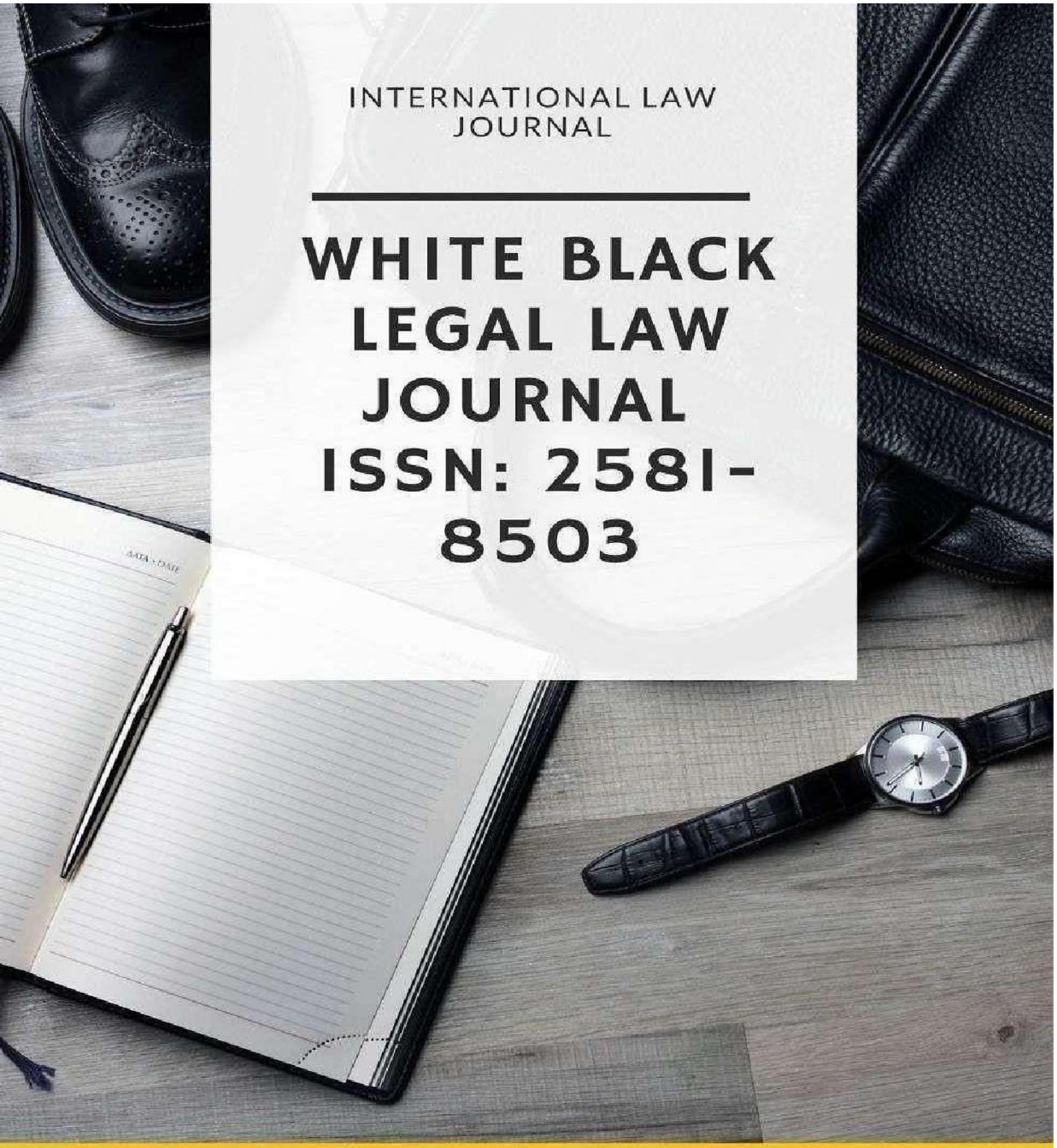


INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

WHITE BLACK LEGAL

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

ONLINE SPEECH, OFFLINE CONSEQUENCES: REGULATING SOCIAL MEDIA IN INDIA

AUTHORED BY - S.THARIKA, UME TAHREEM, SANGAVI S & LAKSHITHA K

ABSTRACT

Social media is now one of the main places where Indians talk politics, argue about public issues and take part in civic life. Article 19(1)(a) of the Constitution protects this speech. But the same platforms have also brought misinformation, hate speech, deepfakes, cyberbullying and organised disinformation. To deal with these, the Government relies on wide powers under the Information Technology Act, 2000 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. These include taking down content, blocking it, intercepting messages and tracing who sent them. Such powers raise fears of censorship, prior restraint, executive overreach and a chilling effect on speech, and they touch Articles 14, 19 and 21.

This paper looks at the constitutional and statutory framework, the leading Supreme Court decisions and recent High Court rulings, and the new problems created by deepfakes, bots, encryption and AI-based content moderation. It combines a doctrinal study of the law with a comparison of the United States, the European Union and the United Kingdom, and a small public survey. The comparison shows that the European and British models build in transparency, independent oversight and a right of appeal for users, which India's blocking and interception scheme does not. In the survey, 75% of respondents had come across fake news or deepfakes, only 39.6% knew of government rules on social media content, and 75% wanted an independent body to decide what is fake or harmful.

The paper concludes that India needs independent checks before content is blocked, openness about blocking orders, clear duties for platforms, user rights to notice and appeal, and a law on AI and deepfakes that respects proportionality. It also argues that responsibility is shared, and that digital literacy is part of the answer.

Keywords: social media regulation; Article 19(1)(a); privacy; IT Act, 2000; IT Rules, 2021; intermediary liability; deepfakes; content moderation; comparative law.

1. INTRODUCTION

1.1 Background

WhatsApp, YouTube, Instagram, Facebook and X are now part of daily life in India. The country is estimated to have more than 800 million internet users and over 460 million active social media users.[1] People use these platforms to debate public issues, criticise those in power, organise protests and share news. Governments use them too, to explain policies and deliver services. Social media has become a central space for political talk and civic participation.

Article 19(1)(a) of the Constitution, which guarantees every citizen the freedom of speech and expression, covers this activity.[2] Courts have accepted that the freedom does not end at the newspaper or the public square. It reaches the internet as well.[3]

Fast growth has also brought serious harm: misinformation, fake news, hate speech, deepfakes, cyberbullying and coordinated disinformation. The World Economic Forum lists misinformation and disinformation among the top global risks.[4] In India, false posts have led to communal tension, public panic, financial fraud and misleading claims during elections.

