Arnab Chanda
Research Scholar,
Dept of Journalism and Mass Communication,
University of Calcutta
acjmc_rs@caluniv.ac.in

Article ID No. 2813 *DOI No.* https://doi.org/10.5281/zenodo.21214989

From Safe Harbour to Algorithmic Camp: India's IT Rules and the Normalization of Digital Exception

Arnab Chanda

Abstract:

India's digital governance framework regulates the legal responsibilities of social media platforms, messaging services, and streaming providers (identified as online intermediaries) primarily through the Information Technology Act, 2000 and executive Rules issued under it. A central feature of this framework is "safe harbour immunity," the legal protection that shields platforms from liability for content posted by their users. Since the notification of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules in 2021, and through successive amendments up to March 2026, the Indian executive has made safe harbour increasingly conditional on compliance with expanding content-removal mandates issued outside formal judicial channels. In the financial year 2024–25 alone, the Ministry of Home Affairs issued an average of 290 blocking orders per day through the Sahyog portal, an automated government takedown infrastructure. Critics argue that the process bypassed the statutory and court-supervised procedures that the Supreme Court of India mandated in Shreya Singhal v. Union of India (2015). Platforms that decline to comply risk losing their safe harbour protection, making non-compliance commercially unthinkable. This article traces the evolution of India's intermediary governance regime from the IT Act 2000 to the IT Rules 2021 and its draft amendment proposals of March 2026.

Drawing on Giorgio Agamben's political philosophy — particularly his argument that modern states have normalized "states of exception" in which executive power operates outside ordinary legal constraints — and Michel Foucault's concept of governmentality, which describes how states govern populations not through direct coercion but through calibrated incentive architectures that shape conduct, the article argues that successive policy interventions constitute a single cumulative structural project, the creation of "algorithmic camp." The algorithmic camp is a regulatory zone in which the procedural safeguards, such as notice, independent review, and judicial oversight, that distinguish constitutional governance from executive arbitrariness have been systematically bypassed through delegated ministerial Rules that carry the force of statute while escaping parliamentary scrutiny.

Keywords*: Algorithmic Camp, State of Exception, Governmentality, Intermediary Governance, India, IT Rules*

1. Introduction:

On an average day in 2024–25, the Ministry of Home Affairs (MHA) issued 290 orders to remove online content from digital platforms across India. In that single year, a total of 1,11,185 pieces of online content were blocked (MHA Annual Report, 2026)[1]. These orders didn't follow a normal democratic procedure. The blocking orders are neither issued by the courts nor through the formal statutory mechanism under Section 69A of the Information Technology Act, 2000 (hereafter IT Act). They are issued through the Sahyog portal, an automated content-removal infrastructure operated by the MHA's Indian Cybercrime Coordination Centre (I4C). On the other hand, platforms that refused to comply with such orders risked the loss of their safe harbour immunity, the legal shield protecting them from liability for user-generated content, making non-compliance commercially unthinkable (The Wire, 2026)[2]. The architecture of this system ensures that different ministries of the Indian government, along with state governments, operating through one centralized technical portal, can now function as the de facto arbiter of what over a billion people may read, watch, and share online. The scale of this intervention sits in stark contrast to India's constitutional self-image as the world's largest democracy. In the 2026 World Press Freedom Index, Reporters Without Borders ranked India 157th out of 180 countries, a six-place drop from 2025. They identified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (hereafter IT Rule 2021) as a major contributor for the decline (RSF, 2026)[3].

This study focuses on the evolution of India's intermediary governance framework from the IT Act 2000 to the IT Rules 2021 and its subsequent amendments, arguing that the regulatory sequence constitutes not a series of disconnected policy adjustments but a single cumulative structural project — the "algorithmic camp." Through a rereading of Giorgio Agamben's (1998[4], 2005[5]) theory of the state of exception, and Michel Foucault's (1991[6], 2007[7]) concept of governmentality, the article demonstrates that India's digital governance architecture has normalised a permanent state of exception within the ordinary mechanics of platform regulation, systematically bypassing the procedural safeguards that distinguish constitutional governance from executive arbitrariness.

---

[1] Ministry of Home Affairs. (2026). *Annual report 2024–2025*. Government of India.
[2]The Wire. (2026, March 27). *MHA took down 290 posts per day in 2024–25, on an average: Ministry data*.
[3]Reporters Without Borders. (2026). *India*. In *2026 World Press Freedom Index*.
[4]Agamben, G. (1998). *Homo sacer: Sovereign power and bare life* (D. Heller-Roazen, Trans.). Stanford University Press. (Original work published 1995)
[5]Agamben, G. (2005). *State of exception* (K. Attell, Trans.). University of Chicago Press. (Original work published 2003)
[6]Foucault, M. (1991). Governmentality (C. Gordon, Trans.). In G. Burchell, C. Gordon, & P. Miller (Eds.), *The Foucault effect: Studies in governmentality* (pp. 87–104). University of Chicago Press.
[7]Foucault, M. (2007). *Security, territory, population: Lectures at the Collège de France, 1977–1978* (G. Burchell, Trans.). Palgrave Macmillan.

Before proceeding, a foundational distinction must be established, one central to the argument this article makes. There is a critical difference between an Act of Parliament and the Rules made under it. An Act, such as the Information Technology Act, 2000, is primary legislation, debated, scrutinized, and passed by Parliament, carrying the democratic legitimacy that the legislative process is designed to confer. Rules, by contrast, are subordinate or delegated legislation, issued by the executive branch under authority granted by a parent statute without requiring parliamentary debate or approval. IT Rules 2021 and its subsequent amendments are not laws passed by Parliament. They are ministerial instruments issued under Section 87 of the IT Act, though they carry the practical force of statute.

2. The Evolution of Intermediary Governance in India:

The journey of digital regulation in India began at the turn of the millennium. The period is defined by a global struggle to navigate the undefined spaces created by the rapid commercialization of the internet (Gupta & Srinivasan, 2023)[8]. In the year 2000, India enacted the Information Technology Act. The legislation aimed to provide legal recognition for electronic records and boost the Information Technology industry (Katkuri, 2024)[9]. This initial legislative framework was primarily inspired by the UNCITRAL Model Law on Electronic Commerce, adopted in 1996-(Standing Committee, 1999)[10]. In this early era, the concept of an intermediary was relatively narrow. The original Section 79 was titled "Network Service Providers not to be liable in certain cases." The network service providers were granted a form of safe harbour protection, a legal shield that exempted them from liability for third-party content. During these formative years, the internet was viewed as a fragile new means of communication that required protection from legal interventions (Gupta & Srinivasan, 2023)[11].

