



Digital Arrest & Police Surveillance in India: Constitutional Limits and Legal Accountability

Dr. Santosh Kumar

B.Sc. (Maths), LL.M., NET, JRF, SRF, Ph.D. (Law)

ARTICLE DETAILS

Research Paper

Keywords :

*Digital Arrest; Police
Surveillance; Right to
Privacy; Article 21;
Criminal Procedure in
India; Constitutional
Accountability*

ABSTRACT

The rapid digitisation of policing practices in India has significantly altered traditional notions of arrest, surveillance, and criminal investigation. The emergence of practices such as real-time digital monitoring, remote surveillance, mobile phone tracking, and coercive online intimidation—often described colloquially as “digital arrest”—has raised serious constitutional concerns. While technological tools have enhanced investigative efficiency, their deployment has largely outpaced the development of clear legal safeguards, judicial oversight, and accountability mechanisms.

This paper critically examines the concept of digital arrest and police surveillance within the framework of the Indian Constitution, particularly Articles 14, 19, and 21. It argues that existing criminal procedure laws, including the Bharatiya Nagarik Suraksha Sanhita, 2023, inadequately address the constitutional implications of technology-enabled policing. Drawing upon Supreme Court jurisprudence on privacy, due process, and proportionality, the study highlights the growing tension between state security imperatives and individual liberties.

The paper further contends that the absence of a rights-based regulatory framework governing digital surveillance risks normalising arbitrary state action and eroding procedural safeguards. By adopting a doctrinal and analytical methodology, this research proposes a constitutional



accountability model that reconciles technological advancement with fundamental rights protection. The study concludes that without explicit legislative standards, transparent oversight, and effective remedies, digital arrest practices threaten to undermine the rule of law in contemporary India.

1. Introduction

The relationship between policing and personal liberty has historically been mediated through constitutional guarantees, statutory procedures, and judicial oversight. In India, the law of arrest and investigation has traditionally been governed by clearly articulated procedural norms, physical custody requirements, and judicial supervision. However, the rapid integration of digital technologies into policing practices has fundamentally transformed this relationship. Contemporary law enforcement increasingly relies on tools such as mobile phone tracking, real-time location surveillance, digital summons, online interrogation, and data extraction from personal devices. These practices have collectively given rise to what is increasingly described as “digital arrest”—a phenomenon where individuals experience restraint, coercion, or control without formal physical detention.

Unlike conventional arrest, digital arrest does not always involve bodily confinement. Instead, it manifests through continuous surveillance, compelled digital presence, restrictions on movement through monitoring, and psychological coercion exercised via electronic communication. While such practices are often justified in the name of efficiency, national security, or crime prevention, they raise serious constitutional questions concerning personal liberty, privacy, and due process.

The Indian constitutional framework, particularly Articles 14, 19, and 21, mandates that any deprivation of liberty must be just, fair, and reasonable. Judicial interpretations have consistently emphasised that procedural safeguards are not mere technicalities but essential components of the rule of law. Yet, digital policing practices often operate in legal grey zones, where statutory authorisation is ambiguous and judicial oversight is minimal. This disconnect between technological capability and constitutional control presents a pressing legal challenge.

This paper seeks to examine whether existing constitutional and statutory safeguards are adequate to regulate digital arrest and police surveillance in India. It argues that the absence of a clear legal framework governing digital restraint enables arbitrary state action and undermines constitutional accountability. By analysing judicial trends, statutory developments, and constitutional doctrines, the study aims to propose



a principled framework for regulating technology-driven policing within the bounds of constitutional legality.

2. Conceptualising “Digital Arrest”: Meaning and Scope

The term “digital arrest” does not currently find explicit recognition in Indian statutory law. Nevertheless, its growing usage reflects a set of practices that functionally resemble arrest without conforming to its formal legal definition. Traditionally, arrest has been understood as the physical apprehension of a person by lawful authority, accompanied by restraint on liberty. Digital arrest departs from this classical understanding by substituting physical restraint with technological control.

Digital arrest may be understood as a situation where law enforcement authorities, through digital means, exercise continuous control or coercion over an individual, thereby substantially restricting their autonomy. This may include compulsory participation in online interrogation, continuous tracking through mobile devices, coercive digital communication threatening legal consequences, or restrictions imposed through surveillance technologies that effectively immobilise the individual’s freedom of movement.

Such practices blur the distinction between investigation and detention. While criminal procedure laws permit certain investigative actions short of arrest, digital surveillance often operates without clear thresholds, safeguards, or accountability. The absence of physical custody further complicates legal scrutiny, as traditional procedural protections associated with arrest—such as production before a magistrate—are often bypassed.

The conceptual ambiguity surrounding digital arrest allows it to function outside established constitutional controls. This raises a fundamental question: can deprivation of liberty occur without physical detention, and if so, what constitutional standards govern such deprivation? Addressing this question requires re-examining arrest not merely as a physical act but as a constitutional event involving the restriction of personal liberty.

3. Constitutional Framework Governing Arrest and Surveillance in India

3.1 Article 21 and the Right to Personal Liberty

Article 21 of the Indian Constitution guarantees that no person shall be deprived of life or personal liberty except according to procedure established by law. Judicial interpretation has transformed this provision from a narrow procedural guarantee into a substantive safeguard against arbitrary state action. The requirement that procedure must be just, fair, and reasonable has become a cornerstone of Indian constitutional jurisprudence.



Digital arrest practices directly implicate Article 21, as continuous surveillance and coercive digital control can significantly impair personal liberty. The absence of explicit statutory authorisation for such practices raises serious concerns regarding the legality of the procedure employed. Where liberty is curtailed without a clear legal basis, the constitutional mandate of Article 21 stands violated.

