The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

THE SECURITISATION OF CYBERSPACE: INTERNET REGULATIONS IN INDIA THROUGH A SECURITY AND GOVERNANCE LENS

-Sristi Dutta

INTRODUCTION

"A law that is vague... leaves the citizen to speculate about what it prohibits — and is therefore invalid." — Supreme Court of India, Shreya Singhal v. Union of India (2015)[1]

India does not have a problem with internet regulations. It has many updated regulations in action. It has a problem with accountability. The regulations are already in place, and many are reasonable. What's lacking is the structure to ensure that these reasonable regulations do not turn into something else and are misused by the public or by the authorities.

This distinction is important. Much of the writing on this topic treats security regulation and democratic freedom as if they are always at odds. It suggests that every content removal is censorship and every surveillance measure is tyranny. This view is overly simplistic and not a deep dive into what should change to make it more ideal. The more complex question this article seeks to address is what conditions make security regulation legitimate, and whether India's current framework meets those conditions.

THE CULTURAL BACKGROUND

Before discussing laws and court rulings, we should take a moment to consider something legal analysis often overlooks: what the internet actually became in India, and why that's crucial for regulation. The way internet was appropriated in the society became a much crucial reason for the regulatory structures that was eventually built.

India gained mass internet access very late but very rapidly. In 2011–2012 and 2013, India saw a variety of agitations and road protests in places like New Delhi, Mumbai, and Bangalore. Social media was fully utilized during the anti-corruption movement and the mass mobilization against the Delhi gang rape to organize people, bring them together, and raise awareness of injustice and the broken system that leads to high-level corruption and poor law-and-order conditions in urban areas. However, in certain other instances, as during the ethnic conflicts in Assam in 2012 and 2013, during the communal riots in Muzaffarnagar, they also served as a means of spreading rumours, distributing false information, and causing panic and mayhem among the general populace. Non-state actors who are domestic and international anti-

[1] Shreya Singhal v. Union of India, AIR 2015 SC 1523 (India).

elements have abused social media to undermine law and order by disseminating rumours and posting misleading information and photographs online.[2]

This context influences everything that follows. When people criticize India's regulatory response as overbearing, they sometimes forget the chaos that prompted it. The disorder was real. The government's intention to manage digital platforms didn't come out of nowhere; it was a reaction to digital platforms enabling violence. Understanding this does not mean agreeing with every regulatory decision made by the government. It indicates that the starting point was a genuine problem, not just an excuse.

THE DUAL FRAMEWORK

Two theoretical perspectives can help explain what has happened.

The first is securitisation theory, developed by Barry Buzan and Ole Wæver. According to Buzan[3], "security is about survival" and from this understanding a matter is presented as "posing an existential threat to a designated referent object", traditionally but not necessarily the state, comprised of government, territory and society. In Wæver's first concept, security is equated with a speech act, while securitization refers to how an issue is linguistically portrayed as an existential threat[4]. Next to generally affirming this concept, Buzan[5] additionally put more emphasis on the role of constituencies to acknowledge and thereby to 'back up' a speech act. By such consent, speech acts – then defined as securitization moves – turn into securitizations. In this regard, speech acts shift from being *"*productive of security" to being "one component of the inter-subjective construction of security".[6]

In the context of Indian cyberspace, this framework reveals something significant. The government's use of "national security" to justify blocking content, monitoring platforms, and shutting down the internet is not merely a reaction to threats. It also shapes how those threats are understood and what responses are available. Securitisation creates the grounds for its own justification.

The second framework is Foucault's concept of governmentality, in which he propounds that "With government it is a question not of imposing law on men, but of disposing things: that is to say, of employing tactics rather than laws, and even of using laws themselves as tactics — to arrange things in such a way that, through a certain number of means, such and such ends may be achieved." [7]In this case, the state does more than block content or shut down the internet. It reshapes the very platforms so that governance becomes ingrained in the daily

[2] N.K. Datta, *Social Media and Internal Security Challenges in India* (2014).

[3] Barry Buzan, Ole Wæver & Jaap de Wilde, *Security: A New Framework for Analysis* 21 (1998).

[4] Ole Wæver, Securitization and Desecuritization, in *On Security* 46 (Ronnie D. Lipschutz ed., 1995).

[5] Barry Buzan, Ole Wæver & Jaap de Wilde, *Security: A New Framework for Analysis* 21 (1998).

[6] Matt McDonald, Securitization and the Construction of Security, 14 Eur. J. Int'l Rels. 563, 566 (2008).

[7] Michel Foucault, Governmentality, in *The Foucault Effect: Studies in Governmentality* 87, 95 (Graham Burchell, Colin Gordon & Peter Miller eds., 1991).

operation of digital infrastructure. The platforms become extensions of the state's regulatory reach, regardless of whether a specific emergency is declared.