The Bazee.com case of 2008, in which an e-commerce platform's CEO was arrested over offensive video content sold on the site, exposed the regulatory vacuum (Avnish Bajaj vs. State (NCT) of Delhi, 2008)[12]. The 2008 Mumbai terror attacks then accelerated state interventionism, as intelligence agencies had struggled to gather surveillance data during the crisis (Nojeim et al., 2021)[13]. The resulting IT Amendment Act of 2008, passed without significant parliamentary

[8] Gupta, I., & Srinivasan, L. (2023). Evolving scope of intermediary liability in India. *International Review of Law, Computers & Technology*, 37(1), 1–23.
[9] Katkuri, S. (2024). Need of encryption legislation: Protecting India's digital realm and beyond. *Indian Journal of Public Administration*, 70(3), 562–578.
[10] Standing Committee on Communications and Information Technology (2025–26). (2026). Twenty-seventh report: Impact of emergence of artificial intelligence and related issues (CCIT No. 439). Lok Sabha Secretariat, Government of India.
[11] See Footnote no. 8
[12] Avnish Bajaj v. State (NCT) of Delhi, 150 DLT 769 (Del. HC 2008).
[13] Nojeim, G., Maheshwari, N., & Miglani, E. (2021). Encryption in India: Preserving the online engine of privacy, free expression, security, and economic growth. *Indian Journal of Law and Technology*, 17(1), Article 2.

debate, broadened the category of "intermediary" to encompass the emerging platform ecology, introduced the controversial Section 66A criminalising "grossly offensive" online messages, and granted the government powers under Section 69A to block content in the interests of national security and public order (IT Amendment Act, 2008)[14]. This marked the decisive shift from a hands-off approach toward cyber sovereignty (Narrain, 2019)[15].

The next major step in this regulatory odyssey was the notification of the Information Technology (Intermediaries Guidelines) Rules in 2011. These rules attempted to define the elusive concept of due diligence (Karanicolas, 2021)[16]. Intermediaries are mandated to take down content within thirty-six hours of receiving a complaint. For the first time, platforms were required to inform their users through service agreements not to host or share objectionable material, a broad category that included anything from defamatory content to material that threatened the unity and integrity of India (IT Rules, 2011)[17]. Critics argued that these rules started incentivizing collateral censorship (Uppaluri, 2012)[18].

The tension between these state-imposed restrictions and the fundamental right to free speech reached a boiling point in the landmark case of Shreya Singhal v. Union of India in 2015. The Supreme Court of India (SCI) delivered a powerful defence of digital expression. SCI struck down Section 66A for its vagueness and overbreadth. The Court recognised that the provision disproportionately infringed upon the freedom of speech guaranteed by the Constitution, potentially curtailing a vast amount of protected and innocent expression. Furthermore, the Court read down the requirement for actual knowledge under Section 79. Intermediaries were not legally required to remove content unless they received a specific court or government order. Though the Court upheld Section 69A, it emphasised that such blocking powers must be exercised by reasoned orders and in compliance with procedural safeguards (Shreya Singhal v. Union of India, 2015)[19]. The judgment was celebrated as a landmark defence of digital expression. Yet, its practical impact was always more limited. Even after the judgment, censorship in India continued and, in many cases, intensified through mechanisms, such as administrative directions, executive pressure, and the structural incentives of conditional

[14] Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, 2009 (India).
[15] Narrain, S. (2018). Social media, violence and the law: "Objectionable material" and the changing contours of hate speech regulation in India. *Culture Unbound*, *10*(3), 388–404.
[16] Karanicolas, M. (2021). Authoritarianism as a service: India's moves to weaponize private sector content moderation
with the 2021 Information Technology Rules. *Indian Journal of Law and Technology*, 17(2), Article 4.
[17] Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, 2009 (India).
[18] Uppaluri, U. (2012). *Constitutional analysis of the Information Technology (Intermediaries' Guidelines) Rules, 2011*. Centre for Internet and Society.
[19] Shreya Singhal v. Union of India, Writ Petition (Criminal) No. 167 of 2012, Supreme Court of India. (2015).

immunity (Banerjee, 2021)[20]. In the wake of the Shreya Singhal judgment, the digital landscape continued to evolve rapidly, characterised by the rise of over-the-top (OTT) streaming services and a vibrant sector of native digital news organizations (Mehta & Amit-Danhi, 2024)[21]. However, with the rapid expansion of internet access, new challenges started to emerge; the proliferation of fake news, the use of social media to incite communal violence, and the growing influence of global tech giants (Press Information Bureau, 2021)[22]. The political environment became increasingly polarised. The state started expressing concerns that unregulated digital platforms were being misused by anti-national elements (Nojeim et al., 2021)[23]. The period also saw India become the global leader in internet shutdowns (Access Now, 2024)[24].

The year 2021 marked a paradigm shift with the notification of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, (Gupta & Srinivasan, 2023)[25]. A core feature of the 2021 Rules was the distinction between ordinary social media intermediaries and significant social media intermediaries (SSMIs). The latter being those with more than five million registered users in India. SSMIs were hit with heavy new obligations, including the requirement to appoint a local chief compliance officer and a nodal contact person for 24/7 coordination with law enforcement agencies (Nagarathna, 2022)[26]. The IT Rules 2021 represented the state's comprehensive response to the new realities, and it is to those rules and their continuous evolution through amendments that the theoretical framework developed in the next section tries to understand.

3. Theoretical Framework:

The structural logic of India's evolving digital governance becomes more prominent if studied from the perspective of political philosophy of sovereign power. This section introduces the key philosophical concepts.

[20] Banerjee, A. (2021). Internet censorship in India: The law and beyond. In S. K. Sandeen, C. Rademacher, & A. Ohly
(Eds.), *Research Handbook on Information Law and Governance* (pp. 339–355). Edward Elgar Publishing.
[21] Mehta, S. N., & Amit-Danhi, E. R. (2025). The road to censorship: The case of digital audiovisual industries in India.
International Journal of Cultural Policy, 31(7), 881–897.
[22] Press Information Bureau. (2021, February 25). Union ministers Prakash Javadekar and Ravi Shankar Prasad address a
press conference. https://www.youtube.com/watch?v=H0eqWuj84-0
[23] See no. 14.
[24] Access Now. (2024, May 15. *India leads the world internet shutdown count for sixth year*.
[25] See no. 8.
[26] Nagarathna, A. (2022). The State's access to data and internet intermediary response – an assessment of India's attempt to reallocate the legal framework to ensure national security. *International Review of Law, Computers & Technology*, 36(3), 404–430.

