others. Hate speech refers to any form of communication directed against a particular group based on their gender, sexual orientation, race, religion, ethnicity, or political beliefs. If a comment incites violence or harm to another individual, it may be classified as hate speech and lead to legal repercussions. [16]

Ultimately, India's efforts to regulate hate speech have significantly progressed since the colonial period. Legislation and regulations designed to govern society have evolved alongside its progression. However, issues arising from the proliferation of social media have prompted the government to enact new legislation aimed at mitigating hate speech on these platforms. The proliferation of hate speech on social media poses a significant challenge for Indian courts. A comprehensive technique is required to navigate the challenges of ambiguous definitions, jurisdictional conflicts, tracking, and identification, in order to balance free expression with the prompt administration of legal remedies. The creation of comprehensive regulatory frameworks that effectively address hate speech while preserving free expression relies on collaboration among the government, social media platforms, the judiciary, and civil society. India's judiciary requires a robust legal framework and proactive measures to effectively combat hate speech and create a safer internet environment. Addressing this substantial issue in the future would necessitate ongoing collaboration among the government, media entities, and civil society.

Addressing Disinformation and Fake News

India is a South Asian nation recognized for disseminating misinformation. Political misinformation in India remains pervasive, despite the discovery that religious and health-related dishonesty can obscure or exacerbate it. Political disinformation becomes most apparent prior to or during major political events. Political and various forms of deception stem from the prevailing political climate. Two political factors that occasionally facilitate the spread of misinformation are populist rhetoric and increasing societal division. Contemporary India exhibits both tendencies. Additionally, factors contributing to disinformation in India may include a fragmented audience, insufficient public service media, pervasive social media usage, and diminished trust in news sources. [17]

The Indian government often restricts internet access to mitigate disinformation instead of implementing a comprehensive and innovative anti-misinformation strategy. The disparate national regulations complicate the tracking of rumor disseminators. While several digital interventions, including Aarogya Setu and chatbots, have been employed throughout the epidemic to combat disinformation, they are simultaneously exacerbating the crisis of confidence in multiple ways.

In India, democracy exhibits a varied performance in combating disinformation methods. Some legislators have persistently propagated inaccurate and misleading health information, so undermining governmental efficacy, while governments have consistently sought collaboration with major digital companies to mitigate the dissemination of misinformation. The federal and state governments of India continued their initiative to prohibit Internet access in various locations of the country, irrespective of the COVID-19 situation. Some contend that this course of action is more conducive to suppressing political dissent and civil unrest.

Government efforts to counter misinformation encounter numerous challenges, including jurisdictional issues and the complexities of implementing new limitations on free speech. The new Intermediary Liability Rules, which impose extensive top-down constraints on platforms to censor content or limit users' right to free expression, may be unlawful and harmful to users both broadly and specifically. Nevertheless, the Indian government has established new regulations to govern over-the-top platforms, messaging applications, social media websites, and online news portals. Entitled "Rules," these directives pertain to intermediaries, digital media ethics, and information technology.

All enterprises operating in India, including multinational technology giants such as WhatsApp, Facebook, Twitter, Netflix, and Amazon, must comply with these regulations. The regulations governing social media platforms such as Facebook and Twitter focus on fraudulent user accounts, misinformation, automated messaging, and the oversight of illicit content. Compliance rates of social media platforms correlate with the size of their user base. Upon reaching 5 million registered users, a social media platform is classified as a significant social media intermediary and must adhere to compliance requirements to the fullest degree. Conversely, if any social media site poses a significant threat to India's sovereignty or security, the government possesses the ability to require compliance from other platforms with the regulations established by the dominant one.

Each major social media platform requires a designated Chief Compliance Officer, Nodal Contact Person, and Resident Grievance Officer. Each individual referenced above must consider India their domicile. Significant social media intermediaries must also be physically situated in India to ensure compliance with regulations. The requisite physical presence in India will substantially influence international corporations about infrastructure development, resource allocation, and taxation. Major social media intermediaries must now include human oversight, technology-driven restrictions, and

regular evaluations of automated systems. The astute scrutiny by intermediaries diminishes the safe harbour protection provided by the 2011 Rules.[18]
Social media and messaging platforms such as Google, Facebook, and WhatsApp have allegedly focused on enhancing awareness regarding political content, augmenting transparency in certain aspects of political material, verifying the legitimacy of political advertisers, and disclosing expenditures on political advertisements. Facebook has been eliminating fraudulent accounts in preparation for the elections, alongside collaborating with external fact-checking organizations. Platforms have initiated awareness campaigns and collaborated with local legislators and law enforcement organizations to combat misinformation. Typically implemented at the eleventh hour, these programs fail to address the specific challenges encountered by the Indian user demographic.