The Government has answered with wide powers under the Information Technology Act, 2000 and the IT Rules, 2021. These cover removing content, tracing the originators of messages and suspending accounts. The stated aims are national security, clean elections and public order. But these measures also raise worries about censorship, prior restraint, executive overreach and a chilling effect on free speech.

The title of this paper, *Online Speech, Offline Consequences*, points to both sides of the problem. What is said online can hurt people in the real world. But the rules made to control online speech also have real consequences for people's rights, their privacy and their ability to take part in democracy.

WHITE BLACK LEGAL

1.2 Statement of the Problem

The main problem is that India has no complete constitutional framework that balances free speech, privacy, platform accountability, national security and democratic governance online. The specific issues are these.

- Critics argue that the powers to block, intercept and trace content may violate Article

[1] Internet and social media user figures differ by source and year. The figures used here (over 800 million internet users and over 460 million active social media users, 2025 estimates) are those compiled in the problem statement of this study and should be read as approximations.
[2] Constitution of India, 1950, art. 19(1)(a): all citizens shall have the right to freedom of speech and expression.
[3] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.
[4] World Economic Forum, Global Risks Report 2024, which ranks misinformation and disinformation among the most severe global risks over the short term.

19(1)(a) (speech), Article 21 (privacy) and Article 14 (protection from arbitrary State action), particularly where safeguards and judicial oversight are weak.

- Platforms are unsure about their own duties, including intermediary liability, content moderation, data protection and compliance with government orders.
- AI-based content moderation raises new questions about transparency, algorithmic bias and due process.
- New problems such as deepfakes and coordinated bot networks are not clearly dealt with in constitutional case law or in the parent statute.

1.3 Need for the Study

- India has no clear constitutional framework for online speech, platform accountability and State action in this area.
- The IT Rules, 2021 and their amendments raise worries of censorship and executive overreach that affect Articles 19(1)(a), 21 and 14.
- Rising misinformation, deepfakes and hate speech make balanced regulation urgent for public order and election integrity.
- AI-driven moderation lacks enough transparency and accountability safeguards.
- A study is needed to suggest a legal framework that balances fundamental rights with responsible digital governance.

1.4 Objectives of the Study

1. To understand what Article 19(1)(a) says about free speech and how it applies to social media in India.
2. To examine how government regulation of social media affects privacy (Article 21) and equality (Article 14).
3. To find gaps in current law on new problems such as deepfakes, fake bots and AI-based content moderation.
4. To understand how people actually feel about online content regulation, using survey data.
5. To suggest a better legal framework that protects people's rights while still letting the Government deal with real online threats.

WHITE BLACK LEGAL

1.5 Research Questions

1. How far does Article 19(1)(a), read with Article 19(2), protect speech on social media, and what limits does the Constitution allow?
2. Do the present powers of blocking, interception, traceability and takedown meet the tests of Articles 14, 19 and 21?
3. What can India learn from the United States, the European Union and the United Kingdom?
4. What do members of the public think about regulation, privacy and independent oversight?

1.6 Scope and Limitations

The paper is limited to India's constitutional and statutory framework for social media, with a comparison of the United States, the European Union and the United Kingdom. It does not go into the regulation of digital news publishers and streaming services in detail. The survey is small and was answered mostly by young people, so it is used only to give a sense of public opinion, not to prove any claim. Several important questions are still before the courts, and the law is stated here as it stood at the time of writing.

2. RESEARCH METHODOLOGY

2.1 Non-Doctrinal Research

Non-doctrinal research studies law in its social setting. In this paper it takes the form of a public opinion survey of 50 members of the public, carried out to learn their views and experiences on social media regulation, censorship, privacy and content moderation. The questions were built around the main issues in the problem statement, such as awareness of government rules, trust in platforms, and concerns about free speech and privacy online.[5] The responses help link the legal analysis to what people really think.

The survey covered these themes:

- The respondent's age and most used social media platform.
- Exposure to fake news, misinformation and deepfakes, and whether misinformation had changed the respondent's opinion.
- Awareness of government rules that regulate social media content, such as the IT Rules,

[5] The survey percentages are reported exactly as generated by the survey tool used by the research team. The respondents are a convenience sample and the results are not statistically representative of India.

2021.

- Views on government control versus platform self-regulation, and on the best way to control fake news and hate speech.
- Views on tracing the origin of messages for national security, even if it reduces privacy.
- Views on whether an independent body should decide what content is fake or harmful.

2.2 Comparative Method

The comparative method looks at how other countries handle the same issue and sets their approach beside India's. It shows the gaps in Indian law and points to practical solutions that already work elsewhere, which strengthens the case for reform. This paper compares India with the United States, the European Union and the United Kingdom on three questions: is there independent oversight, is there a duty of transparency, and can users appeal?

2.3 Sources

Primary sources are the Constitution of India, the Information Technology Act, 2000, the rules made under it, and judgments of the Supreme Court and High Courts. Secondary sources include textbooks on constitutional law and information technology law, online legal databases and commentary. Recent developments were checked against reported court orders and official notifications.

3. THE CONSTITUTIONAL FRAMEWORK

3.1 About Constitutional Law in the Digital Space

Constitutional law sets out the rights citizens hold against the State. It decides how far free speech, privacy and equality go, and how far the Government may limit them. For social media, four provisions matter most: Article 19(1)(a) (freedom of speech and expression), Article 19(2) (reasonable restrictions), Article 21 (right to privacy) and Article 14 (equality and protection from arbitrary State action).

3.2 Article 19(1)(a): Freedom of Speech and Expression

Article 19(1)(a) protects the right to express opinions and also the right to circulate and receive information. The Supreme Court has long held that freedom includes freedom of circulation, because speech that cannot reach anyone has little value.[6] In *Anuradha Bhasin*, the Court held

[6] Romesh Thappar v. State of Madras, AIR 1950 SC 124; Sakal Papers (P) Ltd. v. Union of India, AIR 1962 SC

that speech and expression through the internet is protected by Article 19(1)(a).[7]

In *Shreya Singhal*, the Court drew a key line between discussion, advocacy and incitement. Mere discussion or even advocacy of an unpopular cause lies at the heart of free speech. Only when speech turns into incitement can the State restrict it.[8] This line is very useful for social media, where sharp criticism of public figures and policies is common.

