



LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

[ISSN: 2583-7753]

Volume 4 | Issue 2

2026

DOI: <https://doi.org/10.70183/lijdlr.2026.v04.255>

© 2026 LawFoyer International Journal of Doctrinal Legal Research

Follow this and additional research works at: www.lijdlr.com

Under the Platform of LawFoyer – www.lawfoyer.in

After careful consideration, the editorial board of LawFoyer International Journal of Doctrinal Legal Research has decided to publish this submission as part of the publication.

In case of any suggestions or complaints, kindly contact (info.lijdlr@gmail.com)

To submit your Manuscript for Publication in the LawFoyer International Journal of Doctrinal Legal Research, To submit your Manuscript [Click here](#)

ENCRYPTED BUT NOT FREE: STATE SURVEILLANCE, SECTION 69 IT ACT, AND THE FUTURE OF DIGITAL PRIVACY IN INDIA

Arush Kalsotra¹

I. ABSTRACT

This paper examines the expansion of State surveillance and digital censorship in India through the statutory architecture of the Information Technology Act, 2000, particularly Sections 69, 69A and 79(3)(b), and tests that architecture against the constitutional standards of privacy, proportionality, free speech and chilling effect. Adopting a doctrinal and case-study-based methodology, it analyses primary legal materials, including the IT Act, the 2009 Interception Rules, the Digital Personal Data Protection Act, 2023, and leading decisions such as Shreya Singhal, Puttaswamy, Anuradha Bhasin and the Kunal Kamra litigation. The paper argues that safeguards which justified executive blocking and interception powers in constitutional doctrine have weakened in practice because surveillance and takedown decisions remain largely executive-controlled, opaque and difficult to challenge. The analysis studies specific episodes to demonstrate this pattern: the 2018 authorisation of ten agencies to intercept, monitor and decrypt digital communications; the Sahyog Portal's use of Section 79(3)(b) to route takedown demands outside the procedural discipline of Section 69A; the litigation concerning the government Fact Checking Unit in Kunal Kamra; the proposed Karnataka misinformation framework; and the rollback of end-to-end encryption on Instagram. These examples show how broad statutory language, short compliance windows, absence of judicial oversight and platform dependence can cumulatively chill protected speech and weaken informational privacy. The paper concludes by proposing targeted reforms: prior or prompt judicial scrutiny for Section 69 orders, auditable retention of interception records, restoration of Section 69A-style notice and reasoned-order

¹ B.A. LLB (H), 6th Semester, Student at Himachal Pradesh National Law University, Shimla (India).
Email: arushkalsotra@gmail.com

safeguards for takedowns, constitutionally narrow misinformation regulation, meaningful consent for encryption rollbacks, and a national encryption policy grounded in Article 21.

II. KEYWORDS

Section 69 IT Act, Digital Surveillance, Chilling Effect, Sahyog Portal, and Proportionality.

III. INTRODUCTION AND RESEARCH PROBLEM

हो गई है पीर पर्वत-सी पिघलनी चाहिए, इस हिमालय से कोई गंगा निकलनी चाहिए।²

The pain has become as big as a mountain; a Ganga must come from this Himalaya. Dushyant Kumar has written the lines during the Emergency. He was talking about how a country is born when you don't allow any dissent in it, and begin to eat it. It has been 50 years since the time of Emergency and Indian suppression has been modernized, computerised, re-legalised.

A short satirical video posted on Instagram ridiculed the actions of the Prime Minister during a diplomatic gathering in March, 2026. Millions watched it, the video was taken down quickly by Meta, following a legal notice from the Government of India, which has taken it offline in just a couple of days. Only a private explanation was provided, a hearing was not held. At the same time, dozens of accounts on X, primarily by political satirists and anonymous critics of the ruling party were banned without warning. A political cartoon led to the shut-down of a news web site off the Internet. Those posts that referenced an Election Commission document were removed. But in each case, it was the same: an order from the government, an intermediary that was ready to obey, and no one spoke.

All of this is not new and none is unintentional. The Information Technology Act, 2000, together with the various rules framed for its implementation and the executive order issued in compliance with the Act, has created a regulatory framework for the censorship of online speech with little or no public notice, at a whim, and without accountability. This paper does

² Dushyant Kumar, *Ho Gayi Hai Peer Parvat-Si Pighalni Chahiye*, Kaavyaalaya, <https://kaavyaalaya.org/dush1>

not ask the question of whether or not the individual takedown was legal, many were probably not. Is there a constitutional basis for the retention of the legal structure which produces them?

It has seen a comedian, who is simultaneously facing two sets of challenges a court order and a government for his stand-up routine. It has witnessed intelligence agencies asking Bollywood actors to appear in its offices for questioning through the WhatsApp and also saw a police investigation getting shelved and handed over to the Supreme Court appointed committee who were under pressure due to media. And it is now keeping an eye on a state government's proposal to put social media users in jail for up to seven years for a misposted tweet. All the above are considered seriously in this paper as they are correlated to each other. The question of the lack of judicial oversight and MHA order of 2018 is discussed and Section 69 and the surveillance regime set in place is analysed.