A multitude of inquiries has been posed on the efficacy of existing fact-checking activities. Facebook initiated its third-party fact-checking program in Karnataka, India, in 2018, and it has since expanded to additional Indian states. It has subsequently collaborated with external organizations to combat misinformation in eleven Indian languages. Some observers assert that Facebook's fact-checking policy is ineffective, as the platform fails to remove flagged content and its partner fact-checking systems lack efficiency. WhatsApp has included third-party fact-checking systems and imposed restrictions on bulk messaging to mitigate the dissemination of harmful content, hence complicating the process for users to transmit information to multiple recipients simultaneously. These advancements appear insubstantial and ineffectual to certain individuals.[19]

Political party personnel may employ inexpensive "clone apps" to disseminate materials to numerous recipients or exploit anonymous phone lines to bypass the prohibition on bulk texting. Observers of content regulation assert that social media companies' initiatives to combat misinformation are, at best, superficial remedies, as WhatsApp has introduced a fact-checking hotline to encourage users to report messages for verification. Preserving the intermediary framework would facilitate stability, although it would clarify the specific types of platforms required to qualify as intermediaries and obtain safe harbor protection. Implemented via amendments to the IT Act, a revision, clarification, and classification of the term "intermediaries" based on their functions—including web hosting services, search engines, social media, private messaging, and internet service providers—along with subsequent actions could facilitate this objective. Each of these subgroups may employ distinct operational methodologies, necessitating potential alterations in their respective tasks. One should furnish a detailed and exhaustive enumeration of the materials deemed illegal and detrimental. The current IT Act is inadequate in addressing concerns that could adversely affect individuals, such as cyberbullying, threats, and privacy invasions. Its assistance could also address challenges related to misinformation, disinformation, psychological manipulation, and hate speech.

Elucidate the government's jurisdiction regarding illicit content. Issues include the conditions necessitating eavesdropping or decryption of communications, the capacity and procedure for content removal, and the appropriate punishments for specific types of content. Platforms ought to limit their autonomous content removal authority to prohibited materials, such as pornographic and child sexual abuse content, and minimize such actions concerning verified users. If this happens, platforms—acting as legal authorities—would lose the ability to regulate user interaction content.[20] Platforms must be compelled to cease employing algorithms that prioritize particular types of content based on user profiling and selective promotion, thereby averting echo chambers. This mitigates the likelihood of platforms evolving into divisive knowledge echo chambers that exhibit prejudice.

Digital platforms have facilitated the spread of harmful misinformation on vaccinations, elections, and other public health issues; the circulation of counterfeit news and products; and the manipulation of digital content for political purposes, notwithstanding their significant financial success. The "social dilemma" is evident as digital media can facilitate both positive and negative outcomes. Efficient environmental regulation is essential to facilitate deceit, as platforms are evolving into "contemporary public squares" that govern discourse for billions globally. Neither the platforms nor the government have yet fulfilled this commitment. This article argues for a new participatory and responsive system of rule-making, asserting that India needs a transparent and accountable platform governance framework. Government involvement in oversight will inevitably increase.

Conversely, we believe that platforms should enhance the enforcement of self-regulation. During our examination of self-regulation, we found that businesses occasionally engender a "tragedy of the commons" by favoring their immediate interests over the broader welfare of the public or industry, thereby undermining the foundational conditions of their initial success. Numerous historical lessons are applicable to contemporary online platforms. Similar to modern social media platforms, corporations involved in the production of films, video games, television programs, and advertisements have always contended with the criteria that define "content" suitable for specific audiences.[81] The self-imposed and self-monitored rating system, still in use today, served as a defensive strategy employed by film and video game industries against regulatory bodies. In the 1950s and 1960s, analogous grievances concerning the suitability of advertisements, akin to those currently directed at internet advertising, were raised against the advertising and television industries.

In these conditions, self-regulation typically led to cost-effective and efficient company norms devoid of excessive government interference. These historical examples indicate that self-regulation was most effective when genuine government oversight was a feasible option. Digital platforms may ultimately need to cultivate self-restraint to avert a tragedy of the commons. Secondly, we note that enterprises in emerging areas frequently forgo self-regulation when they anticipate a significant decline in sales or

profitability due to the purported costs. Typically, managers oppose regulations perceived as detrimental to business; yet, this strategy may prove counterproductive. Digital platforms will falter if users begin to distrust them due to unethical practices. These "online intermediariesoxford exempt from accountability for user-generated information placed on their websites. They asserted that circumventing situations expected to create controversy would enhance the efficacy of their political and legal stances. Historically, numerous social media companies resisted stringent curating owing to internal disputes concerning the balance between free speech and censorship, as well as the delineation between a platform and "publishers" are mostly

Despite the relatively minimal involvement of the government in the internet age to yet, the regulatory landscape is rapidly evolving. Furthermore, collaboration between governments and digital platforms will be increasingly essential in the future. New institutional frameworks for enhanced participatory governance are crucial for the survival and profitability of social media platforms such as Twitter, Facebook, Google, and Amazon, particularly in light of the anticipated increase in governmental oversight of these sites. Responses to disinformation by platforms in India lack transparency and consistency across political parties and geographical regions. Implementing solutions is difficult due to the constantly evolving nature of disinformation issues.

