

INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES
[ISSN 2581-5369]

Volume 9 | Issue 3

2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of any suggestions or complaints, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the International Journal of Law Management & Humanities, kindly email your Manuscript to submission@ijlmh.com.

Digital Media and the Law: Emerging Challenges to Press Freedom, Privacy, and Public Discourse

DR. LEENA CHHABRA*

ABSTRACT

The rapid expansion of digital media has fundamentally changed the ways in which information is created, shared, and consumed across the globe. While this transformation has opened numerous opportunities for public engagement, citizen journalism, and the free flow of ideas, it has also raised significant legal and regulatory challenges that existing systems struggle to address. In India, where Article 19(1)(a) of the Constitution guarantees the right to freedom of speech and expression, the digital revolution introduces new complexities into the delicate balance between freedom and responsibility. This paper examines three critical areas in which digital media and legal frameworks are increasingly at odds: press freedom, individual privacy, and the integrity of public discourse. As governments worldwide expand their control over online content through takedown orders, surveillance measures, and platform regulation, press freedom faces serious challenges. At the same time, the widespread collection and misuse of personal data by online platforms have raised urgent concerns about privacy rights, particularly in the absence of a strong and comprehensive data protection regime. The unchecked spread of misinformation, false news, and hate speech on social media has degraded the quality of public discourse, making it more difficult for citizens to distinguish fact from falsehood. The study adopts a doctrinal method, drawing upon Supreme Court decisions, legislative developments, and international regulatory frameworks to examine these issues in depth. The findings demonstrate that India's current legal framework is inadequate to address the challenges posed by digital media effectively. The paper concludes by advocating targeted legislative reform, improved judicial oversight, and accountable platform governance in order to create a digital media environment that is transparent, responsible, and protective of rights.

Keywords: Digital media; press freedom; privacy; misinformation; media regulation

Introduction

Digital media has had an unprecedented effect on the development of journalism, public discourse, and communication. In the current environment, the use of social networks, over-

* Author is an Academician, GD Goenka University, Gurugram, Haryana, India.

the-top (OTT) services, and web-based news applications has expanded significantly. Unlike traditional media, which is controlled by a small number of institutions, digital media makes it simple for people to share knowledge and information. This shift has given everyone easier access to information, but it has also given rise to new problems such as false information, online censorship, privacy violations, cybercrime, and regulatory challenges.

One of the principal changes brought about by digital media is the speed at which information spreads. Data that once took hours or days to reach people can now travel the world in a matter of minutes. This immediacy has strengthened civic engagement and enabled real-time reporting, but it has also made false information more common. Social media platforms deploy artificial intelligence (AI) to develop the algorithms that select which content to promote in order to increase engagement. As a result, these platforms tend to favour sensational content, making it more difficult to distinguish accurate information from falsehood.¹ This has generated serious concerns about political propaganda, media manipulation, and the erosion of public confidence in journalism.

Governments and regulatory bodies must simultaneously strike the ideal balance between responsible content and speed. While safeguarding data privacy, public order, and national security are legitimate concerns, overly stringent regulation may endanger fundamental rights. The legislation that several governments, including India, have enacted to manage and monitor digital information has raised concerns about censorship, the influence of large technology companies, and the crucial task of defending free speech and expression.

As new problems emerge in the digital sphere, such as deepfakes, AI-generated content, and cyberbullying, the legal framework must continually adapt. Information monitoring and secrecy present two further significant issues. With the rapid growth of internet usage, personal information has become a vital resource for businesses, government agencies, and advertisers. People are often unaware that their personal information is being used for surveillance or targeted advertising, a critical concern in the digital environment. Ongoing debates about data protection underscore the need for robust legal frameworks that can impose sanctions and provide a barrier between users and those who exploit their data. As digital media continues to develop, India and other countries must address these challenges while drawing on international best practices. Media literacy initiatives, transparent digital policies, and accountable journalism can improve the effective use of digital media. This paper explores the significant

¹ Eli Pariser, *THE FILTER BUBBLE: WHAT THE INTERNET IS HIDING FROM YOU* 15 (2011).

contemporary issues in digital media, emphasising their legal implications and the evolving regulatory landscape in India and elsewhere.