A. Research Objectives

This paper seeks:

1. to examine the statutory architecture of Section 69 and Section 69A of the Information Technology Act, 2000 and the procedural safeguards that govern their exercise;
2. to trace how executive practice under this architecture has departed from the constitutional standards laid down in *Shreya Singhal v. Union of India* and *Puttaswamy*;
3. to evaluate specific instances of surveillance and takedown, Section 66A prosecutions, the Pegasus controversy, the Sushant Singh Rajput investigation, the Sahyog Portal, the Kunal Kamra litigation, the Karnataka Fake News Bill, and the removal of end-to-end encryption on Instagram as evidence of a wider pattern; and
4. to propose reforms consistent with the proportionality and chilling-effect doctrines developed by Indian courts.

B. Research Question

1. First, does the procedural framework under Section 69 of the IT Act, 2000 and the 2009 Interception Rules satisfy the necessity and proportionality requirements laid down in Puttaswamy?
2. Second, has the removal of the safeguards attached to Section 69A: a reasoned order, a designated committee, and notice to the originator through the use of Section 79(3)(b) and the Sahyog Portal eroded the constitutional basis on which Section 69A was upheld in Shreya Singhal?
3. Third, what does the pattern of enforcement examined in this paper reveal about the gap between the stated safeguards and their practical operation?
4. Fourth, what legislative and institutional reforms would bring India's surveillance and takedown framework into conformity with Articles 14, 19 and 21 of the Constitution.

C. Research Hypotheses

This paper proceeds on three hypotheses. First, that the procedural safeguards attached to Section 69 and Section 69A exist largely on paper and are not, in practice, enforced with the rigour that their constitutional justification requires. Second, that executive authorities have progressively routed content-related and surveillance decisions through mechanisms such as Section 79(3)(b) and the Sahyog Portal precisely because these mechanisms carry fewer procedural constraints than Section 69A itself. Third, that the cumulative effect of these mechanisms, read together rather than as isolated incidents, amounts to a chilling effect on protected speech disproportionate to the interests the framework is meant to serve.

D. Research Methodology

This paper adopts a doctrinal and analytical methodology. It draws on primary legal sources, the Information Technology Act, 2000, the Information Technology (Procedure and

Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, the Digital Personal Data Protection Act, 2023, the Karnataka Misinformation and Fake News (Prohibition) Bill, 2025, and the constitutional text together with judicial decisions including *Shreya Singhal v. Union of India*, *Puttaswamy*, *Anuradha Bhasin v. Union of India*, *Mohammed Zubair v. State of U.P.*, and the Kunal Kamra litigation before the Bombay High Court. It supplements this doctrinal analysis with case studies of specific episodes of surveillance and takedown, drawn from government orders, court records, and reporting by civil society organisations such as the Software Freedom Law Centre, the Internet Freedom Foundation, and the Vidhi Centre for Legal Policy, in order to test how the statutory framework operates in practice rather than only as written.

E. Literature Review

The constitutional foundation for this paper's analysis lies in the nine-judge Bench decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, which recognised the right to privacy as a fundamental right protected under Part III of the Constitution and located informational privacy within the broader values of dignity, autonomy and liberty.³ The decision also supplies the proportionality framework applied throughout this paper, requiring State intrusions into privacy to satisfy legality, a legitimate State aim, rational nexus, necessity and proportionality. *Shreya Singhal v. Union of India* remains the leading authority on intermediary liability and the procedural conditions attached to Section 69A, and its reasoning is the benchmark against which the Sahyog Portal and the Fact Checking Unit are evaluated here.

The chilling effect doctrine, developed in *Anuradha Bhasin v. Union of India* and extended in *Mohammed Zubair v. State of U.P.* and in the Bombay High Court's split verdict in *Kunal Kamra v. Union of India*, supplies the analytical lens through which this paper reads the cumulative impact of the episodes it examines. Reports by the Software Freedom Law Centre, the Internet Freedom Foundation, the Vidhi Centre for Legal Policy, and the Oxford

³ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

Human Rights Hub document the practical operation of the interception and takedown regime and are relied on to move the analysis beyond the bare text of the statute. Gautam Bhatia's work on free speech under the Indian Constitution informs the paper's treatment of vagueness and chilling effect as constitutionally cognisable harms in themselves.

IV. RESEARCH AND ANALYSIS

The analysis below is organised issue-wise, tracing the surveillance and censorship architecture from its statutory source in Section 69 through its extension via the Sahyog Portal and the Fact Checking Unit, instances of documented misuse, the Karnataka Fake News Bill, and the rollback of encryption on Instagram, before turning to the constitutional doctrine that ties these episodes together.

A. Section 69 IT Act: The Architecture of Surveillance

1. What the Provision Actually Says

Section 69 of the Information Technology Act, 2000 gives the Central or State Government or any officer specially authorised by them the power to direct any government agency to intercept, monitor, or decrypt any information generated, transmitted, received, or stored in any computer resource.⁴ The grounds on which this can be done are: sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign states, public order, prevention of the incitement of any cognisable offence, and crucially investigation of any offence.