3.1 The State of Exception and Its Normalisation

Carl Schmitt's proposition that "sovereign is he who decides on the exception" defines sovereignty not by the power to make ordinary law but by the power to determine when ordinary law does not apply (Schmitt, 1985)[27]. The state of exception is the sovereign's declaration that a crisis justifies the temporary or indefinite suspension of constitutional constraints. The paradox is structural: the sovereign is simultaneously inside the legal order as its guardian and outside it as the authority who can suspend it, the threshold at which law and lawlessness become indistinguishable (Agamben, 2005)[28].

Giorgio Agamben historicised Schmitt's analysis to show that what Schmitt presented as a limit case has become the normal mode of modern governance. Following Walter Benjamin's observation that "the 'state of emergency' in which we live is not the exception but the rule," Agamben argues that the exception has migrated from the margins to the centre of political life, becoming "the normal form of governance" — a permanent paradigm that has quietly displaced constitutional normality (Agamben, 2005[29]; Benjamin, 1968[30]). Other scholars have also taken up this task to demonstrate that exception works through law rather than beyond it (Neocleous, 2006[31]; Neal, 2012[32]).

3.2 Bare Life and the Algorithmic Camp

The normalisation of the exception transforms the individual subject. Agamben's concept of "bare life" builds on the Greek distinction between *zoe* (biological existence shared by all living things) and *bios* (the qualified, politically meaningful form of life within the polis). According to Aristotle's political philosophy, political membership led to the transition from *zoe* to *bios.* Following Hannah Arendt's (1963)[33] observation that biological life occupies the very centre of the political scene of modernity, Agamben argues that modern politics does not produce the classical transition from zoe to bios; instead, it captures biological life while stripping it of legal-political protection. Aristotle's proposition, therefore, is reversed; people are reduced to bare life, stripped of every juridical and political attribute (*bios*). In this process, the 'rule of law' ceases to exist; the sovereign works through what Agamben termed 'force of law', creating a

[27] Schmitt, C. (1985). *Political theology: Four chapters on the concept of sovereignty* (G. Schwab, Trans.). MIT Press. (Original work published 1922)
[28] See no. 5.
[29] See no. 5.
[30] Benjamin, W. (1968). *Theses on the philosophy of history*. In H. Arendt (Ed.), Illuminations (H. Zohn, Trans.) (pp. 253–264). Schocken Books. (Original work published 1940)
[31] Neocleous, M. (2006). The problem with normality: Taking exception to 'permanent emergency'. Alternatives: *Global, Local, Political*, 31(2), 191–213.
[32] Neal, A. (2012). Normalization and legislative exceptionalism: Counterterrorist lawmaking and the changing times of security emergencies. *International Political Sociology,* 6(3), 260–276.
[33] Arendt, H. (1963). *On revolution*. The Viking Press.

paradox in which law remains in force without being applied, while executive measures that were not formally considered as law suddenly acquire the 'force' of law. This transition effectively produces a threshold of indeterminacy between democracy and absolutism, as the executive power absorbs the legislative power, leading to the collapse of the traditional separation of powers (Agamben, 2005)[34]. The figure embodying this condition is the *homo sacer* — excluded from the protections of civil law yet included within the political order on the sovereign's terms alone, existing in a "zone of indistinction" where the boundary between legal and illegal, protected and unprotected, dissolves into sovereign discretion (Agamben, 1998)[35].

McQuillan (2015)[36] applies this framework to algorithmic governance, arguing that pervasive data-mining and automated systems create "algorithmic states of exception" in which systems deploy Agamben's "force-of-law" without its corresponding "form of law." They bind, penalise, and assign life-affecting consequences without procedural constraints, judicial oversight, or transparency. Gheytasi et al. (2026)[37] extend this to argue that the twenty-first century produces a form of "digital bare life." In this new formation, the user is reduced to a collection of data points, stripped of privacy and due process, suspended in a juridical void where fundamental rights are contingent upon shifting definitions of permissible content dictated by executive discretion.

The spatial materialization of this condition is what Agamben calls "the camp." The ideal embodiment of the camp is the Nazi concentration camps of Germany. Agamben theorized it as a general political structure. The camp is a territory in which law is suspended, where sovereign power operates directly on bare life without the mediating constraints of rights or procedure. The camp can take many forms, in the modern world, it only requires a space in which law is suspended, and sovereign power operates directly on bare life. This article argues that the space (the camp) that is being constructed in the Indian digital sphere can be termed the *algorithmic camp*. The algorithmic camp is not a metaphor for atrocity, nor is the comparison intended to trivialise historical suffering. Rather, it uses Agamben's structural concept. It depicts the reality of what happens when a digital regulatory architecture systematically removes the procedural safeguards that distinguish governed citizens from governed populations operating in the digital sphere.

3.3. Governmentality and the Conduct of Digital Conduct

Agamben's framework, though powerful, is less equipped to describe the continuous, diffused exceptional mechanisms through which modern states govern populations. Foucault's

[34] See no. 5.
[35] See no. 4.
[36] McQuillan, D. (2015). Algorithmic states of exception. *European Journal of Cultural Studies*, 18(4–5), 564–576.
[37] Gheytasi, S., Khoshnood, A., & Sohrabzadeh, A. (2026). Bare life in the digital age: Homo sacer, necropolitics, and algorithmic control in the selected contemporary fiction. *3L: Language, Linguistics, Literature, 32*(1), 157–171.

governmentality becomes important. In his 1977–78 lectures, Foucault described the modern art of government as operating not primarily through law and force but through the management of "the conduct of conduct" — the calibration of environments, incentives, and norms that guide how populations govern themselves (Foucault, 2007)[38]. Power in governmentality designs environments that shape subjects' choices, labelling certain acts responsible and others irresponsible, so that the sovereign does not need direct coercion (Foucault, 1991)[39]. Applied to digital platforms, governmentality manifests in the architecture of conditional safe harbour immunity. The state moves from direct censorship to creating an incentive structure in which platforms censor on its behalf. Research on the post-Snowden "chilling effect" shows that when users are aware of surveillance, they systematically self-censor, exercising power over themselves through self-restraint "without any coercion". This is where the panoptic logic becomes most effective: discipline without the disciplinarian (Manokha, 2018)[40]. Badouard, Mabi, and Sire (2016)[41] identify three simultaneous logics of digital governmentality: directing conduct through incentives (governmentality by incentives), constraining conduct by removing technical capabilities (governmentality by design), and framing conduct by shaping normative categories (governmentality by framing). As the conclusion demonstrates, India's IT Rules deploy all three simultaneously.