3.3 Article 19(2): Reasonable Restrictions

Free speech is not absolute. Article 19(2) lets the State make a law placing reasonable restrictions on eight grounds only.[9] Two points matter. First, the restriction must be made by law and must be reasonable. Second, the list of grounds is closed. Ideas like "fake news", "annoyance" or "offensiveness" are not on it, so a restriction on such speech has to be tied to one of the eight grounds.

The Supreme Court has also said that the link between the speech and the harm must be close and direct, like a spark in a powder keg, and not remote or based only on a fear that something might happen.[10] For hate speech, the Court has looked at the effect on the dignity and equality of the targeted group.[11]

3.4 Article 21: The Right to Privacy

In *Puttaswamy*, a nine-judge Bench of the Supreme Court held that privacy is a fundamental right under Article 21.[12] Any State interference has to pass a three-part test: (a) it must be backed by law,

(b) it must serve a legitimate aim, and (c) it must be proportionate to that aim, with safeguards against abuse. Even earlier, the Court had set safeguards for phone tapping in *PUCL*.[13]

These principles apply directly to interception, monitoring and tracing of messages online. They also bring up the unresolved clash between traceability and encryption, discussed in Chapter 6.

305.

[7] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.

[8] Shreya Singhal v. Union of India, (2015) 5 SCC 1.

[9] Constitution of India, 1950, art. 19(2). The grounds are: sovereignty and integrity of India, security of the State, friendly relations with foreign States, public order, decency or morality, contempt of court, defamation, and incitement to an offence.

[10] S. Rangarajan v. P. Jagjivan Ram, (1989) 2 SCC 574 (the link between the speech and the harm must be proximate and direct, not remote or fanciful).

[11] See also Amish Devgan v. Union of India, (2021) 1 SCC 1, which discusses hate speech and its effect on the dignity and equality of the targeted group.

[12] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

[13] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301 (safeguards for telephone tapping).

3.5 Article 14: Equality and Non-Arbitrariness

Article 14 forbids arbitrary State action. In *Royappa* and *Maneka Gandhi*, the Court held that arbitrariness is the opposite of equality, and that any procedure that takes away a right must be fair, just and reasonable.[14] For social media, this means blocking or takedown orders should rest on clear standards, give reasons and be open to challenge.

One clarification is needed. Article 14 binds the State, not private companies. The doctrine of arbitrariness can therefore be applied directly to government orders and to the State's own use of automated tools. To place similar fairness duties on the algorithmic decisions of private platforms, a statute would be needed.

3.6 Prior Restraint, Chilling Effect and Proportionality

Three ideas from constitutional case law matter especially for social media.

The first is **prior restraint**, which means stopping speech before it is published or before a court has found it unlawful. Indian courts have viewed this with great suspicion since *Romesh Thappar*, because it stops the public from ever hearing the speech. Blocking and pre-emptive takedown of online content work in much the same way, so they need strong safeguards.

The second is the **chilling effect**. When a law is vague or the penalty is heavy, people stop speaking even on lawful matters out of fear of punishment. This was the main reason for striking down section 66A and, later, the Fact Check Unit rule. The same worry arises when platforms face very short deadlines and the loss of safe harbour, because they may remove content without much thought just to avoid risk.

The third is **proportionality**. A restriction on a fundamental right must have a legitimate aim, must be suitable for achieving that aim, must be necessary because no less intrusive method is available, and must strike a fair balance between the right and the aim. This test, applied in *Puttaswamy* and *Anuradha Bhasin*, gives courts a workable way to examine each new regulatory tool, from traceability to automated removal.

3.7 Constitutional Gaps and Improvements Needed

Table 1 sets out the main gaps in the constitutional position and the improvements needed.

Table 1: Constitutional gaps and improvements

Provision	Limitation	Improvement needed
Art. 19(1)(a)	No clear digital-age test for deepfakes or	A clear judicial standard for

[14] E.P. Royappa v. State of Tamil Nadu, (1974) 4 SCC 3; Maneka Gandhi v. Union of India, (1978) 1 SCC 248.

	coordinated bot disinformation.	synthetic and coordinated content.
Art. 19(2)	No settled constitutional standard for procedural safeguards before restrictions.	Mandatory independent oversight before restriction.
Art. 21	The tension between traceability and encryption is unresolved.	An encryption-compatible privacy test.
Art. 14	No transparency requirement; the public is not told how many blocking or interception orders are issued or on what grounds.	Extend the arbitrariness doctrine to State use of algorithmic decisions and require transparency.

4. THE STATUTORY FRAMEWORK

4.1 The Information Technology Act, 2000

The Information Technology Act, 2000 is India's main law for cyberspace. It gives legal recognition to electronic records and digital signatures, and separately deals with cybercrime and unlawful online content.[15] It was amended significantly in 2008 to widen the cybercrime provisions and to add government powers over intermediaries and online content. That is why the 2008 version is the one most relevant to today's social media issues.

4.2 Section 69: Interception, Monitoring and Decryption

Section 69 lets the Central or a State Government direct any agency to intercept, monitor or decrypt information in any computer resource, when it is necessary or expedient on grounds such as the sovereignty and integrity of India, security of the State, public order or investigation of an offence.[16] The orders are issued by the executive and reviewed by a committee of executive officials. There is no prior judicial check.

4.3 Section 69A: Blocking of Public Access

Section 69A allows the Government to direct an intermediary to block public access to online information on grounds such as sovereignty, defence, security of the State, friendly relations with foreign States and public order. Reasons must be recorded in writing, and the Blocking Rules, 2009 set up a committee process.[17] The Supreme Court upheld the section in *Shreya*

[15] Information Technology Act, 2000 (Act 21 of 2000), as amended by the Information Technology (Amendment) Act, 2008.
[16] Information Technology Act, 2000, s. 69; Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.
[17] Information Technology Act, 2000, s. 69A; Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.

Singhal because of these safeguards. But the rules require blocking requests and actions to be kept confidential. So the public cannot see how many orders are passed or why, and the affected user may not even know what was blocked, let alone get a real chance to defend the content.

4.4 Section 79: Safe Harbour for Intermediaries

Section 79 gives intermediaries a conditional safe harbour. An intermediary is not liable for third-party content if it acts as a passive conduit, does not start or select the content, and follows due diligence.[18] The protection is lost if the intermediary helps in the unlawful act, or if it fails to remove the content quickly after getting actual knowledge. In *Shreya Singhal*, the Court read down this provision and held that "actual knowledge" means a court order or a notification by the appropriate government agency. The law does not clearly explain what "due diligence" means, so platforms follow different practices.