That last ground is worth pausing on. The Indian Telegraph Act, 1885, which governed telephone tapping before the digital era, listed only five grounds for interception, and did not include the investigation of offences as a standalone basis. Section 69 adds it. On its face this seems reasonable of course agencies investigating crimes should be able to access relevant digital communications. But the practical effect is that every single criminal investigation in the country is potentially a basis for electronic surveillance. The provision

⁴Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India), § 69.

does not limit this to serious offences or those punishable above a particular threshold. Any cognisable offence will have the consequences.

B. The Procedural Safeguards and Their Limits

The provision requires reasons to be recorded in writing before any direction for interception is issued, and mandates that a procedure prescribed under sub-section (2) be followed. The 2009 Interception Rules enacted under this sub-section require the competent authority to obtain prior approval from the Ministry of Home Affairs (for the Central Government) or the Home Secretary of the State, prescribe a maximum validity of 60 days per order, and establish a review committee that is supposed to meet every two months.⁵

The problem is that these safeguards exist almost entirely on paper. The Software Freedom Law Centre has documented that RTI applications seeking data on how many interception orders have been issued each year have been uniformly denied because the 2009 Rules themselves require that records of interception be destroyed within 180 days.⁶ There is no way for citizens, courts, or even Parliament to know how many Indians are under surveillance at any given time, which agencies are doing the surveilling, or whether the Review Committee has ever actually rejected a single order. The secrecy is not incidental to the system. It is built into the system.

Equally significant is the absence of any judicial oversight at any stage. The entire process from the initial direction through the surveillance itself to the destruction of records takes place entirely within the executive. The Review Committee that is supposed to provide oversight consists of senior government officials, including the Cabinet Secretary. These are people from the same branch of government as those issuing the orders. There is no independent scrutiny, no requirement of a warrant, no neutral magistrate.

⁵ Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, G.S.R. 780(E), Gazette of India, Extraordinary, pt. II, sec. 3(i) (Oct. 27, 2009)

⁶ Software Freedom Law Centre India, *S. 69 of the Information Technology Act and the Decryption Rules: Absence of Adequate Procedural Safeguards* (May 17, 2023).

C. The 2018 Order and Ten Agencies

On 20 December 2018, the Ministry of Home Affairs issued an order under Section 69 authorising ten central agencies to intercept, monitor, and decrypt information generated, transmitted, received, or stored in any computer resource, subject to the procedure prescribed under the applicable rules. The ten agencies named in the order were the Intelligence Bureau, Narcotics Control Bureau, Enforcement Directorate, Central Board of Direct Taxes, Directorate of Revenue Intelligence, Central Bureau of Investigation, National Investigation Agency, Cabinet Secretariat (Research and Analysis Wing), Directorate of Signal Intelligence, and Commissioner of Police, Delhi. The breadth of this authorisation is significant because it extended interception capacity beyond traditional intelligence agencies to revenue, narcotics, policing and investigative bodies. In practical terms, the order widened the institutional field through which digital surveillance could be initiated, while leaving the approval and review process substantially within the executive branch.

This was manifested in the Pegasus scandal. This manifested itself in the “Pegasus” scandal. In the case of *Manohar Lal Sharma v Union of India*, the Supreme Court set up a technical committee to look into claims that Israeli spy software was being used transparently to monitor journalists, activists, opposition politicians and judges. The government has refused to respond to the Court's specific questions regarding the purchase and use of Pegasus. The Court expressed its concern. Legend doesn't seem to have led to any legislative changes. This is the ecosystem that Section 69 works in.

D. Section 69A and the Sahyog Portal: Censorship Through the Back Door

Section 69A gives the Central Government the power to direct intermediaries to block public access to content on grounds that track Article 19(2) of the Constitution. When the Supreme Court upheld this provision in *Shreya Singhal*, the reasons it gave were specific: the provision required reasons to be recorded in writing, it created a designated committee to make decisions, and it ordinarily required 48 hours' notice to the originator of the content

before it was taken down.⁷ These safeguards, the Court said, distinguished Section 69A from the unconstitutional Section 66A. Lose the safeguards, and you lose the constitutional basis for the provision.

The government has found a way around this. By routing takedown demands through Section 79(3)(b) of the IT Act which deals with when intermediaries lose their safe harbour immunity for user content authorities compel platforms to remove content without any of the Section 69A procedural requirements.⁸ There is no designated committee. There is no reasoned order. There is certainly no notice to the content creator. When a government authority tells an intermediary that a post is 'unlawful,' the intermediary takes it down immediately rather than risk losing its safe harbour protection and that is the end of the matter for most users.

