

# International Journal Research Publication Analysis

Page: 01-10

---

## REGULATING SOCIAL MEDIA IN THE DIGITAL AGE: A COMPARATIVE STUDY OF THE UNITED STATES AND THE UNITED KINGDOM

---

**\* Preeti Sharma**

Student LL.M. (Master of Laws), Amity Institute of Advanced Legal Studies, Amity  
University, Noida, Uttar Pradesh, India.

---

**Article Received: 13 September 2026**

**Article Revised: 03 October 2026**

**Published on: 23 October 2026**

**\*Corresponding Author: Preeti Sharma**

Student LL.M. (Master of Laws), Amity Institute of Advanced Legal Studies,  
Amity University, Noida, Uttar Pradesh, India.

DOI: <https://doi-doi.org/101555/ijarp.9956>

---

### ABSTRACT

Social media has changed how people talk to one another. It has opened up access to information for millions, but it has also created hard legal problems: misinformation travels fast, unlawful content circulates freely, personal data is mishandled, and platforms are rarely held to account. The central difficulty for any regulator is deciding how to tackle these harms without trespassing on speech that the Constitution protects.

This paper looks at how India, the United States and the United Kingdom have responded. For India, the discussion draws on Articles 19 and 21 of the Constitution, the Information Technology Act, 2000, the Intermediary Guidelines Rules, 2021 and the Digital Personal Data Protection (DPDP) framework. For the United States, it turns to First Amendment case law and Section 230 of the Communications Decency Act. For the United Kingdom, it considers the systemic, regulator-led model of the Online Safety Act 2023. Using doctrinal and comparative methods, the paper shows how each system divides responsibility between the State, platforms and users. Its conclusion is that India should build its regime on proportionality, fair procedure, transparency in algorithms and genuinely independent oversight.

**KEYWORDS:** Social Media Regulation, Freedom of Expression, Intermediary Liability, Digital Privacy, Data Protection, Online Safety.

## 1. INTRODUCTION

The internet has rearranged the way public debate takes place. Anyone with a phone can now publish to a wide audience, without going through editors or broadcasters. That shift has strengthened democratic participation and widened the space for free speech. It has also brought serious risks, from viral falsehoods and state-backed disinformation to targeted harassment, algorithmic radicalisation and intrusions into private life. So the real question has changed. Few people still ask whether platforms should be regulated at all; the live issue is how to regulate them so that harm is reduced while expression and privacy remain safe. The question becomes especially pressing when a State measure cuts directly into a constitutional right.

India is a revealing case. Its law has to reconcile the freedoms in Article 19(1)(a)<sup>1</sup> and Article 21<sup>2</sup> of the Constitution with the restrictions found in the Information Technology Act, 2000<sup>3</sup>, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021<sup>4</sup> and the digital Personal Data Protection Framework<sup>5</sup>. Placing this layered arrangement beside the strongly constitutional, hands-off American approach and the administrative, risk-focused British one helps show how public-interest goals can be pursued without sacrificing individual rights.

## 2. Statement of the Problem

Indian law on digital platforms is scattered across statutes, executive rules and court rulings. Content moderation is governed by the IT Act and the IT Rules, while personal data is governed separately by the Digital Personal Data Protection Act, 2023 (DPDP Act) and the Digital Personal Data Protection Rules, 2025. Intermediaries must therefore satisfy two sets of obligations at once, and state agencies face messy enforcement questions. The result is a standing tension between acting early against harm and protecting lawful speech and informational privacy.

The core problem this paper takes up is whether India's present framework meets the standard of constitutional proportionality, and which regulatory principles can be drawn from the contrasting American and British models.

## 3. Research Questions

1. How far does India's constitutional and statutory framework manage to regulate social media intermediaries while protecting the rights guaranteed by Articles 19 and 21?
2. How do the United States and the United Kingdom regulate social media in terms of

intermediary liability, online safety and user rights?

3. Where do the Indian, American and British approaches to platform governance converge, and where do they part ways?

4. Which principles can India take from these comparative experiences to arrive at a

Framework that is proportionate, transparent and compatible with rights?

#### **4. Research Objectives**

1. To examine the constitutional principles, statutes and subordinate legislation that govern social media in India.

2. To assess the American and British models of intermediary liability and online safety.

3. To compare the three jurisdictions on free expression, safe harbours, data privacy and platform accountability.

4. To propose reasoned reforms that strengthen procedural safeguards, algorithmic transparency and fundamental rights in India's digital governance.