4.5 Section 66A: Struck Down

Section 66A punished sending "menacing" or "grossly offensive" online messages with up to three years in prison and a fine.[19] In 2015 the Supreme Court struck it down as vague and overbroad, holding that it violated Article 19(1)(a) and was not saved by Article 19(2). The judgment remains the strongest constitutional statement against vague online speech laws.

4.6 The IT Rules, 2021 and Later Amendments

The IT Rules, 2021 put due diligence duties on intermediaries, and extra duties on significant social media intermediaries, meaning those with more than 50 lakh registered users.[20] The main features are:

- A grievance redressal system, and a Grievance Appellate Committee created by the 2022 amendment.[21]
- A duty on significant messaging services to enable identification of the first originator of a message, but only under a judicial order or a competent authority's order under section 69, and only for serious offences.[22]

[18] Information Technology Act, 2000, s. 79.
[19] Information Technology Act, 2000, s. 66A (struck down in Shreya Singhal v. Union of India, (2015) 5 SCC 1).
[20] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), dated 25 February 2021. A significant social media intermediary is one with more than 50 lakh registered users in India.
[21] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2022, which inserted r. 3A (Grievance Appellate Committee).
[22] IT Rules, 2021, r. 4(2).

- A duty to make efforts to use automated tools to find certain categories of content, such as child sexual abuse material, and a duty to notify users before removing content and give them a chance to dispute the action.

In 2023, an amendment allowed a government Fact Check Unit to identify "fake, false or misleading" content about the Government's business. The Bombay High Court struck this down in 2024 as vague and as creating a chilling effect on free speech.[23] The Supreme Court has agreed to hear the Union's appeal.

In February 2026, further amendments came into force. They bring "synthetically generated information", including deepfakes, within the rules. Platforms must label such content and embed provenance information where technically possible, and the time to remove flagged unlawful content was cut sharply, to as little as three hours in some cases.[24] This is an important step towards handling AI-generated content. However, it was done through subordinate rules and not by Parliament, and critics warn that very short deadlines may push platforms to remove lawful content just to be safe.

4.7 Related Laws

Harmful speech online can also be punished under the Bharatiya Nyaya Sanhita, 2023, which covers offences such as promoting enmity, outraging religious feelings, statements causing public mischief, and defamation.[25] The Digital Personal Data Protection Act, 2023 deals with the processing of personal data and matters for how platforms and the Government handle user data.[26]

4.8 Limitations of the Present Framework

- **Sections 69 and 69A:** The Government can order interception or blocking on its own decision. No court or independent body checks the order before it takes effect.
- **Section 69A:** Blocking orders are confidential. People do not know how many orders are passed or why, and the affected person cannot easily defend the content.
- **Section 79:** The law asks for "due diligence" but does not define it clearly, so

[23] Kunal Kamra v. Union of India, Bombay High Court (tie-breaker opinion of Chandurkar J. dated 20 September 2024; final order dated 26 September 2024). The Union's appeal is before the Supreme Court, which issued notice in March 2026 but did not stay the High Court's order.
[24] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E), notified 10 February 2026 and in force from 20 February 2026.
[25] Bharatiya Nyaya Sanhita, 2023, including s. 196 (promoting enmity between groups), s. 299 (deliberate acts intended to outrage religious feelings), s. 353 (statements conducing to public mischief) and s. 356 (defamation).
[26] Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

platforms follow different rules.

- **No way to fight back:** If content is blocked, there is no clear and easy way for the user to ask why or to appeal, apart from going to court through a writ petition.
- **Old law, new problems:** The Act was written before deepfakes and AI-generated content. The parent Act says nothing about them, and the gap is being filled only by delegated rules.

4.9 Improvements Needed

Table 2: Key provisions of the IT Act and improvements needed

Section	What it does	Improvement needed
s. 69	Power to intercept, monitor or decrypt information.	Independent authority or court to check orders before they take effect.
s. 69A	Power to block public access to content on stated grounds.	Publish basic details of orders and reasons; give users notice and a chance to appeal.
s. 79	Conditional safe harbour for intermediaries.	Clearly define what "due diligence" means.
s. 66A	Struck down in 2015.	Any new law on online speech must avoid vagueness.
Whole Act	Written before AI and deepfakes.	Update the law by legislation to cover AI moderation and deepfakes clearly.

4.10 Duties and Uncertainty of Platforms

Platforms are not passive in this system. They get orders from many authorities, have to decide quickly whether content is unlawful, and risk losing safe harbour if they decide wrongly or too slowly. At the same time, their own moderation choices can silence lawful speakers. Three uncertainties stand out. First, the line between a takedown notice under section 79(3)(b) and a blocking order under section 69A is disputed, as the X Corp case shows. Second, platforms are unsure how far they must use automated tools without violating user rights. Third, platforms must follow data protection duties while also giving information to investigating agencies. A clear statute would help platforms, the Government and users alike.

5. JUDICIAL APPROACH: KEY CASE LAWS

5.1 Shreya Singhal v. Union of India (2015): Free Speech

The petitioners challenged section 66A and other provisions of the IT Act. The Supreme Court struck down section 66A, read down section 79(3)(b), and upheld section 69A along with its procedural safeguards. The Court held that internet speech is protected by Article 19(1)(a) and that vague laws have a chilling effect. The case is still the foundation of online speech law in India.

5.2 K.S. Puttaswamy v. Union of India (2017): Privacy

The Court held that privacy is a fundamental right and set out the test of legality, legitimate aim and proportionality. For social media regulation, this means surveillance, data collection and tracing of messages must be justified on these grounds and come with safeguards.

5.3 Anuradha Bhasin v. Union of India (2020): Internet Access and Proportionality

The case arose from the internet shutdown in Jammu and Kashmir. The Court held that freedom of speech and expression through the internet, and the freedom to carry on trade or business over it, are protected. Restrictions must be proportionate and open to judicial review, and orders restricting the internet must be published so they can be challenged.[27] This supports the argument for transparency in blocking orders.

5.4 Maneka Gandhi v. Union of India (1978): Arbitrariness

The Court held that Articles 14, 19 and 21 are linked, and that a law taking away a right must follow a procedure that is fair, just and reasonable, not arbitrary. This is the source of the argument that unguided executive power to block content violates Article 14.