In 2024, the government centralised and formalised this mechanism through the Sahyog Portal, a unified platform connecting authorities issuing notices under Section 79(3)(b) with major social media intermediaries. X Corp. challenged this framework before the Karnataka High Court, contending that blocking or takedown directions could not be routed through Section 79(3)(b) so as to bypass the procedural safeguards of Section 69A and the Blocking Rules. The Court rejected the challenge in *X Corp. v. Union of India*, holding, inter alia, that X Corp., as a foreign corporation, could not invoke Article 19 rights, and characterising the Sahyog Portal as a cooperative mechanism between the State and intermediaries.⁹ The judicial approval of the portal, however, does not answer the deeper constitutional concern raised in this paper: that routing takedown demands through Section 79(3)(b) risks diluting the notice, reasoned-order and review safeguards that formed the basis on which Section 69A was upheld in *Shreya Singhal*.

⁷*Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (India).

⁸Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India), § 79(3)(b)..

⁹ *X Corp. v. Union of India*, W.P. No. 7405 of 2025, Karnataka High Court, decided on 24 September 2025, per M. Nagaprasanna J.

A further tightening came through the IT Amendment Rules 2026, which reduced the window for intermediaries to comply with government takedown demands from 36 hours to 3 hours. Three hours is not a window. It is a formality. No content creator can be heard, no independent review can be conducted, and no proportionality can be assessed in three hours. The executive becomes, in effect, the judge of what the public is permitted to see online.

E. The Kunal Kamra Case and the Fight Over Fact-Checking

On 6 April 2023, the Ministry of Electronics and Information Technology amended the IT Rules 2021 to create a government Fact Checking Unit (FCU) within the Press Information Bureau. The FCU was given the power to flag content relating to the 'business of the Central Government' as 'fake, false or misleading.' Once flagged, intermediaries were required to remove it or lose their safe harbour protection. Comedian and political satirist Kunal Kamra challenged this before the Bombay High Court, joined by the Editors' Guild of India and several media organisations.¹⁰

The case produced a split verdict. Justice Gautam Patel held the amendment unconstitutional vague, overbroad, lacking procedural safeguards, and creating an unmistakable chilling effect on expression. Justice Neela Gokhale upheld it. Justice A.S. Chandurkar, as the tie-breaker, agreed with Justice Patel. The amendment violated Articles 14, 19(1)(a), and 19(1)(g). Its undefined terms would push intermediaries to remove more content than any specific prohibition actually required because when the legal consequence of inaction is loss of safe harbour, no platform will take risks.

Justice Chandurkar's reasoning draws on the principle of the chilling effect as developed in *Anuradha Bhasin v. Union of India*¹¹ and *Mohammed Zubair v. State of U.P.* the government cannot be its own judge in matters of online speech, and vague laws do not merely punish

¹⁰ Kunal Kamra v. Union of India, Writ Petition (L) No. 9792 of 2023 (Bombay High Court, Jan. 31, 2024) (per Patel J.); tie-breaker opinion by Chandurkar J. (Sept. 2024).

¹¹ *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637 (India).

those convicted under them; they change the behaviour of everyone who might be.¹² The FCU was stayed by the Supreme Court and the appeal is pending.

It should be noted that the same Kunal Kamra was simultaneously facing contempt of court proceedings before the Supreme Court for social media posts about the judiciary. After prolonged hearings, the Court issued a warning but declined to penalise him, citing the need to balance judicial dignity with the fundamental right of expression. The state's regulatory machinery had reached a comedian on two fronts simultaneously for mocking the government, and for mocking the courts. The breadth of that reach is itself a data point.

V. WHEN THE LAW BECOMES A WEAPON: INSTANCES OF MISUSE

A. Section 66A

Section 66A was the main tool for suppressing digital content prior to 69. This was added in 2008 and it now makes it an offence to send a message using a computer that is grossly offensive, 'menacing' or 'annoying'. No use of the terms was a formal definition. What was inevitable, happened: arbitrary arrests, because of the political sensitivity, not harm.

On the surface, the case that sparked the fuse was an unremarkable one. In November 2012, two women in Mumbai, Shaheen Dhada and Rinu Srinivasan, were booked under Section 66A for a post on Facebook where they questioned the statewide shutdown which was called after the death of Bal Thackeray. One commented it and the other liked it. This caused furor nationwide when both were arrested and handcuffed, and subjected to criminal justice system for an expression of opinion, as any reading of PIL would indicate. Shreya Singhal, a law student, filed the PIL that eventually resulted in the complete removal of the provision by the Supreme Court.

Other instances followed the same pattern. Priyanka Sharma was sent to judicial custody for fourteen days for sharing a meme featuring the Chief Minister of West Bengal.¹³ A

¹² Mohammed Zubair v. State of U.P., (2022) SCC OnLine SC 897 (India).

¹³ Mamata Banerjee Meme Case: SC Says Arrest of Activist Was Arbitrary, [The Hindu](#) (May 15, 2019).

Puducherry businessman was arrested for a Facebook post alleging that a senior politician's son-in-law had accumulated disproportionate wealth.¹⁴ A class eleven student from Bareilly was arrested for a post critical of a state minister.¹⁵ In each instance, the offence was criticism of power. The law was the instrument, not the reason.