#### **5. Research Methodology**

The study is qualitative and relies on doctrinal and comparative legal research. The doctrinal part reads primary materials closely (constitutional text, statutes, executive rules, notifications and judgments) together with scholarly articles, law review pieces and institutional reports. The comparative part takes a functional approach: it asks how three different constitutional systems deal with the same problems that digital platforms create.

The work is purely legal in nature and rests on qualitative analysis, not on survey or empirical data.

#### **6. Research Hypothesis**

A regulatory framework that is both effective and constitutionally sound must share responsibility sensibly among the State, the platforms and the users. Too much State control may chill lawful speech and widen surveillance, while complete immunity for intermediaries leaves users exposed to large-scale digital harm. If India improves platform transparency, procedural due process, independent oversight and privacy protection, its intermediary regime will sit more comfortably within constitutional proportionality.

## 7. Literature Review

The Academic literature on social media regulation broadly converges on three interconnected thematic domains:

The first deals with private power over public speech. Jack Balkin, among others, argues that doctrines built to restrain the State need rethinking for a "triadic" structure involving the State, the companies that run the infrastructure, and the users. When public conversation takes place on privately owned systems, platforms can act as private rulers who silence speech while facing none of the limits that bind governments.

The second strand concerns intermediary liability. Anupam Chander and Lilian Edwards trace the move from treating intermediaries as passive conduits to holding them responsible for what they actively do. A recurring point in this work is that recommendation engines and curation tools weaken the old case for blanket immunity, since platforms plainly shape what people see.

The third strand links data protection to online harm. Shoshana Zuboff's account of surveillance capitalism suggests that moderation cannot be separated from data processing, because platform business models depend on extracting behavioural data. Data protection law is therefore part of platform governance, not an add-on.

**Research gap:** Much of the existing writing handles content moderation, safe harbours and data protection as separate subjects. This paper brings them together in one comparative public-law analysis and asks how India, the United States and the United Kingdom connect constitutional rights, statutory liability and data governance.

## 8. Social Media Regulation in India

### 8.1 Constitutional framework

Article 19(1)(a) of the Indian Constitution protects speech and expression on digital platforms, but the right is not unlimited. Article 19(2) allows reasonable restrictions on grounds such as the sovereignty and integrity of India, the security of the State, public order, and decency or morality. In *Shreya Singhal v. Union of India*<sup>6</sup>, the Supreme Court made clear that speech online deserves the same constitutional protection as speech offline.

Furthermore, the Article 21, which secures life and personal liberty, was read in *K.S. Puttaswamy v. Union of India*<sup>7</sup> by a nine-judge Bench to include informational privacy. The Court held that the State may interfere with privacy only if three conditions are met: the interference must have a legal basis (backed by law), it must pursue a legitimate State

aim, and the means chosen must be proportionate to that aim. Any Indian regime for social media must therefore respect speech and privacy together.

## **8.2 The Information Technology Act, 2000**

The Information Technology Act, 2000 is the main statute for digital governance. Section 79 gives intermediaries conditional protection from liability for third-party content, provided they act as neutral facilitators and follow due-diligence requirements. In *Shreya Singhal*, the Court struck down Section 66A as vague and overbroad and read down Section 79(3)(b). As a result, an intermediary forfeits its safe harbour only when it fails to remove unlawful material promptly after receiving "actual knowledge", which means a court order or a direction from an authorised government agency, and not merely a complaint from a user.

## **8.3 The Information Technology Rules, 2021**

The government notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 to put these obligations into practice. The Rules work in tiers. Significant Social Media Intermediaries (SSMIs), meaning those with more than five million registered users in India, carry heavier duties. They must appoint a Chief Compliance Officer, a Nodal Contact Person and a Resident Grievance Officer, publish monthly compliance reports, enable identification of the first originator of a message on encrypted messaging services, and use automated tools to filter content.

The aim is to curb online harm and make platforms answerable, but the Rules have been challenged in court. Critics say that automated filtering and traceability weaken end-to-end encryption and anonymity, and that they push platforms to over-remove lawful speech so as to keep their immunity.<sup>1</sup>

## **8.4 Data protection Framework: The DPDP Act, 2023 and DPDP Rules, 2025**

The Digital Personal Data Protection Act, 2023<sup>8</sup> and the Digital Personal Data Protection Rules, 2025<sup>9</sup> give India its first full privacy regime. Social media platforms are Data Fiduciaries and handle huge amounts of personal data belonging to Data Principals. The framework places duties on them concerning notice, clear consent, purpose limitation, data minimisation and security.

This regime touches social media governance directly, because it covers profiling, behavioural advertising and the collection of user data. A platform operating in India must now meet content-moderation requirements under the IT Rules and data-processing

standards under the DPDP framework at the same time.