Misinformation, fake news, and media manipulation

Data moves faster than ever in today's hyperconnected world. A single post, video, or headline can affect millions of people within minutes, regardless of borders, languages, or social groups. While this speed offers real advantages, it has also produced a troubling problem: the widespread dissemination of misinformation, fake news, and deliberate media manipulation. Once a minor issue, it has become one of the greatest threats to public health, democracy, and social harmony.

Misinformation refers to inaccurate or false information disseminated without a clear intent to deceive, whereas fake news is content deliberately produced with the intention of misleading the audience. Media manipulation, by contrast, is a broader and more intentional phenomenon involving the selective presentation, alteration, or exaggeration of information to advance political, commercial, or ideological goals. Taken together, these three phenomena have the power to weaken governments, incite violence, and erode public trust in institutions. The COVID-19 pandemic may be the clearest example: the virus was accompanied by a dangerous wave of health disinformation that caused real and serious harm.²

Social media networks are now the primary source of false information. Regardless of the veracity of the information, algorithms designed to increase engagement frequently favour dramatic, emotionally charged, and divisive content. Because online platforms offer anonymity, unscrupulous actors are encouraged to spread misleading information without fear of repercussions. Political actors in particular have exploited these gaps to attack opponents, shape public opinion, and widen societal divides. In India, incidents of mob violence triggered by rumours circulated on WhatsApp have repeatedly highlighted the dangers of unchecked false information.

Authorities and regulatory bodies have taken action against false information through a number of laws and regulations. Critics counter that some of these measures may promote censorship and impede free speech. Although fact-checking and AI-enabled detection technologies have become essential strategies to combat misinformation, their efficacy is frequently constrained by the evolving tactics of bad actors. Public awareness campaigns are also crucial in teaching people how to identify false information and prevent its spread. Rather than being consolidated

² WORLD HEALTH ORG., *Infodemic Management Report* (2020); see also Ramachandra Guha, *COVID-19 and the Crisis of Misinformation in India*, 56 ECON. & POL. WKLY. 12 (2021).

into a single, comprehensive statute, India's legal response to disinformation is dispersed across several enactments.

The Information Technology Act, 2000

In the past, the Information Technology Act, 2000, particularly Section 66A, was used to restrict online communication and was frequently misused to stifle legitimate dissent. The Supreme Court struck down that provision as unconstitutional and excessively broad in *Shreya Singhal v. Union of India*.³ Under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, social media companies must identify the origins of false information and take down reported content within specified time frames. Critics argue that these rules give the government excessive control over online material, raising serious concerns about media freedom and censorship.

The Press Council of India, which regulates print media, has no jurisdiction over digital platforms. The absence of a unified and independent regulatory body for digital media is a significant weakness in the system. Combating false information requires more than legislation; it also calls for media education, platform accountability, and vigilant courts. People must be able to evaluate critically the information to which they are exposed. Platforms ought to take responsibility for the content they promote. Legislators must draft law that protects free speech while addressing harmful disinformation. Ultimately, combating misinformation is a democratic challenge rather than merely a legal one.

The Press Council of India Act, 1978

The Press Council of India Act, 1978 governs ethical journalism but lacks enforcement power over digital platforms.⁴

Election law: the Representation of the People Act, 1951

Section 123(4) of the Representation of the People Act, 1951 treats as a corrupt practice the publication of false statements of fact relating to a candidate's personal character or conduct, made with the object of prejudicing that candidate's electoral prospects.⁵ Section 126 prohibits the dissemination of election-related propaganda during the silence period, namely the forty-eight hours ending with the hour fixed for the conclusion of the poll.

³ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

⁴ Press Council of India Act, 1978, No. 37 of 1978, § 13; see also Madhavi Goradia Divan, FACETS OF MEDIA LAW 156 (2d ed. 2013).

⁵ Representation of the People Act, 1951, No. 43 of 1951, § 123(4).