4. The IT Rules 2021: Institutionalizing the Exception:

The notification of the IT Rules 2021 represented a definitive shift from a relatively open internet toward high-intensity executive control (Bapat et al., 2021)[42]. Using the delegated authority of Section 87 of the IT Act, the Rules brought digital news media and OTT streaming platforms under direct executive oversight for the first time. The government justified this as necessary to combat fake news, protect women from online abuse, and ensure a "level playing field" between digital and legacy media. Critics contended that the Rules co-opted the enormous power of private platforms, turning content moderation into a mechanism targeting dissent outside traditional judicial scrutiny (Karanicolas, 2022)[43]. The three-tier grievance redressal mechanism was the Rules' central structural innovation. The first tier required platforms to appoint a resident grievance officer to address user complaints within thirty days. The second tier consisted of self-regulatory bodies. The third and decisive tier is the Inter-Departmental

[38] See no. 8.
[39] See no. 7.
[40] Manokha, I. (2018). Surveillance, Panopticism, and Self-Discipline in the digital age. *Surveillance & Society*, *16*(2), 219–237.
[41] Badouard, R., Mabi, C., & Sire, G. (2016). Beyond "Points of Control": logics of digital governmentality. *Internet Policy Review*, *5*(3).
[42] Bapat, K., Jain, A., Gupta, A., & Singh, T. (2021, February 27). *How the intermediaries rules are anti-democratic and unconstitutional*. Internet Freedom Foundation.
[43] See no. 17.

Committee (IDC). IDC is a body composed entirely of government representatives from various ministries, empowered to hear appeals from the second tier and to order platforms to delete or modify content (IT Rules, 2021)[44]. The IDC can be convened by the Ministry of Information and Broadcasting, and its orders carry the force of law as non-compliance risks the platform's safe harbour protection (Nayak, 2021)[45]. The structural implications of this architecture for the concept of sovereign exception are direct and significant. The accountability mechanism is inverted from what constitutional governance requires. In a functioning democracy governed by the rule of law, if the state wants to suppress expression, it must go before an independent court, justify its action against constitutional standards, and bear the burden of demonstrating that the restriction is proportionate and necessary (Sweet & Mathews, 2019)[46].

The IT Rules reversed this structure. Under the new rules, the platform bears the burden of satisfying a committee of government officials, and if it fails to comply, it loses the legal protection on which its entire commercial existence depends. The structure is viewed as a form of 'authoritarianism as a service,' where the executive branch can override private moderation decisions and act as the final arbiter of meaning (Karanicolas, 2022)[47]. The state achieves the effects of direct censorship without formally attributing it. The IDC creates the zone that Agamben identifies as the space where the categorical distinction between lawful and unlawful is dissolved into sovereign discretion, the hallmark of the state of exception. IDC is a body that simultaneously acts as an executive and a judicial organ. The structure bypasses the procedural safeguards established by the Supreme Court in the *Shreya Singhal* case (Nagarthna, 2022)[48]. The IDC order carries the practical force of a compulsory direction but lacks democratic protections. (Sharma, 2026)[49].

The traceability mandate of Rule 4(2) of the IT Rules 2021 illustrates how the Indian state constructs the figure of digital bare life. The rule mandates that messaging platforms identify the "first originator" of a specific piece of information (IT Rules, 2021)[50], which critics count as a

[44] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (India).
[45] Nayak, N. (2021). Legalizing executive control: On the law of online journalism in India. *Indian Law Review*, 8(1), 20–41.
[46] Sweet, A. S., & Mathews, J. (2019). *Proportionality balancing and constitutional governance: A Comparative and Global Approach*. Oxford University Press.
[47] See no. 17.
[48] See no. 26.
[49] Sharma, S. (2026). Algorithmic censorship and shadow banning: Legal blind spots in India's digital speech regime. *Zenodo.*
[50] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (India).

threat to end-to-end encryption in India (Balendra, 2024)[51]. The mandate not only restricts a category of harmful speech; it constructs a new kind of digital subject. A communicating subject with anonymity is a subject capable of dissent, whistleblowing, and political opposition. The speech of those who challenge power needs protection. The traceability mandate demands that the digital citizen be permanently identifiable, permanently traceable, and permanently available to sovereign scrutiny. The person who posts anonymously about police abuse, the journalist who protects a source, the dissident who challenges government policy, all are required by this rule to shed the protective clothing of anonymity. This is digital bare life in Agamben's sense. Inclusion in the digital public sphere is only possible on the condition of absolute transparency to sovereign authority, with the alternative being exclusion from communication entirely (Peerzada et al, 2025)[52].

The governmentality dimension of the Rules is visible in what India's digital rights community calls "mob censorship" (Abhishek, 2023)[53] — the weaponisation of the complaint mechanism by organised political groups and majoritarian vigilante formations to harass independent journalists and dissenting voices (Banaji, 2018)[54]. It appears, superficially, to be a democratic feature where citizens are empowered to hold publishers accountable. In practice, it distributes disciplinary function across the social body. The state doesn't need to act directly once it has engineered an environment in which organized political formations manage the information space on its behalf. As any person can file a grievance regarding any content, the mechanism is structurally susceptible to weaponization by political troll armies and majoritarian vigilante groups seeking to harass independent journalists and dissenting voices. -The state's objective is not the suppression of any specific content item but the management of the conditions under which political will and collective opposition can be formed and expressed (Sahoo, 2023)[55].

Scholars have raised concerns that the Over-the-Top (OTT) entertainment sector, which previously enjoyed a vibrant period of complex and diverse storytelling, is now facing the crisis of self-censorship (Mehta & Amit-Danhi, 2024)[56]. Here, the control is exercised through the threat of legal backlash and economic consequences (Basu & Sen, 2023)[57]. A controversy erupted over

[51] Balendra, S. (2024). *Free speech in the puzzle of content regulation: Insights from the West and the Global South*. Springer Nature Switzerland AG.

[52] Peerzada, R. A., Sharma, A. P., & Kannan, S. (2025). The jurisprudence of digital blackouts: Law and its exceptions in Jammu and Kashmir. *Human Geography*.

[53] Abhishek, A. (2023). The state deputizing citizens to discipline digital news media: The case of the IT Rules 2021 in India. *Digital Journalism*, 11(10), 1769–1787.

[54] Banaji, S. (2018). Vigilante publics: Orientalism, modernity and Hindutva fascism in India. *Javnost – The Public,*
25(4), 333–350.

[55] Sahoo, S. (2023). India's internet shutdowns as biopolitics: The formation of political will and opinion through collective action under attack. *Critical Studies in Media Communication*, *40*(5), 291–305.

[56] See no. 22.