## **9. Comparative Models: United States and United Kingdom**

### **9.1 The United States: the First Amendment and Section 230**

American law combines firm constitutional protection for speech with statutory immunity for intermediaries. Under the First Amendment, government restrictions on speech are examined with strict scrutiny and are presumed unconstitutional unless they are narrowly tailored to a compelling State interest.

Section 230 of the Communications Decency Act of 1996<sup>10</sup> is the foundation of internet governance there. Section 230(c)(1) says that no provider or user of an interactive computer service is to be treated as the publisher or speaker of information supplied by someone else. Section 230(c)(2) shields platforms from civil liability when they, in good faith, restrict access to material that is obscene, harassing, excessively violent or otherwise objectionable. The outcome is very broad protection for intermediaries, which has encouraged both innovation and private moderation. In *Moody v. NetChoice, LLC*<sup>11</sup>, the Supreme Court recognised that when platforms curate and arrange the content they display, they are engaged in expressive activity that the First Amendment protects. The decision signals tight limits on state laws that try to dictate how platforms moderate, though the Court sent the cases back to the lower courts for a fuller analysis.

### **9.2 The United Kingdom: the Online Safety Act 2023**

The United Kingdom has moved away from the passive-conduit idea by passing the Online Safety Act 2023<sup>12</sup>. Supervised by the independent regulator, the office of Communications (Ofcom), the Act replaces piecemeal takedowns with systemic duties of care.

Regulated services must carry out risk assessments, take proactive steps against illegal content, protect children from harmful material and offer clear complaint procedures. Notably, the Act also requires Ofcom and the platforms to weigh their safety duties against the protection of lawful expression and user privacy. The British model is thus administrative and risk-based.

## 10. Comparative Analysis

The three systems rest on quite different ideas about public law and regulatory design.

| Dimension                    | India                                                                                       | United States                                                           | United Kingdom                                                                   |
|------------------------------|---------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| <b>Primary Mechanism</b>     | Conditional safe harbor paired with mandatory executive due-diligence rules.                | Near-absolute statutory safe harbor (Section 230) and self-regulation   | Systemic statutory duty of care enforced by an independent regulator (Ofcom)     |
| <b>Constitutional Anchor</b> | Article 19(1)(a) speech, balanced against Article 19(2) restrictions and Article 21 privacy | Strong First Amendment protection against government content regulation | Human Rights Act 1998, incorporating European Convention rights (Arts. 8 and 10) |
| <b>Content Curation</b>      | Executive or judicial takedown orders with strict timelines                                 | Platform editorial discretion protected as First Amendment speech       | Risk-assessment obligations and systemic design duties to reduce illegal harms   |
| <b>Data Governance</b>       | Dedicated statutory regime (DPDP Act, 2023 and Rules, 2025)                                 | Sectoral federal laws plus state statutes (e.g., CCPA)                  | UK GDPR and Data Protection Act 2018, operating alongside the Online Safety Act  |

India sits somewhere between the hands-off American position and the administrative British one. The United States prizes corporate editorial freedom, and the United Kingdom stresses managing systemic risk, whereas India leans heavily on direct executive oversight. That reliance on executive orders under the IT Rules raises procedural concerns, which the United Kingdom softens by giving oversight to an independent statutory body, the office of Communications (Ofcom).

## 11. Critical Analysis: Major Challenges in India

In India's Social Media Governance framework faces a lot of conceptual and the operational challenges:

1. Chilling effect on speech and the Expression: Short compliance deadlines and penalties for failure give platforms every reason to over-remove content. Taking down anything controversial is the safest way to keep statutory immunity.
2. Encryption and anonymity: Traceability requirements for messaging apps clash with end-to-end encryption and sit uneasily with the privacy protection recognised in *Puttaswamy* under Article 21.
3. Regulatory overlap: Platforms must follow both the IT Rules and the DPDP framework, which creates operational complexity and calls for clearly drawn institutional boundaries.

4. Algorithmic opacity: Automated moderation often misses context, regional languages and satire. Content can then be suppressed arbitrarily, with little real chance of judicial review.

## **12. Findings and Recommendations**

### **12.1 Key findings**

1. Regulating social media cannot be separated from constitutional public law, since both content removal and data processing affect free expression and privacy.
2. India's framework has many layers, but compared with other democracies it leans strongly on administrative and executive control.
3. The American model gives the most room to free expression at the cost of limiting harm reduction, while the British model builds in a proactive duty of care that protects users through the way systems are designed.