Although India has legal safeguards against misinformation, stronger fact-checking, greater platform accountability, and improved digital literacy are needed to reconcile regulation with free speech.

Digital censorship, free speech, and government regulation

To address hate speech, threats to national security, and indecency, many nations, including India, have imposed restrictions on digital content. However, excessively stringent laws may endanger press and speech freedoms. Although governments contend that digital censorship is necessary to maintain public order and national security, critics point to instances in which authorities have used regulatory instruments to stifle dissent and curtail press freedom. With the rise of AI-based content moderation, automatic removals, and the growing influence of private firms over speech, the debate about digital censorship has intensified. The influence of digital corporations over what constitutes acceptable discourse, and the opacity of the criteria governing content regulation, have prompted wider discussion about the need for clear regulatory frameworks. In order to protect people from fraud while preserving their right to free speech and expression, governments must act as a buffer between wrongdoers and consumers of digital media.

The Constitution of India: Article 19

Article 19(1)(a) guarantees to every citizen the fundamental right to freedom of speech and expression, allowing individuals to express their opinions without government interference.⁶ Article 19(2) permits reasonable restrictions on that freedom in specified circumstances, including the interests of the sovereignty and integrity of India, the security of the State, public order, decency, and morality.⁷

The Information Technology Act, 2000

Section 69A empowers the government to block or remove any online content that may harm the sovereignty, integrity, security, or public order of the country.⁸ The provision is implemented through blocking orders, with which platforms must comply. Non-compliance can expose platform officials to fines and imprisonment.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

⁶ India Const. art. 19(1)(a).

⁷ India Const. art. 19(2).

⁸ Information Technology Act, 2000, No. 21 of 2000, § 69A; see also *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.

The Rules introduce a three-tier regulatory framework for digital content moderation.⁹ The first tier is self-regulation by platforms, including social media, news portals, and OTT services. The second is an industry-level oversight mechanism for grievances. The third is government oversight of content takedowns. The Rules mandate the removal of flagged content within thirty-six hours and require large platforms, such as Twitter, Facebook, and Instagram, to appoint compliance officers to liaise with the government.

The Cinematograph Act, 1952

Originally designed for film censorship under the Central Board of Film Certification (CBFC), the Cinematograph Act, 1952 has been supplemented by measures that bring OTT platforms, such as Netflix and Amazon Prime, under a comparable regulatory regime. These measures allow the government to revoke certification or block content deemed contrary to the public interest.

Privacy concerns, data protection, and surveillance

Data privacy concerns, unauthorised sharing of user data, and unauthorised data collection are among the negative aspects of digital media. Online privacy risks have increased in India owing to the historical absence of strong data protection legislation. The growth of digital platforms, greater reliance on AI-powered analytics, and extensive corporate and governmental monitoring programmes have deepened concerns about the erosion of personal privacy.

Privacy protection has become even more complex because of the surveillance economy, which is driven by targeted advertising and data monetisation. Users are often unaware of how various agencies use, retain, and access their data without their knowledge or consent. Incidents involving the widespread abuse of personal information without consent have raised concerns about safeguarding against data breaches. Although the European Union's General Data Protection Regulation (GDPR) has become an influential global benchmark, India long lacked a robust domestic legal regime of comparable strength.

The right to privacy: the Puttaswamy judgment

In *Justice K.S. Puttaswamy v. Union of India*, the Supreme Court held that privacy is a fundamental right under Article 21, which guarantees the right to life and personal liberty.¹⁰ The Court held that the State cannot infringe an individual's privacy except in accordance with a procedure that satisfies the requirements of legality, necessity, and proportionality.

⁹ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 9.