[57] Basu, S., & Sen, S. (2023). Silenced voices: Unravelling India's dissent crisis through historical and contemporary

the *Tandav* web series. Creators faced multiple police complaints across several states for allegedly hurting religious sentiments. Global platforms like Netflix and Amazon Prime Video have become increasingly risk-averse (Rai, 2024)[58]. The resulting communicative ecology is one where alternative and resistant narratives are filtered out at the creator level, while majoritarian cultural narratives are amplified. The 2021 Rules have fundamentally reconfigured the relationship between the state and global tech giants (Wadha, 2025)[59]. The skirmish with Twitter (now X) during the farmers' protests exemplified the new discourse. The government demanded the removal of accounts and tweets related to the farmers' protests. The platform initially resisted. However, the state threatened to jail its employees, eventually forcing compliance (Wadha, 2025)[60].

The FCU (Fact-Check Unit) amendment of 2023, which empowered the central government to designate information about its own conduct as "false", exemplified the state's most audacious assertion: the authority to define factual reality. Bhatia (2025)[61] noted with precision that this would have given the state the power to "judge its own cause." The Bombay High Court struck it down on grounds of equality and freedom of expression, recognising that truth is often a function of interpretation and cannot be coercively mandated (Ravi & Sundar, 2024)[62].

5. The 2025–2026 Amendment Cycle: Normalizing the Emergency:

The regulatory developments between October 2025 and March 2026 mark the most ambitious phase of India's project of digital governance and the clearest empirical demonstration of what it means for the state of exception to become permanent. This section analyses each of the three regulatory interventions in sequence.

5.1 The October 2025 Amendment and the Sahyog Portal:

The October 2025 amendment, effective November 2025, amended Rule 3(1)(d) to introduce "reasoned intimation." According to the amended rules, any directive for content removal must be issued in writing by an officer not below Joint Secretary rank, with a mandatory monthly

analysis of free speech and suppression. *Information & Communications Technology Law*, 33(1), 42–65.

[58] Rai, S. (2024). Between the divine and digital: Parsing Modi's charismatic avatar. *Media, Culture & Society*, *46*(4), 834–850.

[59] Wadhwa, S. (2025). Content blocking orders and status of digital rights: Assessment of two key verdicts in India. *Information & Communications Technology Law*, 34(1), 44–61.

[60] See no. 63.

[61] Bhatia, G. (2025). Disinformation, misinformation and democracy: An Indian constitutional perspective. In R. J. Krotoszynski Jr., A. Koltay, & C. Garden (Eds.), *Disinformation, misinformation, and democracy: Legal approaches in comparative context* (pp. 258–269). Cambridge University Press.

[62] Ravi, A., & Sundar, A. (2024). The constitutional case against state-controlled fact-checking: A case comment on Kunal Kamra v. Union of India. *National Law School of India Review*, *36*(2), Article 1.

review by a secretary-level officer to audit all intimations (MeitY, 2025)[63]. The amendment was the statutory formalisation of the Sahyog portal, the mass-scale takedown infrastructure operated by the I4C under the MHA that had already processed bulk takedowns (Gupta & Pahwa, 2026)[64]. The Sahyog portal's capacity for administrative overreach had been demonstrated when railway officials used it in early 2025 to issue takedown orders suppressing videos and news reports documenting a station stampede (Agrawal, 2025[65]; IFF, 2025[66]). The significance of the amendment is considerable. It expanded the definition of "actual knowledge" under Section 79(3)(b) to include reasoned intimations transmitted through Sahyog. The amendment created a permanent secondary pathway for content removal operating outside the transparency requirements. Speech can now be erased at mass scale, without notification to the affected user. Moreover, any removal directive is audited by a Secretary-level officer from the same department that originally requested the takedown, transforming a single department into its own judge and jury (IFF, 2025)[67]. The Schmittian exception becomes visible. The sovereign is deciding what constitutes the exception from within the very structure whose exception it declares.

5.2 The February 2026 Amendment and the Logic of the Technological Emergency:

The February 2026 amendment introduced the most stringent content removal timelines in India's regulatory history. Intermediaries must now remove unlawful synthetic content within three hours of receiving an order; for content involving nudity or impersonation, the window is reduced to two hours (MeitY, 2026b)[68]. The government invoked the full vocabulary of technological emergency: rapid advances in AI rendering synthetic media indistinguishable from authentic content, threats to electoral integrity, documented use of deepfakes for financial fraud, and the special vulnerability of women and children to AI-generated abuse (Verma & Wahi, 2026)[69]. Each element performs a specific rhetorical function. "Rapid advances in AI" construct unprecedented novelty that places the problem beyond existing legal frameworks, establishing the situation's exceptionality. The reference to women and children invokes the most powerful justification for state intervention, activating protective instincts difficult to argue

[63] Ministry of Electronics and Information Technology. (2025, October 22). *Explanatory note: Proposed amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 in relation to synthetically generated information*. Government of India.

[64] Gupta, A., & Pahwa, N. (2026, April 12). *The rise of infrastructure for digital censorship*. Internet Freedom Foundation.

[65] Agrawal, A. (2025, February 21). *Remove videos of station stampede: Rlys notice to X*. Hindustan Times.

[66] Internet Freedom Foundation. (2025, October 23). IFF's statement on the Sahyog Rules, 2025.

[67] See no. 70.

[68] Ministry of Electronics and Information Technology. (2026b, February 10). Frequently asked questions on the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 (Version 1.0). Government of India.

[69] Verma, G., & Wahi, M. (2026, April 15). *Deepfakes, due diligence and the Good Samaritan paradox: How India's 2026 IT Amendment Rules resolve global platform liability debate*. LiveLaw.

against. The electoral integrity argument frames opposition to the provision as opposition to democracy itself. The rhetorical moves accomplish what Agamben identifies as the precondition for the normalised state of exception: the continuous production of a sense of emergency that makes extraordinary measures seem necessary and reasonable (Agamben, 2005)[70].