Ensuring Platform Liability and Responsibility

Currently, content providers predominantly select social media as their platform. Contemporary digital content providers has a straightforward and expedient means to disseminate their work. Such quick access, however, is not without challenges and repercussions. Included among these nuances are the promotion of false information, the exploitation of intellectual property, and the use of vulgar language. This is why we should examine how social media may facilitate the dissemination of pornographic and misleading content. For social media businesses to be held liable for intellectual property rights violations, it is essential that they intentionally neglect to remove infringing content from their platforms while possessing reasonable awareness of the infringement.[21]

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (the "IT Rules") established specific compliance standards for social media intermediaries upon their enactment on February 25, 2021. To utilize the "Safe Harbour" defense under Section 79 of the Information Technology Act of 2000, several social media intermediaries required compliance. This Section protects intermediaries from liability for third-party content on their platform when the social media platform can prove it used adequate "due diligence" to comply with Act requirements.

The IT Rules possess several notable characteristics as outlined below:

The intermediary's grievance redressal system enables users or victims to report violations of IT regulations to the designated officer. The IT Rules stipulate that the Grievance Officer must promptly respond to complaints requesting the deletion of data or a communication link.

Major social media platforms in India—characterized by over 5 million registered users—are mandated to employ two individuals:

a) a Chief Compliance Officer (Key Managerial Personnel or other senior staff) residing in the country, and
b) a Nodal Officer (available around the clock to liaise with authorities) to facilitate compliance issues.

It delineated the parameters for the due diligence mandated for these social media intermediaries.

Although these regulations aimed to curtail the proliferation of hate speech, misinformation, and online harassment, it quickly became apparent that social media corporations occasionally misused the powers conferred upon them by the IT Rules. The inadvertent suspension of users' accounts without providing an opportunity for appeal has garnered the attention of Twitter and other social networking platforms. This unequivocally contravened Articles 14, 19, and 21 of the Indian Constitution, thereby protecting the rights of an Indian citizen. [22]

The Grievance Appellate Committee ("GAC") website, accessible at https://gac.gov.in/, indicates that the Indian government has initiated efforts to address this issue by implementing The IT Rules, which facilitate a digital method of conflict settlement. Social media users possess the right to contest decisions made on these platforms. Users of the social media intermediary may appeal to the Grievance Appeal Committee if they are dissatisfied with decisions made by Grievance Officers. Individuals who believe they have been aggrieved by a decision from the new website, may submit an appeal or complaint after 30 days of getting information from the grievance officer of an intermediary, such as Meta or Twitter.

Social Media Regulation

The proliferation of social media platforms has established new arenas for both positive and harmful occurrences. Users possess access to previously unimaginable knowledge and can articulate their thoughts freely. A disadvantage of this transparency is the prevalence of issues such as cyberbullying, misinformation, and hate speech. The tendency of social media to propagate dangerous content prompts the essential inquiry of how to mitigate these hazards without infringing upon free expression. Every democracy fundamentally guarantees the right to free expression. Nonetheless, there are constraints; unrestricted freedom of expression is impermissible when it significantly harms others.

Legislation prohibiting violence and slander is enacted to safeguard individuals and communities alike. Identifying the authority responsible for imposing limits and the substance requiring regulation is the difficulty. This becomes even more difficult when one contemplates social media. A singular solution cannot effectively accommodate the diverse cultural backgrounds of billions of users. Overreach is a significant concern as governments worldwide strive to regulate social media. Legislation should not restrict free expression under the guise of security, as this contravenes their fundamental purpose. Legislation intended to combat misinformation often raises concerns over censorship, as beneficial discourse may be perceived as detrimental content. We must engage in an inclusive dialogue that takes into account the perspectives of all stakeholders—including users, sociologists, legal experts, and IT firms—to achieve a balanced consensus.

Current Scenario Analysis

The rise of social media is significantly influencing the operation of democracies worldwide. Individuals can unite despite geographical constraints. The significant influence of India's social media rules has transformed the digital landscape. Their heightened content filtering criteria have substantially affected online free expression and raised concerns regarding potential curbs on it. These regulations establish intermediary accountability, therefore social media corporations are now progressively responsible for user-generated content.