Together, these frameworks illustrate a dual movement: securitisation opens the door to extraordinary measures, while governmentality creates the space for those measures to become normalised

HOW INDIA GOT HERE: A CHRONOLOGICAL VIEW

The Information Technology Act of 2000 was mainly an economic law. It focused on e-commerce, digital signatures, and cybercrime. Section 69A, which allows the government to block access to digital content, existed but was limited.[8]

The amendment in 2008 changed the course. The 26/11 attacks highlighted India's vulnerability to coordinated cross-border violence. The government responded by significantly expanding its digital powers. Section 69A was broadened, and cyber-terrorism was defined as a specific offense. The idea of national security became embedded in the IT Act in a way it had not been before.[9]

However, 2008 was mostly reactive. The real shift occurred in 2021 with the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules. These established a new proactive governance framework. Platforms with large user bases had to appoint grievance officers, adhere to content removal timelines, and, most controversially, identify the "first originator" of viral messages.[10] This requirement effectively pressured messaging platforms to compromise end-to-end encryption. The government framed this as a measure for counter-terrorism and child safety. This coincided with the Indian government blocking well over 250 applications of Chinese origin to protect its digital borders as a direct geopolitical response following the Galwan Valley clash in 2020.[11]

Then came 2025. Operation Sindoor faced India with a challenge that the 2021 Rules aimed to address. The Observer Research Foundation documented about 265 million security alerts across monitored sources during that time. Pakistani state-linked actors used AI-generated misinformation, fabricated government communications, manipulated videos, and fabricated military victory claims to sow confusion, erode public trust and to manipulate global opinion. [12]The scale and sophistication of this operation partially justified the case for stronger online governance. This was not a fabricated threat; it was real, documented, and serious.

WHERE THE FRAMEWORK BREAKS DOWN

Recognizing that the security argument has merit doesn’t mean the framework is effective. Let’s start with Section 69A. The Blocking Rules of 2009 state that orders must be "reasoned

[8] Information Technology Act, No. 21 of 2000, Section 69A (India).
[9] Information Technology (Amendment) Act, No. 10 of 2009 (India).
[10] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 4(2) (India).
[11] India Today Tech, *BGMI, Garena Free Fire, TikTok and More Banned in India: Check the Full List* (Aug. 19, 2022), https://www.indiatoday.in/technology/news/story/bgmi-garena-free-fire-tiktok-and-more-banned-in-india-check-the-full-list-1990048-2022-08-19
[12] Harsh V. Pant & Sameer Patil eds., *Current Trends in India's National Security 2025*, ORF Special Report No. 245 (2025).

and recorded." [13]However, Rule 16 keeps those reasons secret. Affected parties cannot see why they were blocked. They cannot challenge a case they cannot access. The Supreme Court's ruling in Anuradha Bhasin v. Union of India, stating that shutdowns must be proportionate, temporary, and subject to judicial review, is an important development.[14]But challenges come after the damage is done. The gap between action and review often favors the executive.

The grievance committees established under the 2021 Rules face a similar issue. They are presented as independent review bodies, but they are not truly independent. Government representatives and platform officials dominate their composition. Calling them independent is a legal fiction that serves no one but the government's desire to look procedurally legitimate.

The traceability requirement poses the biggest issue. Requiring platforms to identify message senders is not just a privacy concern; it is also about the architecture of the system. Once the ability exists to trace any message back to its origin, that capability will be used. The rules offer no warrant requirement for its implementation, no sunset clause, and no independent audit. Counter-terrorism justifications are being used to create infrastructure that does not discriminate based on what is being monitored.

The Digital Personal Data Protection Act of 2023 mirrors this issue on a larger scale. Section 17(2)(a) exempts state data processing for national security in such broad language that it undermines most of the privacy rights the Act otherwise provides.[15]The security exception once again overshadows the rule itself.

WHAT NEEDS TO CHANGE

Judicial warrants should be needed before blocking orders are enacted under Section 69A, except in emergencies, which should be reviewed by a judge within 48 hours. This is standard practice in other democracies. There is no valid reason India cannot implement it.

Blocking orders should be published in redacted form. Not the operational details that truly need protection, but the legal basis, the provision cited, and the type of harm alleged. This information should allow a court or citizen to understand what happened and challenge it if necessary.

The traceability requirement should be refined. Retaining metadata like information about when and between whom communications occurred can serve legitimate security needs without breaking encryption. It should be the default option.

Grievance committees require true independence. This means representation from the judiciary, involvement from civil society, and the authority to review government blocking decisions with access to the underlying reasoning. Without these measures, they remain mere window dressing.

---

[13] Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 16 (India).

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

[15] Digital Personal Data Protection Act, No. 22 of 2023, § 17(2)(a) (India).

Finally, Parliament should establish a standing oversight committee for national security orders. This committee would conduct classified briefings when needed, hold quarterly reviews, and monitor for patterns of misuse. Democracies that take security seriously also prioritize oversight. The two do not conflict.

CONCLUSION

India's approach to cybersecurity reflects a real confrontation with real threats. The chaos during India's early internet years, the documented reality of cross-border information warfare, and the operational lessons from Operation Sindoor are not mere excuses; they are reasons.

But security governance without accountability is not true governance. It is simply discretion. And discretion, no matter how well-intentioned at the start, tends to expand toward its limits. The institutional reforms proposed here are not about weakening India’s ability to respond to threats. They are about ensuring that response is responsible and accountable.