Comparative regulatory literature makes clear how extraordinary India's approach is. An analysis of deepfake regulation across jurisdictions demonstrates that balancing harm prevention with creative and political expression requires definitional precision, human review, and proportionality analysis (Van der Sloot & Wagensveld, 2022)[71]. Even the EU AI Act's deepfake provisions include explicit carve-outs for satire, parody, artistic expression, and journalism (Moreno, 2024)[72]. India's rules contain no such protections. Rule 3(3)(a)(i) categorically prohibits any synthetic information creating a "false document or false electronic record." The standards are so broad that they capture anything from AI-assisted political commentary to satirical impersonation (NewsClick Report, 2026)[73]. Three hours is not a window for due process. It is a window for automated compliance without the possibility of human review, contextual analysis, or proportionality assessment. The force of executive law operating without its form, sovereign power over digital speech exercised instantaneously, invisibly, and beyond meaningful challenge (McQuillan, 2015)[74]. Platforms inevitably resort to automated over-removal to avoid losing safe harbour protection, creating what advocates describe as a "prior restraint regime" fundamentally incompatible with the freedom of expression under Article 19(1)(a) of the Constitution (Lakra, 2026)[75]. Rule 3(1)(ca)(ii)(III) introduces a further dimension extending digital bare life beyond the expressive to the personal. It mandates that platforms disclose user identities to complainants who claim to be victims (MeitY, 2026a)[76]. This strips digital subjects of anonymity protection that is critical precisely for political dissidents, human rights workers, and journalists using AI-generated avatars or voice modifications to conceal their identities from actors who would use disclosed personal information to locate, harass, or silence them. The amendment creates the digital homo sacer: the user whose identity can be exposed without any of the procedural protections that normally mediate between citizen and sovereign.

[70] See no. 5.
[71] Van Der Sloot, B., & Wagensveld, Y. (2022). Deepfakes: regulatory challenges for the synthetic society. *Computer Law & Security Review*, *46*, 105716.
[72] Moreno, F. R. (2024). Generative AI and deepfakes: a human rights approach to tackling harmful content. *International Review of Law Computers & Technology*, *38*(3), 297–326.
[73] News Click Report. (2026, February 11). *New IT Rules violate digital rights, undermine constitutional protection for users: IFF*. News Click.
[74] See no. 38.
[75] Lakra, R. (2026, April 23). Decoding the amendments to India's IT Rules: Further on the road to control. *The India Forum*.
[76] Ministry of Electronics and Information Technology. (2026a). *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021: Updated as on 10.02.2026*. Government of India.

5.3. The March 2026 Draft Proposals: Universalizing the Exception:

The March 2026 draft proposals represent the extension of the exception from institutional publishers to every person sharing news-related content on social media. The proposed amendment to Rule 8(1) would classify individual social media accounts sharing "news and current affairs content" as publishers subject to the full Code of Ethics framework previously applicable only to professional news organisations (MeitY, 2026c)[77]. An Instagram post about a local protest, a Twitter thread about a government scheme, and a podcast discussing political events could all be classified as publisher content. Individual creators, lacking institutional resources, legal departments, or financial capacity to navigate the state machinery, would be subjected to oversight designed for established media houses.

The proposed Rule 3(4) closes the accountability loop by giving government guidance documents the practical force of binding law (MeitY, 2026d)[78]. This accomplishes what the FCU sought. The executive branch's informal communications become, through the conduit of conditional immunity, the effective law of digital speech. The incentive structure is irresistible. Platforms that comply with ministerial directives retain their protection; those who insist on due process face liability for all user content across services with hundreds of millions of users. The conduct of digital conduct is achieved, at scale and without visibility, through the architecture of compliance itself. Further, the proposed expansion of the IDC's mandate under Rule 14(2) to include "matters referred to it by the Ministry" transforms the committee from a grievance resolution body into a proactive surveillance and censorship mechanism, capable of initiating scrutiny of any content or publisher at ministerial direction (IFF, 2026)[79].

6. Conclusion:

The regulatory sequence from IT Rules 2021 to the March 2026 draft proposals follows a single cumulative structural logic. Each instrument — the three-tier grievance redressal mechanism, the Sahyog portal formalisation, the deepfake regulations, the proposed extension of publisher oversight to individual users — extends an underlying architecture: the algorithmic camp, a zone in which the categorical distinction between the legally protected and the legally abandoned has been dissolved into sovereign discretion. When a platform can be compelled to remove content within three hours without human review, when a user's identity can be disclosed to a private

[77] Ministry of Electronics and Information Technology. (2026c, March 30). Notice: Inviting feedback/comments of stakeholders on the draft amendments to Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 [Public notice]. Government of India.

[78] Ministry of Electronics and Information Technology. (2026d, March 30). Draft Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Second Amendment Rules, 2026 [Draft notification]. Government of India.

[79] Internet Freedom Foundation. (2026, April 6). *IFF's comments on the MeitY's proposed amendments to the 2021 IT Rules*.

complainant without a court order, and when ministerial advisories acquire the practical force of binding law through conditional immunity, the procedural architecture that gives law its legitimating character in a constitutional democracy has been structurally bypassed. The reason behind calling it an algorithmic camp, not a simple digital camp, is a bit nuanced. As the intermediaries are forced to follow blocking orders instantly and flag content, it becomes a task of automation, which alters the previous operating algorithms. The algorithms automate the exclusion process to protect the safe harbour shield. Similarly, the concept emphasizes how data structures, data mining, and machine learning accelerate the use of predictive models to identify 'harmful content' in advance (McQuillan, 2015)[80].

The subordinate position of Rules in democratic governance deserves emphasis. Rules are delegated instruments issued by the executive without parliamentary debate, yet they carry the force of statute. This is precisely why they are the preferred instrument of a state seeking to govern digital speech without submitting that governance to constitutional scrutiny. What makes the Indian case theoretically significant is that these Rules do not merely supplement the law; they override it. This is the decoupling of the "force of law" from its "form" that Agamben's concept of the state of exception describes. The three logics of digital governmentality, identified by Badouard, Mabi, and Sire (2016)[81], explain how power operates within this zone. The directing logic works through conditional safe harbour immunity. The constraining logic operates through the systematic dismantling of the technical conditions under which protected speech can occur. The traceability mandate and the identity disclosure provision eliminate the possibility of anonymous dissent. The framing logic operates through definitional categories. The executive now possesses the sole authority to define what counts as "unlawful synthetic content," "false information about government business," and "news and current affairs content." Together, these three logics produce the condition of digital bare life. Studies focusing on India's internet governance in Kashmir show that the logic of the exception, the differentiation between citizens entitled to full communicative rights and populations subjected to surveillance and disconnection, has long been operative in India's peripheral regions (Parray, 2021[82]; Peerzada et al., 2025[83]). IT Rules 2021 and its subsequent amendments are instruments through which the exception is normalised from the periphery to the mainland. The algorithmic camp is built through individually defensible administrative steps whose cumulative structural effect is visible only when the entire sequence is analysed as a whole.

[80] See no. 38.
[81] See no. 43.
[82] Parray, M. I. (2021). Choking the 'periphery': Pride and prejudice in India's globalizing internet imaginary. *InternetHistories*, 5(3–4), 355–378.
[83] See no. 54.