In 2015, Shreya Singhal struck Section 66A down as unconstitutionally vague void ab initio. What followed reveals something even more disturbing than the provision itself. Researchers found that as of 2020, at least 1,307 cases had been filed under Section 66A after the Supreme Court struck it down. It was, as one study put it, a zombie law dead, but still walking through police stations and courts, because no one thought to tell the constable on the ground that the provision no longer existed.¹⁶

B. The Sushant Singh Rajput Case: WhatsApp Chats and the Celebrity Dragnet

When actor Sushant Singh Rajput died in June 2020, the investigation that followed became one of the most dramatic illustrations of how digital surveillance powers can be deployed without any of the constitutional guardrails that are supposed to constrain them.¹⁷

The Narcotics Control Bureau one of the ten agencies authorised under the 2018 MHA order began its investigation by retrieving WhatsApp chats from Rhea Chakraborty's phone. Those chats were then shared with the CBI and formed the basis for a sprawling drug investigation that eventually drew in actors Deepika Padukone, Shraddha Kapoor, and Sara Ali Khan, among dozens of others. Rhea Chakraborty was arrested in September 2020 after days of questioning.

Several things about this case deserve scrutiny from a legal perspective. First, the mechanism by which personal WhatsApp messages became the foundation of a criminal investigation

¹⁴Bosco Dominique, *Puducherry Man Who Was Booked Under Section 66A of IT Act Hails Supreme Court Verdict*, [The Times of India](#) (Mar. 24, 2015).

¹⁵ *Class 11 Student Sent to Jail for Facebook Post Against UP Minister Azam Khan*, *Times of India* (Mar. 20, 2015, 11:38 PM IST).

¹⁶ Gauri Kashyap, *Section 66A: The Dead Law That Still Haunts India*, *Supreme Court Observer* (July 26, 2021),

¹⁷*Drug Probe Against Rhea Chakraborty Over Phone Chats*, [NDTV](#) (Aug. 26, 2020).

was never publicly explained in terms of which provision authorised the access and whether the procedural safeguards under the IT Interception Rules were followed. Second, the scale of the digital dragnet summons issued to multiple well-known individuals based on private communications raises serious questions about proportionality. Third, the public broadcast of private chat contents through what appeared to be a combination of official leaks and media cooperation transformed a criminal investigation into a national spectacle, with consequences for the reputations of people who were never charged, let alone convicted.

What the case illustrated, more than anything, is that the combination of broad interception powers under Section 69, the absence of judicial oversight, and the 2018 authorisation of multiple investigative agencies created a system in which private digital communications could be accessed, shared between agencies, and made the basis of public accusation without any of the safeguards that the right to privacy under Article 21 should require.¹⁸

VI. THE KARNATAKA FAKE NEWS BILL, 2025

In March 2025, the Government of Karnataka introduced the draft Misinformation and Fake News (Prohibition) Bill, 2025.¹⁹ Its stated purpose is to curb the spread of disinformation on social media. Its actual effect, if enacted, would be to create the most sweeping criminal speech regime in any Indian state broader than defamation law, broader than sedition, and enforced by a body whose chair is the state's own Cabinet Minister for Information.

The consequences are dire. To the extent that Section 3(2) applies, misinformation communicated will carry a maximum penalty of 5 years imprisonment for the communication of misinformation related to public health, public safety, public tranquillity or the conduct of free and fair elections. Up to seven years and 10 lakh rupees for fake news on social media is available in Section 7. To give some perspective: Defamation is punishable

¹⁸ Constitution of India, art. 21.

¹⁹Karnataka Misinformation and Fake News (Prohibition) Bill, 2025 (Draft) (India), <https://sabrangindia.in/wp-content/uploads/2025/07/Karnataka-Mis-information-and-Fakenews-Prohibition-Bill-2025-13.06.2025-.pdf>

by up to 2 years in prison under the Bharatiya Nyaya Sanhita. This Bill would bring back a carelessly forward to its value of 3 ½ times.

The definitions are where the Bill most clearly reveals its intent. 'Misinformation' covers not just false facts but also content deemed misleading, distorted, or anti-feminist, and expressions that disrespect Indian culture, religious beliefs. None of these categories are defined. An enforcement body chaired by a political appointee is left to determine, without any stated methodology, what counts as disrespectful to Sanatan symbols or prejudicial to public tranquillity.²⁰

The Vidhi Centre for Legal Policy has pointed out that the Bill restricts speech on grounds including public health and free and fair elections that do not appear in Article 19(2) of the Constitution at all.²¹ This is not a technicality. The constitutional grounds for restricting speech are exhaustively listed in Article 19(2). A law that restricts speech on additional, unenumerated grounds is not a reasonable restriction, it is an unconstitutional one.²²