5.5 Recent Developments: Kunal Kamra and X Corp

In *Kunal Kamra*, discussed above, the Bombay High Court struck down the Fact Check Unit rule as vague, and because it let the Government decide what is true about its own work. In *X Corp v. Union of India*, the Karnataka High Court upheld the Sahyog portal, a government platform through which authorised agencies send takedown notices to intermediaries under section 79(3)(b) and rule 3(1)(d).[28] The Court also held that a foreign company cannot claim

[27] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 (orders restricting the internet must be published and are open to judicial review).
[28] X Corp v. Union of India, W.P. No. 7405 of 2025, Karnataka High Court, judgment dated 24 September 2025.

rights under Article 19. Critics argue that this creates a parallel blocking route without the safeguards of section 69A. The matter is under appeal, and it shows that the boundary between takedown and blocking is still unsettled.

5.6 Principles Drawn from the Case Law

Table 3 gathers the main principles from these decisions and shows how each applies to social media regulation.

Table 3: Principles from key decisions

Case	Principle	Use for social media
Shreya Singhal (2015)	Vague criminal laws on speech are invalid; discussion and advocacy are protected; blocking is valid only with safeguards.	Any new online speech offence must be precise; blocking must follow a reasoned procedure.
Puttaswamy (2017)	Privacy is a fundamental right; legality, legitimate aim and proportionality are required.	Test for traceability, monitoring and data sharing.
Anuradha Bhasin (2020)	Restrictions on the internet must be proportionate, reasoned, published and reviewable.	Supports transparency of blocking orders.
Maneka Gandhi (1978)	Procedure affecting rights must be fair, just and reasonable, not arbitrary.	Tests unguided executive power to block or take down.
Rangarajan (1989)	Speech can be curbed only where it has a close and direct link to the harm.	Guards against removal based on remote fears.

6. EMERGING CHALLENGES

6.1 Misinformation and Fake News

False content spreads fast on social media, especially in closed messaging groups. The difficulty for the law is that "fake news" is not a ground under Article 19(2). A law that punishes falsehood as such is likely to be attacked as vague, as the Fact Check Unit case shows. Regulation should therefore focus on content linked to a recognised ground, such as public order or defamation, and should give the speaker a chance to respond.

An appeal by X Corp is reported to have been filed before a Division Bench.

6.2 Hate Speech and Cyberbullying

Hate speech and online harassment can badly hurt individuals and social harmony. Existing criminal law already covers many of these acts. The real issues are enforcement and speed, and making sure the response is proportionate and does not silence honest criticism.

6.3 Deepfakes and Synthetic Content

Deepfakes and AI-morphed videos can damage reputations, influence elections and enable fraud. Constitutional case law does not yet offer a clear test for such content. The 2026 amendments to the IT Rules brought in labelling and faster takedown, but the definition of synthetic content and the risk of over-removal will have to be tested in court.

6.4 Bots and Coordinated Disinformation

Fake accounts and bots can make a false message look popular. The law needs to tell apart genuine speech by many people from coordinated fake behaviour by a few. Article 19(1)(a) protects speakers who are real persons, so action against fake networks should target the coordination and the deception, not the opinion.

6.5 Traceability and Encryption

Tracing the first originator of a message is defended as necessary to detect serious crimes and threats to national security. Privacy advocates and platforms reply that it may mean breaking end-to-end encryption or collecting more data about all users. Under the *Puttaswamy* test, a measure must be necessary and proportionate, and less intrusive alternatives must be considered. The rule itself says such an order should be made only when no less intrusive means are effective. The tension is still unresolved and needs an encryption-compatible test.

6.6 AI-Based Content Moderation

Platforms increasingly use automated tools to find and remove content. These tools can make mistakes, can reflect bias in their training data, and often do not explain their decisions. The lack of transparency and of a right to human review raises due process concerns. Rules that push for very fast automatic removal can make these problems worse.

6.7 Elections, Public Order and Communal Harmony

False information on social media has caused communal tension, panic and misleading political messages in India. These are real concerns that link to public order and the integrity of

elections. The constitutional difficulty is that the same tools that stop harmful rumours can also be used against political criticism. For this reason, powers to act against election-related content should be used under clear rules, with reasons recorded, and with the possibility of review by an independent body.

7. COMPARATIVE ANALYSIS

7.1 United States

Section 230 of the Communications Decency Act protects online platforms from liability for most third-party content, and also protects their good-faith decisions to remove content.[29] The First Amendment sharply limits government control over speech. As a result, platforms are mostly self-regulated and the Government has very little control over content. People enjoy very strong free speech, but companies are not held very accountable for harmful content, and users have only a limited right to challenge moderation decisions.

7.2 European Union

The Digital Services Act requires platforms to be open about content moderation, to explain their rules clearly, to give reasons when they remove content, and to let users appeal.[30] Very large platforms must also assess and reduce systemic risks and disclose how their recommendation systems work. Independent regulators supervise compliance and can impose heavy fines. The Act does not impose a general duty to monitor all content. This makes the system fairer for users. Germany's earlier law, the NetzDG, required quick removal of clearly unlawful content, but was criticised for pushing platforms to over-remove.[31]

7.3 United Kingdom

The Online Safety Act gives an independent regulator, Ofcom, the power to oversee platform safety duties and enforce accountability.[32] Platforms must assess risks, protect children and deal with illegal content, and Ofcom can act against platforms that break the safety rules. It is a regulator-led model with independent supervision, though its transparency duties are only

[29] 47 U.S.C. § 230 (Communications Decency Act, 1996, s. 230). See also Reno v. ACLU, 521 U.S. 844 (1997), and Moody v. NetChoice, LLC, 603 U.S. 707 (2024).
[30] Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act).
[31] Netzwerkdurchsetzungsgesetz (NetzDG), 2017, whose main content-moderation duties have largely been overtaken by the Digital Services Act.
[32] Online Safety Act 2023 (United Kingdom).

partial and some critics worry about its effect on privacy and lawful speech.