### **12.2 Recommendations for India**

1. Statutory Incorporation of proportionality into the law: Blocking orders under Section 69A of the IT Act and under the IT Rules should follow the proportionality standard laid down in *Puttaswamy*.
2. Create independent appellate oversight: Instead of executive-controlled Grievance Appellate Committees, India should set up an independent, quasi-judicial digital tribunal to hear user appeals against platform decisions.
3. Require algorithmic audits: SSIMs should undergo regular independent audits of their automated filtering tools, to guard against discriminatory or overbroad suppression of content.
4. Align the IT and DPDP regimes: Regulators should issue clear guidance reconciling intermediaries' compliance duties under the IT Rules with the data-minimisation requirements of the DPDP Rules, 2025.

## **13. CONCLUSION**

Regulating social media is hard because two things we care about pull in opposite directions. People deserve protection from hate speech, harassment, fraud and misinformation. But these platforms are also where people argue, organise, share news and use rights the Constitution guarantees them. A rule that makes the internet safer by quietly shrinking free speech hasn't solved much.

Countries have handled this very differently. In the US, Section 230 and a strong free-speech tradition leave most content decisions to the platforms themselves. The UK went the other way with the Online Safety Act, which makes platforms assess the risks their services create and gives Ofcom the power to enforce it. India sits somewhere in between, and it's messy. Our approach is stitched together from the IT Act, the 2021 IT Rules, court rulings and executive directions, so neither users nor companies can always tell where the lines are.

So what should India do? First, move away from governing by sudden orders. Section 69A blocking orders and similar powers are often used with little transparency, and the Shreya Singhal judgment already told us that vague restrictions on speech don't survive constitutional scrutiny. We need clear laws that spell out what platforms, users and the government may and may not do. Any limit on speech should be necessary and proportionate to the harm it targets.

Process matters just as much. If your post or account is taken down, you should be told why, be able to appeal, and have the decision reviewed by someone independent of both the platform and the government. The state needs checks too, because powers without oversight tend to get misused. And none of this works without solid data protection. The DPDP Act is a start, but people's personal information shouldn't be collected or passed around without real safeguards.

India doesn't have to copy anyone. It can borrow what has worked, avoid what hasn't, and build something that fits its own constitutional values and social reality.

The aim is a digital public space that is safe without being stifling, accountable without being oppressive, and open without being lawless. Proportionality, transparency, fair procedure, independent oversight and data protection are the foundations for getting there.

## **BIBLIOGRAPHY**

### **Primary Sources – India**

1. The Constitution of India, 1950.
2. The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).
3. The Digital Personal Data Protection Rules, 2025, Ministry of Electronics and Information Technology, Government of India.
4. The Information Technology Act, 2000 (Act No. 21 of 2000).
5. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

### Primary Sources – Foreign Jurisdictions

6. Communications Decency Act of 1996, 47 U.S.C. § 230 (United States).
7. The Constitution of the United States of America, 1787, Amendment I.
8. Human Rights Act 1998, c. 42 (United Kingdom).
9. Online Safety Act 2023, c. 50 (United Kingdom).

### Judicial Decisions

10. *K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
11. *Moody v. NetChoice, LLC*, 603 U.S. 707 (2024).
12. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

### Secondary Sources and Institutional Materials

13. Balkin, Jack M., "Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation", *University of California, Davis Law Review*, Vol. 51, 2017, pp. 114U–1210.
14. Chander, Anupam, "How Law Made Silicon Valley", *Emory Law Journal*, Vol. 63, 2014,
15. pp. 639–694.
16. Edwards, Lilian, *Law, Policy and the Internet*, Hart Publishing, Oxford, 2019.
17. The office of Communications (Ofcom), *Regulatory Policy Framework under the Online Safety Act 2023*, London, 2024.
18. Zuboff, Shoshana, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, New York, 2019.
19. The Constitution of India, 1950, art. 19(1)(a).
20. The Constitution of India, 1950, art. 21.
21. The Information Technology Act, 2000, No. 21 of 2000, Acts of Parliament, 2000 (India).
22. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), Ministry of Electronics and Information Technology, Government of India.
23. The Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament, 2023 (India).
24. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
25. *K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
26. Digital Personal Data Protection Act, 2023, ss. 4–11.
27. The Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Ministry of Electronics and Information Technology, Government of India, 13 November 2025.
28. Communications Decency Act of 1996, 47 U.S.C. § 230.
29. *Moody v. NetChoice, LLC*, 603 U.S. 707 (2024).
30. Online Safety Act 2023, c. 50 (UK).