The Bill also copies the structural fault that the Bombay High Court noted and decried in *Kunal Kamra* it creates a quorum in the Executive to determine what is true about the Government to say. A penal prohibition on the expression of ideas that does not explicitly state the prohibition on the expression of ideas is unconstitutional it leaves citizens in a state of unawareness of what is legal and what is not, and it gives those who have power the power to decide what's legal and what's not.²³

A journalist covering government corruption, a stand-up comedian satirising the Chief Minister, a researcher publishing finding that contradict official health policy all of them

²⁰Oxford Human Rights Hub, *Weaponizing Vagueness: The Chilling Effect of Karnataka's Fake News Bill on Free Speech and Democratic Pluralism* (July 21, 2025), <https://ohrh.law.ox.ac.uk/weaponizing-vagueness-the-chilling-effect-of-karnatakas-fake-news-bill-on-free-speech-and-democratic-pluralism/>

²¹Vidhi Centre for Legal Policy, *An Analysis of the Karnataka Fake News Bill* (Sept. 12, 2025), <https://vidhilegalpolicy.in/blog/an-analysis-of-the-karnataka-fake-news-bill/>

²²Constitution of India, 1950, arts. 14, 19(1)(a), 19(2), 21.

²³*Kartar Singh v. State of Punjab*, (1994) 3 SCC 569 (India); *Chintaman Rao v. State of Madhya Pradesh*, (1950) SCR 759 (India).

would operate under the threat of this Bill's undefined prohibitions. The result, as the Internet Freedom Foundation has noted, is a right to speak that survives in name but is rationed in practice.

VII. INSTAGRAM AND THE END OF ENCRYPTION: CONSENT, COMPLIANCE, AND THE DPDP ACT

In early 2026, Meta confirmed that end-to-end encryption (E2EE) would be removed from Instagram Direct Messages with effect from 8 May 2026.²⁴ The decision affected approximately 481 million Instagram users in India. E2EE means that message content is visible only to sender and recipient not to the platform, not to advertisers, and not to governments issuing legal process. Its removal means that all of those parties potentially gain access to what were previously private conversations.

Meta cited low adoption as the reason. Critics have pointed to the coincidence with Meta's December 2025 privacy policy update, which allows interactions with the Meta AI assistant to inform personalised advertising across platforms.²⁵ With E2EE removed, the content of Instagram DMs which previously could not be accessed even by Meta's own systems becomes part of the data environment that already serves advertising algorithms. The commercial logic is not subtle.

The legal dimension is equally significant. Meta is a data fiduciary under the Digital Personal Data Protection Act, 2023 and must ordinarily process personal data on the basis of free, specific, informed and unambiguous consent, unless another lawful basis applies. Removing end-to-end encryption is not a minor privacy-policy update; it alters the nature of the data environment itself by making the content of Instagram Direct Messages potentially accessible to the platform in a form that was previously unavailable. For Indian users, this

²⁴Internet Freedom Foundation, IFF Joins the GEC in Raising Concern on Instagram's Roll Back of Encryption Features (Apr. 13, 2026), <https://internetfreedom.in/iff-joins-the-gec-in-raising-concern-on-instagram-rollback-of-encryption-features/>

²⁵Medianama, Meta to End Instagram End-to-End Encryption for DMs (Mar. 13, 2026), <https://www.medianama.com/2026/03/223-meta-ending-instagram-dm-e2ee/>

change therefore raises questions of fresh notice, meaningful consent and purpose limitation under the DPDP framework. It also sits uneasily with the DPDP Rules, 2025, which operationalise the Act's security obligations and require data fiduciaries to maintain reasonable security safeguards for digital personal data.

The more serious constitutional concern, however, is that the DPDP Act does not merely regulate Meta's private processing of user data; it also creates a parallel route through which State access may be insulated from ordinary data-protection duties. Section 17(2) empowers the Central Government to exempt notified instrumentalities of the State from the application of the Act where processing is considered necessary in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order, or preventing incitement to cognisable offences connected with those grounds.²⁶ These grounds substantially overlap with the grounds invoked under Section 69 of the IT Act. Once end-to-end encryption is removed, therefore, the privacy risk is not confined to Meta's commercial use of message data. The same data environment may become more accessible to State agencies operating under exemption-based processing, with fewer consent, notice, purpose-limitation and user-rights constraints than would apply to ordinary private processing.

The DPDP Rules, 2025, by operationalising the Act's compliance framework, do not cure this structural concern unless exemptions under Section 17 are subjected to narrow notification, independent review, transparency and audit requirements.²⁷ In this sense, the rollback of encryption and the State-exemption architecture of the DPDP Act together illustrate the central thesis of this paper: privacy safeguards are weakened not only by direct surveillance powers, but also by overlapping statutory regimes that convert previously inaccessible communications into data capable of lawful or quasi-lawful access.