7.4 Comparison with India

Table 4: Comparison of regulatory approaches (simplified)

Country	Approach	Independent oversight?	Transparency requirement?	User right to appeal?
India	Government blocks or intercepts directly (ss. 69/69A)	No	No	No
US	Platform self-regulation	No	No	Limited
EU	Transparency and accountability mandated	Yes	Yes	Yes
UK	Independent regulator (Ofcom)	Yes	Partial	Yes

The table is a simplified summary. For India, the "No" entries refer to the statutory blocking and interception scheme. They do not mean courts are unavailable, since a person can always approach the High Court or the Supreme Court by a writ petition. The 2022 Grievance Appellate Committee also gives users a route against a platform's grievance decisions, but it is a government-appointed body and not an independent regulator.

Table 5 adds more detail on the legal source, the supervising body and the consequence of non-compliance in each system.

Table 5: Legal source, supervision and enforcement

System	Main law	Who supervises	Consequence of non-compliance
India	IT Act, 2000; IT Rules, 2021 and amendments	Central Government (MeitY) and designated officers	Loss of safe harbour; penal liability of the intermediary for non-compliance with blocking orders under s. 69A
US	Section 230, Communications Decency Act	No general content regulator	Limited federal liability for third-party content; private litigation

EU	Digital Services Act	National Digital Services Coordinators and the European Commission	Fines up to 6% of global annual turnover for serious breaches
UK	Online Safety Act 2023	Ofcom (independent regulator)	Fines up to 10% of qualifying worldwide revenue or 18 million pounds, whichever is greater

7.5 Lessons for India

- **From the EU:** mandatory transparency, reasoned decisions and a user right to appeal.
- **From the UK:** an independent regulator with clear duties and enforcement powers.
- **From the US:** strong protection for speech, and a warning against giving the Government broad power over lawful content.

India's own tradition of proportionality and fair procedure fits best with a model that combines independent oversight with transparency and user remedies.

8. SURVEY ANALYSIS

8.1 Profile of Respondents

A survey was carried out among 50 members of the public.[33] Most respondents (91.7%) were between 18 and 25 years old, and Instagram was the most used platform. The findings therefore mainly reflect the views of young, frequent social media users.

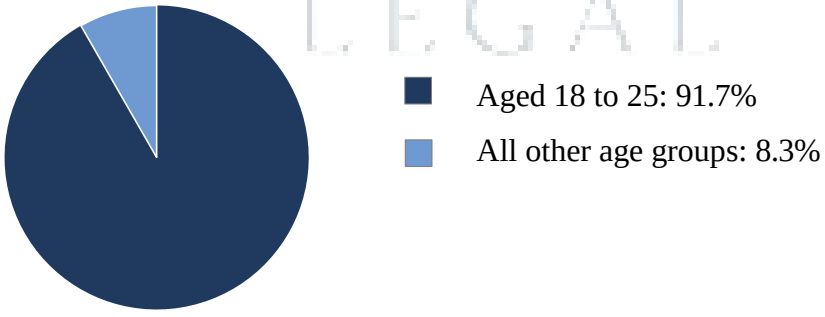


Figure 1: Age of respondents

[33] The percentages in this chapter are reported exactly as generated by the survey tool.

8.2 Exposure to Misinformation

Respondents were asked if they had ever come across fake news, misinformation or a manipulated video or deepfake on social media. Three-fourths (75%) said yes, 18.8% said maybe, and only about 6.2% said no.

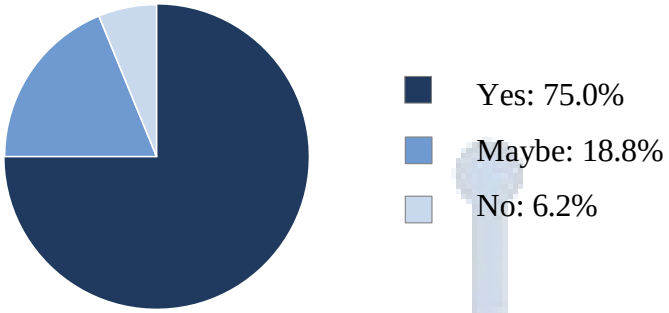


Figure 2: Have you come across fake news, misinformation or a deepfake?

When asked whether misinformation had ever affected their opinion on a political or social issue, 56.3% said yes and 31.3% said maybe, while only 12.5% said no.

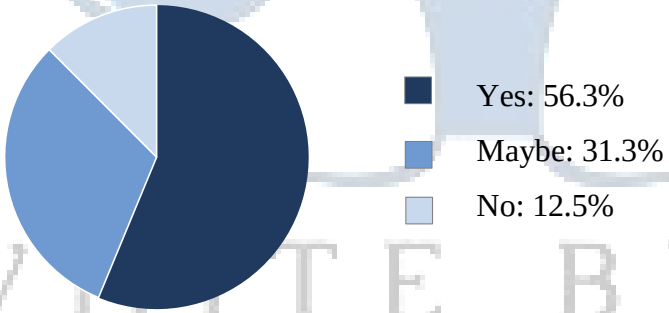


Figure 3: Has misinformation affected your opinion on a political or social issue?

So exposure to false content is common, and many people admit it has influenced them. This supports the worry that misinformation can shape political and social views.

8.3 Awareness of Government Rules

Respondents were asked if they knew of any government rules that regulate social media content in India, such as the IT Rules, 2021. Only 39.6% said yes, while 43.7% said no and 16.7% said maybe.

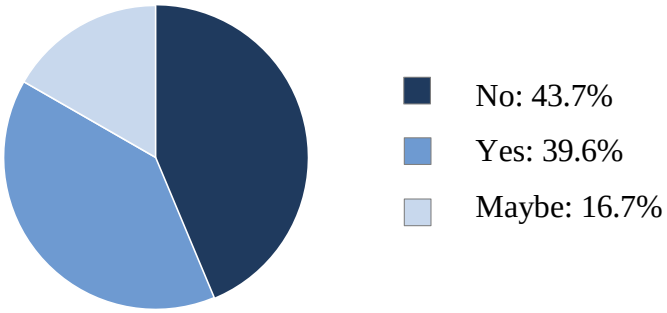


Figure 4: Awareness of government rules regulating social media content

Fewer than half the respondents knew about the rules that govern the platforms they use every day. This shows a gap in legal awareness, and supports the need for public education and for publishing information about how content rules are used.

8.4 Who Should Regulate?

On whether there should be more government control or whether platforms should regulate themselves, 41.7% preferred self-regulation by platforms, 35.4% chose both, and 22.9% chose government control.