¹⁰ *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

The Personal Data Protection Bill, 2019, and the Digital Personal Data Protection Act, 2023

Modelled on the EU's GDPR, the Personal Data Protection Bill, 2019 sought to regulate the storage and processing of personal data, to impose user-consent requirements for data sharing, to require the localisation of sensitive data, and to create a Data Protection Authority for oversight. The Bill was subsequently withdrawn, and Parliament enacted the Digital Personal Data Protection Act, 2023 in its place.¹¹

The Information Technology Act, 2000: Sections 43A and 72A

Section 43A requires companies to compensate users for data breaches caused by negligence in protecting sensitive personal data. Section 72A penalises the unauthorised disclosure of personal information by intermediaries or service providers in breach of a lawful contract.¹²

The Indian Telegraph Act, 1885, and surveillance mechanisms

The Indian Telegraph Act, 1885 empowers the government to act, in specified circumstances, against material or information that may harm the sovereignty, integrity, security, or public order of India. India's surveillance apparatus includes the Central Monitoring System (CMS), which enables real-time tracking of calls, emails, and messages, as well as NETRA and NATGRID, which support the monitoring of digital communication.

Social media accountability and the IT Rules, 2021

Social media platforms have become important instruments of public discourse, influencing politics, business, and interpersonal relationships. However, their largely unchecked power has raised concerns about misinformation, content moderation, cyberbullying, and user protection. With billions of users, social media profoundly shapes opinions and beliefs, yet it frequently permits the spread of false information and invasions of privacy. The absence of clear accountability has resulted in increased regulatory scrutiny. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 were introduced to address these concerns. By imposing better content standards and requiring conformity with government directions, the Rules were intended to contribute to the protection of individual rights.

Classification of intermediaries

¹¹ Personal Data Protection Bill, 2019 (withdrawn); Digital Personal Data Protection Act, 2023, No. 22 of 2023; see also COMM. OF EXPERTS UNDER THE CHAIRMANSHIP OF JUSTICE B.N. SRIKRISHNA, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018).

¹² Information Technology Act, 2000, No. 21 of 2000, § 43A; id. § 72A.

The Rules distinguish between Significant Social Media Intermediaries (SSMIs), namely platforms with more than fifty lakh (five million) users, which must comply with stricter obligations, and ordinary social media intermediaries, namely smaller platforms subject to fewer compliance obligations.

Grievance redressal mechanism

Platforms must appoint a Grievance Officer to address user complaints within fifteen days. This mechanism enables users to report misinformation, offensive content, and privacy violations.

Identification of the first originator

Messaging services such as WhatsApp and Telegram may be required, on the order of a competent authority, to disclose the identity of the first originator of a message. This requirement aims to curb fake news and harmful viral content, although critics argue that it undermines end-to-end encryption and thereby raises privacy concerns.

Content removal and compliance with government orders

Social media companies must act swiftly against unlawful content, removing it within thirty-six hours of receiving a complaint. Non-compliance may result in the loss of safe-harbour protection, rendering platforms legally liable for user-generated content.

Oversight mechanism and self-regulation

The Rules introduce a three-tier regulatory framework for content moderation.¹³ The first tier is self-regulation by platforms, ensuring compliance with their own policies. The second comprises industry-level regulatory bodies for grievance redressal. The third is government oversight, including an inter-departmental committee to monitor compliance.

Conclusion

The complex problems posed by the evolving landscape of digital media and legal regulation require a careful balance between governance and fundamental rights. India needs rules that balance democratic rights, user rights, and press freedom in order to address misinformation, digital censorship, privacy concerns, and social media accountability. While measures such as the IT Rules, 2021 aim to combat online harms, they also raise concerns about data privacy, state overreach, and free speech.

Future-focused legislation should take into account international best practices while remaining attentive to India's particular sociopolitical context. It should strengthen fact-checking

¹³ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 9.

initiatives, encourage corporate responsibility, and educate the public about misinformation and manipulation on digital platforms. Furthermore, a robust data protection regime is essential to safeguard user privacy against extensive surveillance and the illicit use of data. Regulatory systems must be guided by judicial oversight and transparency in order to prevent arbitrary enforcement and overzealous censorship. A safer and more transparent online environment can be achieved by encouraging self-regulation on digital platforms alongside government oversight, subject to appropriate checks and balances. Given the growing impact of technology on public discourse and governance, policymakers, the judiciary, technology companies, and civil society must collaborate to create progressive, adaptable, and rights-focused digital regulation that supports innovation while preserving individual liberty.