²⁶ *The Digital Personal Data Protection Act, No. 22 of 2023, § 17(2), INDIA CODE (2023).*

²⁷ *Digital Personal Data Protection Rules, 2025, Ministry of Electronics and Information Technology, notified in 2025.*

The Supreme Court's observations in the WhatsApp privacy policy litigation are instructive. When Meta's 2021 policy forced users to accept expanded data sharing or lose access, the bench questioned whether a person selling vegetables on a street could meaningfully consent to the terms of a policy she cannot read or understand.²⁸ The same question applies here, in sharper form. Instagram did not ask its Indian users whether they consented to having their private messages become accessible. It informed them, after the decision had been made, that it was happening.

For the specific communities that depend on encrypted communication to function safely—journalists, human rights defenders, political activists, members of minority communities—this rollback is not an inconvenience. It is a structural shift in the surveillance landscape. Without E2EE, DM content is obtainable by Indian authorities through legal process under Section 69 of the IT Act, through DPDP Act provisions²⁹, or through the informal pressure that the government has demonstrated it is willing to bring to bear on intermediaries. The Sushant Singh Rajput investigation, in which WhatsApp chats retrieved under surveillance powers formed the evidentiary basis for a dragnet involving dozens of individuals, is a precedent for what that access can produce.

VIII. CONSTITUTIONAL DOCTRINE: PROPORTIONALITY, CHILLING EFFECT, AND THE RIGHT TO DISSENT

In the context of restrictions on the right to privacy under Article 21, the nine-judge Bench in *Justice K.S. Puttaswamy (Retd.) v. Union of India* recognised that any State intrusion into privacy must satisfy the requirements of legality, legitimate State aim, rational nexus, necessity and proportionality between the restriction imposed and the objective pursued.³⁰ In the context of the surveillance framework under Section 69, the necessity and

²⁸ R. Venkataramanan, *What Meta's Quiet Retreat from Encryption Privacy on Instagram Means*, Telegraph India (May 15, 2026)

²⁹ The Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023).

³⁰ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

proportionality prongs remain especially vulnerable: ten agencies were authorised under the 2018 order; there is no prior judicial oversight; interception records may be destroyed before meaningful external review; and the ground of “investigation of any offence” is framed with considerable breadth.

The chilling-effect doctrine, as applied in *Anuradha Bhasin* and extended in *Kunal Kamra*, captures what is happening across the landscape described in this paper. Vague laws do not merely punish those who are convicted under them; they alter the behaviour of everyone who might reasonably fear prosecution, takedown or surveillance.³¹ As Gautam Bhatia has argued, the constitutionally relevant harm is not only conviction, but the silence that the threat of coercive legal action produces, including among persons who had every legal right to speak.³²

The Supreme Court made the foundational point in *Romesh Thapar v. State of Madras*: freedom of speech lies at the foundation of all democratic organisation, because without free political discussion no public education so essential for the proper functioning of popular government is possible.³³ When the mainstream media has largely accommodated itself to power, as several commentators have observed, the online space is often the last place where genuinely critical voices survive. If that space is regulated by a combination of the Sahyog Portal, three-hour takedown windows, the Karnataka Fake News Bill, and a surveillance architecture with no judicial oversight, the result is not a regulated internet. It is a managed one.

IX. SUGGESTIONS AND RECOMMENDATIONS

³¹ *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637 (India), ¶¶ 70–71; *Kunal Kamra v. Union of India*, *Writ Petition (L) No. 9792 of 2023*, Bombay High Court.

³² *Gautam Bhatia*, *Offend, Shock, or Disturb: Free Speech Under the Indian Constitution* 211–25 (Oxford University Press 2016).

³³ *Romesh Thapar v. State of Madras*, (1950) SCR 594 (India).

What is needed are systemic solutions to the problems highlighted in this paper. Even if a brave person will file a lawsuit, it is not a solution to the problem of an architecture of the system.

1. First, there needs to be judicial oversight of the Section 69 surveillance system. The interception, monitoring or decryption of digital communications shall be authorised, monitored or decrypted only with prior authorisation from a designated judicial authority, exception for the circumstances of a genuine emergency to permit the interception, monitoring or decryption of digital communications, then: Compulsory and binding post-factum judicial review, within 48 hours of the interception. The Rules for 2009 require that the records be destroyed, but this should be modified to enable independent audits to be carried out.
2. Secondly, the Sahyog Portal should be placed under the purview of Section 69A's procedural discipline. Any demands to deduct shall be made by the committee and shall be accompanied by a written reasons statement and provide notice to the content creator and shall provide an opportunity for response. IT Rules' compliance window, which was reduced to three hours, should be extended back to 24 hours and mandatory disclosure of reasons to the user.
3. Thirdly, the Karnataka Fake News Bill needs to be rethought from the ground up. The answer to disinformation is media literacy, independent fact checking without the government getting in the way, no civil liability for false speech (and no government minister as head of fact checking).
4. Fourth, a fresh and specific informed consent of the Indian users' needs to be obtained by Meta prior to the rollback of E2EE in application of the DPDP Act. This represents a significant alteration of the relationship between platform and user between the two, in regards to the processing of data. In the DPDP Act, the consent process is approached directly, and should be acted upon by the regulator.