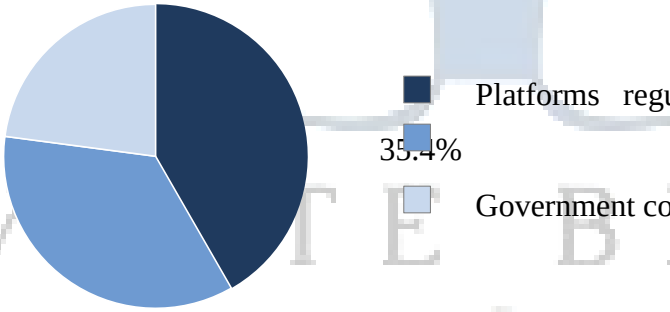


Figure 5: Government control or platform self-regulation?

Asked for the best way to control fake news and hate speech, half the respondents (50%) chose public awareness and education, 35.4% chose platform self-regulation and only 14.6% chose government regulation.

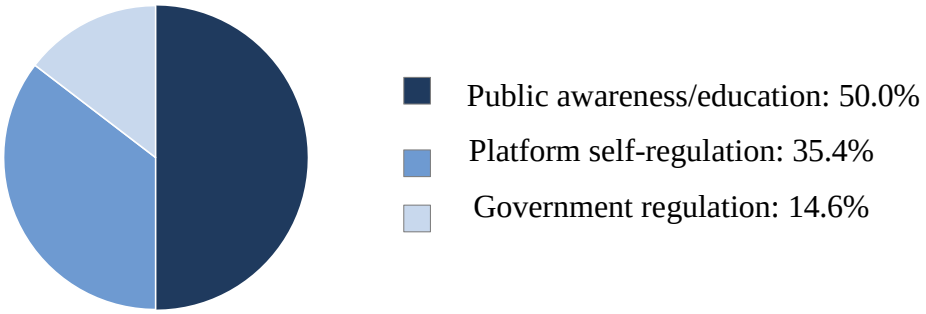


Figure 6: Best way to control fake news and hate speech online

Very few respondents saw government regulation alone as the best solution. Most preferred education or a role for platforms. This hints at low public trust in exclusive government control, though the sample is small and young.

8.5 Traceability and Privacy

Respondents were divided on whether tracking the origin of messages is necessary for national security even if it reduces privacy. A slim majority (52.1%) said yes, and 47.9% said no.

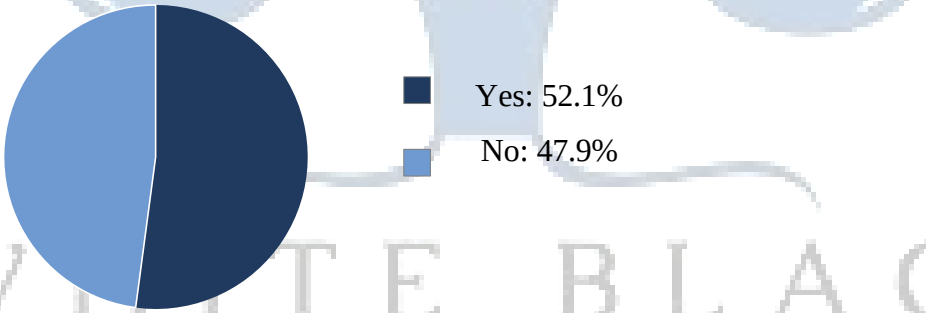


Figure 7: Is tracing the origin of messages necessary, even if it reduces privacy?

The almost even split reflects the real constitutional tension between security and privacy. It suggests that any traceability rule must be narrowly designed and protected by safeguards.

8.6 Independent Oversight

When asked whether an independent body, not directly controlled by the Government, should decide what content is "fake" or harmful, 75% said yes and 25% said no.

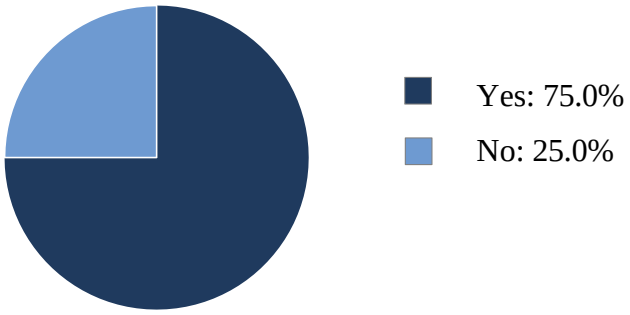


Figure 8: Should an independent body decide what content is fake or harmful?

This is the strongest result in the survey. It backs the recommendation for independent oversight of blocking and takedown decisions.

8.7 Summary and Limitations of the Survey

Table 6: Summary of survey findings

Theme	Main finding
Exposure to false content	75% have come across fake news or deepfakes; 56.3% say it affected their opinion.
Legal awareness	Only 39.6% know of government rules on social media content.
Who should regulate	41.7% prefer platform self-regulation; 22.9% prefer government control.
Best remedy	50% choose public awareness and education.
Traceability	52.1% support tracing message origin; 47.9% oppose.
Independent body	75% want an independent body to decide what is fake or harmful.

The survey has clear limits. The sample is small, it was not chosen at random, and it is dominated by respondents aged 18 to 25. The results should be read as a sign of opinion among young users, not as a measure of what all Indians think.

8.8 Linking the Survey to the Legal Analysis

The survey connects with the legal gaps found earlier in four ways. First, the high exposure to false content confirms the problem is real and that some form of regulation or education is justified. Second, the low awareness of the rules suggests that the transparency gap in the law is also felt by ordinary users, who do not know when and why content may be removed. Third, the small support for government regulation alone, and the strong support for an independent

body, match the constitutional concern that decisions on speech should not rest with the executive alone. Fourth, the divided opinion on traceability shows that privacy and security must be balanced case by case and cannot be settled by a blanket rule.

9. SOLUTION AND SUGGESTIONS

9.1 A Balanced Approach

Social media connects the world, but fake news, AI-morphed videos and online fraud are growing fast. The IT Act, 2000 no longer matches today's technology, and the parent Act does not deal with AI-generated content. Stronger laws and more public awareness are urgently needed. At the same time, equality, privacy and freedom of speech under Article 19(1)(a) must stay central. Everyone has the right to express opinions online, but reasonable restrictions on content such as vulgar or abusive material are necessary and allowed within Article 19(2).