However, the ongoing project is neither complete nor irreversible. The Bombay High Court's invalidation of the Fact-Check Unit amendment demonstrates that constitutional limits remain operative. The exception has not yet fully absorbed the norm, and judicial institutions retain the capacity to recognise and resist sovereign overreach. The IFF's detailed tracking of Sahyog portal misuse (IFF, 2025)[84], journalist bodies' coordinated opposition to the March 2026 proposals (Maktoob, 2026)[85], and platform companies' disclosure of government takedown demands in court battles (Bhatia, 2026)[86] are not peripheral responses but central democratic practices through which the exception is made visible and thereby contestable.

References:

Abhishek, A. (2023). The state deputizing citizens to discipline digital news media: The case of the IT Rules 2021 in India. *Digital Journalism*, 11(10), 1769–1787. https://doi.org/10.1080/21670811.2022.2134163

Access Now. (2024, May 15). *India leads the world internet shutdown count for sixth year*. https://www.accessnow.org/press-release/india-keepiton-internet-shutdowns-2023-en/

Agamben, G. (1998). *Homo sacer: Sovereign power and bare life* (D. Heller-Roazen, Trans.). Stanford University Press. (Original work published 1995)

Agamben, G. (2005). *State of exception* (K. Attell, Trans.). University of Chicago Press. (Original work published 2003)

Agrawal, A. (2025, February 21). *Remove videos of station stampede: Rlys notice to X*. Hindustan Times.

Arendt, H. (1963). *On revolution*. The Viking Press.

Avnish Bajaj v. State (NCT) of Delhi, 150 DLT 769 (Del. HC 2008).

Badouard, R., Mabi, C., & Sire, G. (2016). Beyond "Points of Control": logics of digital governmentality. *Internet Policy Review*, *5*(3). https://doi.org/10.14763/2016.3.433

Balendra, S. (2024). *Free speech in the puzzle of content regulation: Insights from the West and the Global South*. Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-031-75813-3

Banaji, S. (2018). Vigilante publics: Orientalism, modernity and Hindutva fascism in India. *Javnost – The Public, 25*(4), 333–350. https://doi.org/10.1080/13183222.2018.1463349

Banerjee, A. (2021). Internet censorship in India: The law and beyond. In S. K. Sandeen, C. Rademacher, & A. Ohly (Eds.), *Research Handbook on Information Law and Governance* (pp. 339–355). Edward Elgar Publishing. https://doi.org/10.4337/9781785363962

Bapat, K., Jain, A., Gupta, A., & Singh, T. (2021, February 27). *How the intermediaries rules are anti-democratic and unconstitutional*. Internet Freedom Foundation. https://internetfreedom.in/how-the-intermediaries-rules-are-anti-democratic-and-unconstitutional/

Basu, S., & Sen, S. (2023). Silenced voices: Unravelling India's dissent crisis through historical and contemporary analysis of free speech and suppression. *Information & Communications Technology Law*, 33(1), 42–65. https://doi.org/10.1080/13600834.2023.2249780

Benjamin, W. (1968). *Theses on the philosophy of history*. In H. Arendt (Ed.), Illuminations (H. Zohn, Trans.) (pp. 253–264). Schocken Books. (Original work published 1940)

Bhatia, G. (2025). Disinformation, misinformation and democracy: An Indian constitutional perspective. In R. J. Krotoszynski Jr., A. Koltay, & C. Garden (Eds.), *Disinformation, misinformation, and democracy: Legal approaches in comparative context* (pp. 258–269). Cambridge University Press.

[84] See no. 69.

[85] Maktoob. (2026, April 12). *Journalist bodies demand withdrawal of Draft IT Rules 2026, warn of censorship and chilling effect*. Maktoob Media.

[86] Bhatia, S. (2026, April 14). *Full text | The building of a censorship infrastructure* [Interview transcript]. The Wire.

Bhatia, S. (2026, April 14). *Full text | The building of a censorship infrastructure* [Interview transcript]. The Wire. https://thewire.in/rights/full-text-the-building-of-a-censorship-infrastructure

Foucault, M. (1991). Governmentality (C. Gordon, Trans.). In G. Burchell, C. Gordon, & P. Miller (Eds.), *The Foucault*

effect: Studies in governmentality (pp. 87–104). University of Chicago Press.

Foucault, M. (2007). Security, territory, population: Lectures at the Collège de France, 1977–1978 (G. Burchell, Trans.). Palgrave Macmillan.

Gheytasi, S., Khoshnood, A., & Sohrabzadeh, A. (2026). Bare life in the digital age: Homo sacer, necropolitics, and algorithmic control in the selected contemporary fiction. *3L: Language, Linguistics, Literature, 32*(1), 157–171. https://doi.org/10.17576/3L-2026-3201-10

Gupta, A., & Pahwa, N. (2026, April 12). *The rise of infrastructure for digital censorship*. Internet Freedom Foundation. https://internetfreedom.in/the-rise-of-infrastructure-for-digital-censorship/

Gupta, I., & Srinivasan, L. (2023). Evolving scope of intermediary liability in India. *International Review of Law, Computers & Technology*, 37(1), 1–23. https://doi.org/10.1080/13600869.2022.2164838

Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, 2009 (India).

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (India). https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf

Internet Freedom Foundation. (2025, October 23). IFF's statement on the Sahyog Rules, 2025. https://internetfreedom.in/iffs-statement-on-the-sahyog-rules-2025/

Internet Freedom Foundation. (2026, April 6). *IFF's comments on the MeitY's proposed amendments to the 2021 IT Rules*. https://internetfreedom.in/iffs-comments-on-the-meitys-proposed-amendments-to-the-2021-it-rules/

Karanicolas, M. (2021). Authoritarianism as a service: India's moves to weaponize private sector content moderation with the 2021 Information Technology Rules. *Indian Journal of Law and Technology*, 17(2), Article 4. https://doi.org/10.55496/VBGQ9491

Katkuri, S. (2024). Need of encryption legislation: Protecting India's digital realm and beyond. *Indian Journal of Public Administration*, 70(3), 562–578. https://doi.org/10.1177/00195561241271590

Lakra, R. (2026b, April 23). Decoding the amendments to India's IT Rules: Further on the road to control. *The India Forum*. https://www.theindiaforum.in/law/decoding-indias-it-rules-amendments

Maktoob. (2026, April 12). *Journalist bodies demand withdrawal of Draft IT Rules 2026, warn of censorship and chilling effect*. Maktoob Media.