5. Fifth, India should have a National Encryption Policy which explicitly declares that the right to communicate with encryption is part of the right to privacy guaranteed by Article 21 of Indian Constitution and admits only exceptions for lawful access to the information by law enforcement agencies in a narrowly drawn and judicially supervised manner". This "status quo" where there is no policy governing the use of encryption, and there is no legal action that may be taken to remove encryption from the platform, is not governance. It is drift.

X. CONCLUSION

The question posed in this paper is whether communications in India can be termed free even if they are so much so nominally encrypted. The evidence indicates the answer is: hardly, and less and less. A jester is forbidden to make jokes about the rulers. The government has a fact-checking unit that makes the decisions on what is true regarding the government. A social media user is proposing to be sent to seven years in jail by a minister. Any digital communication is subject to a blanket licence for interception by 10 intelligence agencies and records are destroyed before they can be reviewed. And an app that almost half a billion Indians use takes away privacy from their personal chats without their permission.

All of these can be explained as they are one by one. They make a direction if combined together. It's all about a state that's monitoring more, censoring quicker, providing less explanation, and punishing more. This is not the vision of the Constitution. It is its negation.

The Constitution was NOT the product of power trusters. Written by a group of people who had seen unrestrained power for themselves. Article 19 includes speech because the founders knew that if the first thing an authoritarian government would try to take from you is the right to speak, it is the most important right to keep. The right to life and liberty guaranteed under Article 21 was necessary as they knew that without life and liberty there could be no dignity. Puttaswamy added privacy to that, arguing that the Court was living in an age of digital communication, "which is an age of surveillance of thoughts".

It's important to close where we opened.

हो गई है पीर पर्वत सी पिघलनी चाहिए, इस हिमालय से कोई गंगा निकलनी चाहिए।

The pain is as great as a mountain. The law has a way that will cause it to melt. The issue is whether or not it will use them.

XI. REFERENCES

1. Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 (India).
2. Bosco Dominique, Puducherry Man Who Was Booked Under Section 66A of IT Act Hails Supreme Court Verdict, The Times of India (Mar. 24, 2015).
3. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
4. Class 11 Student Sent to Jail for Facebook Post Against UP Minister Azam Khan, Times of India (Mar. 20, 2015, 11:38 PM IST).
5. Constitution of India, 1950, arts. 14, 19(1)(a), 19(2), 21.
6. Drug Probe Against Rhea Chakraborty Over Phone Chats, NDTV (Aug. 26, 2020).
7. Dushyant Kumar, Ho Gayi Hai Peer Parvat-Si Pighalni Chahiye, Kaavyaalaya.
8. Gauri Kashyap, Section 66A: The Dead Law That Still Haunts India, Supreme Court Observer (July 26, 2021).
9. Gautam Bhatia, Offend, Shock, or Disturb: Free Speech Under the Indian Constitution 211–25 (Oxford Univ. Press 2016).
10. Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, G.S.R. 780(E), Gazette of India, Extraordinary, pt. II, sec. 3(i) (Oct. 27, 2009).
11. Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India), § 69, § 79(3)(b).
12. Internet Freedom Foundation, IFF Joins the GEC in Raising Concern on Instagram's Roll Back of Encryption Features (Apr. 13, 2026).
13. Karnataka Misinformation and Fake News (Prohibition) Bill, 2025 (Draft) (India).

14. Kartar Singh v. State of Punjab, (1994) 3 SCC 569 (India); Chintaman Rao v. State of Madhya Pradesh, (1950) SCR 759 (India).
15. Kunal Kamra v. Union of India, Writ Petition (L) No. 9792 of 2023 (Bombay High Court, Jan. 31, 2024) (per Patel J.); tie-breaker opinion by Chandurkar J. (Sept. 2024).
16. Mamata Banerjee Meme Case: SC Says Arrest of Activist Was Arbitrary, The Hindu (May 15, 2019).
17. Medianama, Meta to End Instagram End-to-End Encryption for DMs (Mar. 13, 2026).
18. Ministry of Home Affairs, Order No. 33/4/2013-IS.IV (Dec. 20, 2018) (India).
19. Mohammed Zubair v. State of U.P., (2022) SCC OnLine SC 897 (India).
20. Oxford Human Rights Hub, Weaponizing Vagueness: The Chilling Effect of Karnataka's Fake News Bill on Free Speech and Democratic Pluralism (July 21, 2025).
21. R. Venkataramanan, What Meta's Quiet Retreat from Encryption Privacy on Instagram Means, Telegraph India (May 15, 2026).
22. Romesh Thapar v. State of Madras, (1950) SCR 594 (India).
23. Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).
24. Software Freedom Law Centre India, S. 69 of the Information Technology Act and the Decryption Rules: Absence of Adequate Procedural Safeguards (May 17, 2023).
25. The Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023).
26. Vidhi Centre for Legal Policy, An Analysis of the Karnataka Fake News Bill (Sept. 12, 2025).
27. X Corp. v. Union of India, W.P. No. 7405 of 2025, Karnataka High Court, decided on 24 September 2025.