9.2 Suggested Legal Reforms

1. **Independent check before blocking:** Require an independent authority or court to review interception and blocking orders under sections 69 and 69A before they take effect, with a fast-track procedure for real emergencies followed by review.
2. **Transparency:** Require the Government to publish basic details of how many blocking orders are issued and on what grounds, while protecting genuinely sensitive information.
3. **Clear due diligence standards:** Define what "due diligence" means for platforms under section 79, so every platform knows its duties.
4. **Notice, reasons and appeal:** Give users the right to know why their content was blocked and a chance to appeal.
5. **Legislation for AI and deepfakes:** Deal with AI-based moderation and deepfakes through a law passed by Parliament, with clear definitions, proportionate penalties and human review of automated decisions.
6. **Encryption-compatible privacy test:** Apply the *Puttaswamy* proportionality test to traceability, and prefer less intrusive methods that do not weaken encryption.
7. **Fairness in algorithmic decisions:** Extend the arbitrariness doctrine to the State's use of algorithms, and require platforms by law to give reasons and a right to appeal.

9.3 Protecting Privacy

Platforms and the Government should work together to restrict harmful content and enforce age restrictions, without freely sharing personal data with third parties. Government action should apply only in genuine cases of suspicion, and valid, transparent reasons should be given to the public whenever fundamental rights are restricted.

9.4 Shared Responsibility and Digital Literacy

The Government and the public share responsibility. The law must be strengthened to match technology, while citizens, from a young age, must also be aware of the content they consume. The survey shows that half the respondents see public awareness and education as the best remedy. Media literacy in schools and colleges, public fact-checking by independent organisations and clear labelling of synthetic content can reduce harm without giving the State broad power over speech.

9.5 Anticipating Objections

Several objections can be expected. The Government may say that prior independent review will slow action against urgent threats such as incitement to violence or child abuse material. This can be met by allowing immediate interim action in real emergencies, followed by prompt review within a fixed time. Platforms may say that transparency and appeal rights will raise their costs. The answer is that these duties can be scaled to the size and reach of the platform, as the IT Rules already separate out significant social media intermediaries. Others may worry that an independent body could itself turn political. That risk is reduced by fixed tenure, open appointment, published reasons and the availability of judicial review.

9.6 Summary of Proposed Reforms

Table 7 links each problem to a reform and its constitutional basis.

Table 7: Problems, reforms and constitutional basis

Problem	Suggested reform	Constitutional basis
Blocking and interception without prior independent check	Independent authority or court review before orders take effect.	Art. 14 and Art. 19(2): fair procedure; Maneka Gandhi.
Secret blocking orders	Publish statistics and grounds; notice and appeal for users.	Art. 19(1)(a): Anuradha Bhasin (orders to be

		published).
Undefined platform duties	Statutory definition of due diligence.	Art. 14: clarity and non-arbitrariness.
Deepfakes and AI content	Parliamentary law with clear definitions and human review.	Art. 19(2): restriction must be by law and proportionate.
Traceability versus encryption	Narrow, less intrusive, encryption-compatible method.	Art. 21: Puttaswamy proportionality.
Low public awareness	Digital literacy programmes and public reporting.	Informed exercise of Art. 19(1)(a).

10. CONCLUSION

Millions of Indians use social media to exercise their freedom of speech. Yet the current laws, the IT Act, 2000 and the IT Rules, 2021 with their amendments, lack independent oversight, enough transparency and settled rules for AI-based content moderation. The Supreme Court has given strong principles in *Shreya Singhal*, *Puttaswamy*, *Anuradha Bhasin* and *Maneka Gandhi*, but these are not yet fully reflected in the statutory scheme.

Fixing this would protect free speech and privacy, build public trust, give users a fair right to appeal and help control misinformation that threatens public order and elections. The key improvements are independent checks before content is blocked, transparency in blocking orders, clear rules for platforms, user appeal rights and fair standards for AI moderation. The comparison with the European Union and the United Kingdom shows that such a system is workable, and the survey shows that the public supports independent oversight.

Further research could study the pending appeals, how the 2026 synthetic-content rules work in practice, and larger surveys across age groups.

The aim should be a system that protects both individual rights and public safety. Regulation of online speech is legitimate only if it is clear, proportionate, transparent and open to challenge.

END NOTES AND REFERENCES

Detailed citations appear in the notes at the end of each chapter. The sources relied upon are listed below.

A. Constitution, Statutes and Rules

1. Constitution of India, 1950, arts. 14, 19(1)(a), 19(2) and 21.

2. Information Technology Act, 2000 (Act 21 of 2000), as amended in 2008, ss. 66A, 69, 69A and 79.
3. Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.
4. Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.
5. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), 25 February 2021, and Amendment Rules of 2022, 2023 and 2026 (G.S.R. 120(E), 10 February 2026).
6. Bharatiya Nyaya Sanhita, 2023.
7. Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

B. Indian Cases

1. Romesh Thappar v. State of Madras, AIR 1950 SC 124.
2. Sakal Papers (P) Ltd. v. Union of India, AIR 1962 SC 305.
3. E.P. Royappa v. State of Tamil Nadu, (1974) 4 SCC 3.
4. Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
5. S. Rangarajan v. P. Jagjivan Ram, (1989) 2 SCC 574.
6. People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.
7. Shreya Singhal v. Union of India, (2015) 5 SCC 1.
8. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
9. Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.
10. Amish Devgan v. Union of India, (2021) 1 SCC 1.
11. Kunal Kamra v. Union of India, Bombay High Court, 2024 (appeal pending before the Supreme Court).
12. X Corp v. Union of India, W.P. No. 7405 of 2025, Karnataka High Court, 24 September 2025.

C. Foreign and International Sources

1. 47 U.S.C. § 230 (Communications Decency Act).
2. Reno v. ACLU, 521 U.S. 844 (1997); Moody v. NetChoice, LLC, 603 U.S. 707 (2024).
3. Regulation (EU) 2022/2065 (Digital Services Act).
4. Online Safety Act 2023 (United Kingdom).
5. Netzwerkdurchsetzungsgesetz (NetzDG), Germany, 2017.
6. World Economic Forum, Global Risks Report 2024.

WHITE BLACK LEGAL

D. Books and Online Sources

1. Dr. J.N. Pandey, Constitutional Law of India.
2. Vakul Sharma, The Information Technology Act, 2000: A Handbook.
3. SCC Online, scconline.com.
4. Indian Kanoon, indiankanoon.org.
5. Bare Acts: The Constitution of India, 1950; The Information Technology Act, 2000.

WHITE BLACK
LEGAL