Manokha, I. (2018). Surveillance, Panopticism, and Self-Discipline in the digital age. *Surveillance & Society*, *16*(2), 219–237. https://doi.org/10.24908/ss.v16i2.8346

McQuillan, D. (2015). Algorithmic states of exception. *European Journal of Cultural Studies*, 18(4–5), 564–576. https://doi.org/10.1177/1367549415577389

Mehta, S. N., & Amit-Danhi, E. R. (2025). The road to censorship: The case of digital audiovisual industries in India. *International Journal of Cultural Policy*, 31(7), 881–897. https://doi.org/10.1080/10286632.2024.2402257

Ministry of Electronics and Information Technology. (2025a, October 22). *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2025* (Notification No. G.S.R. 775(E)). The Gazette of India.

Ministry of Electronics and Information Technology. (2025b, October 22). *Explanatory note: Proposed amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 in relation to synthetically generated information*. Government of India.

Ministry of Electronics and Information Technology. (2026a). *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021: Updated as on 10.02.2026*. Government of India.

Ministry of Electronics and Information Technology. (2026b, February 10). Frequently asked questions on the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 (Version 1.0). Government of India. https://www.meity.gov.in/static/uploads/2026/02/RAQ_IT_Rules_amendment_2026_February.pdf

Ministry of Electronics and Information Technology. (2026c, March 30). Notice: Inviting feedback/comments of stakeholders on the draft amendments to Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 [Public notice]. Government of India.

Ministry of Electronics and Information Technology. (2026d, March 30). Draft Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Second Amendment Rules, 2026 [Draft notification]. Government of India.

Ministry of Home Affairs. (2026). *Annual report 2024–2025*. Government of India.

Moreno, F. R. (2024). Generative AI and deepfakes: a human rights approach to tackling harmful content. *International Review of Law Computers & Technology*, *38*(3), 297–326. https://doi.org/10.1080/13600869.2024.2324540

Nagarathna, A. (2022). The State's access to data and internet intermediary response – an assessment of India's attempt to reallocate the legal framework to ensure national security. *International Review of Law, Computers & Technology*, 36(3), 404–430. https://doi.org/10.1080/13600869.2022.2030038

Narrain, S. (2018). Social media, violence and the law: "Objectionable material" and the changing contours of hate speech regulation in India. *Culture Unbound*, *10*(3), 388–404. https://doi.org/10.3384/cu.2000.1525.18103388

Nayak, N. (2021). Legalizing executive control: On the law of online journalism in India. *Indian Law Review*, 8(1), 20–41. https://doi.org/10.1080/24730580.2023.2266979

Neal, A. (2012). Normalization and legislative exceptionalism: Counterterrorist lawmaking and the changing times of security emergencies. *International Political Sociology,* 6(3), 260–276.

Neocleous, M. (2006). The problem with normality: Taking exception to 'permanent emergency'. Alternatives: *Global, Local, Political*, 31(2), 191–213.

NewsClick Report. (2026, February 11). *New IT Rules violate digital rights, undermine constitutional protection for users: IFF*. NewsClick.

Nojeim, G., Maheshwari, N., & Miglani, E. (2021). Encryption in India: Preserving the online engine of privacy, free expression, security, and economic growth. *Indian Journal of Law and Technology*, 17(1), Article 2. https://doi.org/10.55496/LPNZ6069

Parray, M. I. (2021). Choking the 'periphery': Pride and prejudice in India's globalizing internet imaginary. *Internet Histories*, 5(3–4), 355–378. https://doi.org/10.1080/24701475.2021.1984732

Peerzada, R. A., Sharma, A. P., & Kannan, S. (2025). The jurisprudence of digital blackouts: Law and its exceptions in Jammu and Kashmir. *Human Geography*. https://doi.org/10.1177/19427786251389340

Press Information Bureau. (2021, February 25). Union ministers Prakash Javadekar and Ravi Shankar Prasad address a press conference. https://www.youtube.com/watch?v=H0eqWuj84-0

Rai, S. (2024). Between the divine and digital: Parsing Modi's charismatic avatar. *Media, Culture & Society*, *46*(4), 834–850. https://doi.org/10.1177/01634437231214200

Reporters Without Borders. (2026). *India*. In *2026 World Press Freedom Index*.

Ravi, A., & Sundar, A. (2024). The constitutional case against state-controlled fact-checking: A case comment on Kunal Kamra v. Union of India. *National Law School of India Review*, *36*(2), Article 1. https://doi.org/10.55496/YVEW3627

Sahoo, S. (2023). India's internet shutdowns as biopolitics: The formation of political will and opinion through collective action under attack. *Critical Studies in Media Communication*, *40*(5), 291–305. https://doi.org/10.1080/15295036.2023.2265995

Schmitt, C. (1985). *Political theology: Four chapters on the concept of sovereignty* (G. Schwab, Trans.). MIT Press. (Original work published 1922)

Sharma, S. (2026). Algorithmic censorship and shadow banning: Legal blind spots in India's digital speech regime. Zenodo. https://doi.org/10.5281/zenodo.18350717

Shreya Singhal v. Union of India, Writ Petition (Criminal) No. 167 of 2012, Supreme Court of India. (2015). https://indiankanoon.org/doc/110813550/

Standing Committee on Science and Technology, Environment and Forests. (1999). *79th report on the Information Technology Bill, 1999*.

Sweet, A. S., & Mathews, J. (2019). *Proportionality balancing and constitutional governance: A Comparative and Global Approach*. Oxford University Press.

The Wire. (2026, March 27). *MHA took down 290 posts per day in 2024–25, on an average: Ministry data*.

Uppaluri, U. (2012). *Constitutional analysis of the Information Technology (Intermediaries' Guidelines) Rules, 2011*. Centre for Internet and Society. https://cis-india.org/internet-governance/constitutional-analysis-of-intermediaries-guidelines-rules

Van Der Sloot, B., & Wagensveld, Y. (2022). Deepfakes: regulatory challenges for the synthetic society. *Computer Law & Security Review*, *46*, 105716. https://doi.org/10.1016/j.clsr.2022.105716

Verma, G., & Wahi, M. (2026, April 15). *Deepfakes, due diligence and the Good Samaritan paradox: How India's 2026 IT Amendment Rules resolve global platform liability debate*. LiveLaw. https://www.livelaw.in/law-firms/law-firm-articles-/deepfakes-due-diligence-and-the-good-samaritan-paradox-how-indias-2026-it-amendment-rules-resolve-global-platform-liability-debate-530344

Wadhwa, S. (2025). Content blocking orders and status of digital rights: Assessment of two key verdicts in India. Information & Communications Technology Law, 34(1), 44–61. https://doi.org/10.1080/13600834.2024.2406678