Social media projects have generated numerous societal benefits. Kerala exemplifies a modern approach to optimising the right to free expression on social media. Mohammed, aged one and a half years, was afflicted with the relatively uncommon condition known as spinal muscular atrophy. Despite its cost of 18 crore rupees, Zolgensma is a medicine capable of curing this sickness. Due to an extensive social media effort initiated to save the child's life, 460 million was raised in within one week. In the aftermath of natural disasters, social media demonstrated significant importance. Social media advertisements can highlight unethical conduct and offer mechanisms for its cessation. As social media expands, individuals with similar ideologies have a platform to convene and articulate their thoughts openly.[24]

References

1. Parul Sharma, 'A Critical Evaluation of Social Media Regulation in India' (2022) *SSRN*
2. 'Regulated Social Media in India: A Study of Media User Perception' (2022) 3(2) *DME Journal of Communication*
3. 274.
4. Ministry of Electronics and Information Technology, 'Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021' (2021)
5. Chinmayi Arun, 'Gatekeepers of the Online Public Sphere: Intermediary Liability and Corporate Responsibility' (2019) 9 *NUJS Law Review* 1.
6. Parliament of India, 'Report of the Committee on Fake News and Paid News' (2019)
7. [18] Ministry of Electronics and Information Technology, 'Information Technology [Intermediary Guidelines (Amendment) Rules] 2018' (2018)
8. [19] Pratik Sinha and Arjun Sidharth, 'Misinformation and Its Impact on the Upcoming Indian Elections' (2019) *The Quint*
9. Anja Kovacs, 'Fake News, Hate Speech and Social Media Regulation in India' (2018) *Internet Democracy Project*
10. [15] Law Commission of India, 'Report No. 267: Hate Speech' (2017)
11. [16] Siddharth Narrain, 'Disaffection and the Law: The Chilling Effect of Sedition Laws in India' (2011) 46 *Economic and Political Weekly* 33.
12. [14] Prashant Iyengar, 'Hate Speech Laws in India' (2019) *Internet Democracy Project*
13. [13] Kedar Nath Singh v. State of Bihar AIR 1962 SC 955.
14. [11] Anirudh Burman, 'Will India's Proposed Data Protection Law Protect Privacy and Promote Growth?' (2020 *Carnegie India*
15. [12] Gautam Bhatia, 'Offend, Shock, or Disturb: Free Speech under the Indian Constitution' (Oxford University Press 2016
16. [9] Apar Gupta, 'Data Protection Law in India: A Constitutional Perspective' (2014) 50 *Economic and Political Weekly* 20.
17. [10] Ministry of Electronics and Information Technology, 'The Personal Data Protection Bill, 2019' (2019)
18. [2] Kharak Singh v. State of Uttar Pradesh AIR 1963 SC 1295.
19. [3] Rajagopal v. State of Tamil Nadu AIR 1994 SC 264.
20. [4] Pavan Duggal, *Cyber Law: The Indian Perspective* (4th edn, Saakshar Law Publications 2019).
21. [5] Usha Ramanathan, 'Illegality and the Right to Privacy' (2012) 4 *Indian Journal of Constitutional Law* 1.
22. [1] K.S. Puttaswamy v. Union of India (2017) 10 SCC 1

ABOUT LEX SCRIPTA JOURNAL

Lex Scripta Magazine is a premier peer-reviewed online and print journal dedicated to advancing scholarly research in law, policy, and social sciences. With the vision of promoting academic excellence and fostering a culture of intellectual exchange, the magazine provides a distinguished platform for academicians, researchers, legal professionals, and students to publish their original work and contribute to contemporary legal discourse.

Each submission undergoes a rigorous double-blind review process conducted by a panel of eminent national and international professors, ensuring the highest standards of quality and academic integrity. Lex Scripta not only encourages original and innovative research but also strives to bridge the gap between theoretical insights and real-world applications in the legal domain.

Contributors and editorial members receive global recognition through certificates and publication opportunities, while readers gain access to insightful, authoritative, and thought-provoking content across diverse areas of law and policy.

Now managed by Integrity Education India, Lex Scripta Magazine is committed to expanding its academic footprint through enhanced digital presence, global collaborations, and university partnerships. Upholding its ISSN identity, Lex Scripta continues to evolve as one of India's most trusted and respected journals in the field of legal research and education.

KEY FEATURES

- **Scholarly Insights** – Access in-depth, peer-reviewed research articles written by distinguished academicians and legal experts.
- **Global Perspectives** – Explore diverse viewpoints on law, policy, and governance from national and international scholars.
- **Authentic Content** – Read verified and academically sound articles that uphold the highest standards of research quality.
- **Knowledge Enhancement** – Stay updated with emerging trends, case studies, and policy developments across multiple legal domains.
- **Easy Accessibility** – Enjoy seamless access to online editions and exclusive hardcover issues for academic and professional use.

LEX SCRIPTA JOURNAL
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

CONNECT WITH US 9811 666 216
7011 605 618