3.2 Article 14 and Arbitrary State Action

Article 14 prohibits arbitrary and discriminatory state action. Digital policing practices often lack uniform standards, leading to selective application and discretionary abuse. Without clear guidelines governing when and how digital surveillance may be employed, law enforcement agencies enjoy wide discretion, increasing the risk of arbitrariness.

The unequal impact of digital surveillance on marginalised communities further aggravates Article 14 concerns. Individuals lacking digital literacy or access to legal remedies are particularly vulnerable to coercive online policing practices.

3.3 Article 19 and Chilling Effect on Freedoms

Continuous digital surveillance can have a chilling effect on freedoms guaranteed under Article 19, particularly freedom of speech and movement. When individuals are aware that their digital activities are being monitored, they may self-censor or restrict lawful expression, thereby undermining democratic participation.

4. Research Gap and Objectives

While existing scholarship has extensively examined police powers, arrest procedures, and surveillance laws in isolation, limited attention has been paid to the emerging phenomenon of digital arrest as a distinct constitutional issue. Most studies focus either on traditional arrest jurisprudence or on data protection and privacy without integrating these strands into a comprehensive analysis of technology-enabled coercive policing.

This paper seeks to fill this gap by:

Conceptually defining digital arrest within constitutional jurisprudence

Examining the adequacy of existing legal frameworks governing police surveillance

Analysing judicial responses to technology-driven policing practices

Proposing a constitutional accountability framework for regulating digital arrest



5. Judicial Jurisprudence on Surveillance and Personal Liberty in India

Judicial interpretation has played a pivotal role in shaping the constitutional contours of arrest, surveillance, and personal liberty in India. Although Indian courts have not explicitly used the term “digital arrest,” their jurisprudence on privacy, surveillance, and procedural safeguards provides critical doctrinal tools to assess technology-enabled policing practices. The evolution of judicial reasoning reflects a gradual recognition that liberty can be curtailed not only through physical detention but also through indirect and non-physical forms of state control.

5.1 Early Judicial Approach to Surveillance

In its early phase, Indian jurisprudence exhibited a relatively deferential attitude towards state surveillance. Judicial scrutiny was largely confined to whether surveillance measures complied with statutory authorisation, with limited engagement with broader constitutional values. Surveillance was often viewed as an extension of executive power necessary for maintaining public order and national security.

However, this approach failed to adequately address the intrusive potential of emerging technologies. Surveillance measures such as phone tapping, postal interception, and shadowing were assessed primarily on procedural grounds, without recognising their cumulative impact on dignity, autonomy, and psychological freedom. This narrow conception of liberty allowed surveillance practices to operate with minimal constitutional resistance.

5.2 Expansion of Article 21 and the Substantive Due Process Doctrine

A significant transformation occurred with the judicial expansion of Article 21, wherein the Supreme Court held that “procedure established by law” must be just, fair, and reasonable. This doctrinal shift marked the incorporation of substantive due process into Indian constitutional law. Liberty was no longer confined to freedom from physical restraint but encompassed a broader spectrum of human autonomy.

This expanded interpretation is crucial for evaluating digital arrest practices. Continuous digital monitoring, compelled online engagement with law enforcement, and coercive electronic communication may not involve physical custody, yet they substantially interfere with an individual’s freedom to act, think, and communicate autonomously. Such interference, when not backed by a fair and reasonable procedure, falls foul of Article 21.



5.3 Right to Privacy and Informational Autonomy

The judicial recognition of privacy as a fundamental right represents a watershed moment in Indian constitutional jurisprudence. Privacy was conceptualised not merely as spatial seclusion but as informational autonomy and decisional freedom. The court acknowledged that unchecked state access to personal data and digital footprints poses a serious threat to individual liberty.

This recognition has direct implications for police surveillance. Digital arrest practices often rely on real-time data extraction, location tracking, metadata analysis, and behavioural profiling. When such measures are deployed without clear statutory limits or judicial oversight, they violate the core of informational privacy. The absence of transparency further exacerbates the harm, as individuals are frequently unaware of the extent and duration of surveillance imposed upon them.

5.4 Proportionality as a Constitutional Test

The proportionality doctrine has emerged as a central tool for assessing the constitutionality of rights restrictions. Under this doctrine, any limitation on fundamental rights must satisfy four requirements: legitimate aim, rational connection, necessity, and proportionality in the strict sense. Surveillance measures must therefore be narrowly tailored and must not impose excessive burdens on individual liberty.

Digital arrest practices frequently fail this test. Broad and continuous surveillance, often justified on vague grounds such as “investigative necessity,” lacks demonstrable necessity and fails to consider less intrusive alternatives. The absence of sunset clauses, periodic review, and independent oversight further undermines proportionality. As a result, digital policing risks becoming a tool of convenience rather than a constitutionally justified measure.

6. Statutory Framework Governing Police Surveillance and Arrest

6.1 Criminal Procedure Laws and Their Limitations

Indian criminal procedure law traditionally regulates arrest, search, and investigation through detailed provisions designed to prevent abuse of power. These safeguards include requirements such as reasonable suspicion, recording of reasons, and judicial oversight. However, these provisions were primarily crafted in an era of physical policing and do not adequately account for digital forms of restraint.

The Bharatiya Nagarik Suraksha Sanhita, 2023, while introducing certain reforms, does not comprehensively address the constitutional implications of digital surveillance. The law remains largely silent on issues such as continuous electronic monitoring, remote interrogation, and coercive digital

communication. This silence effectively creates a legal vacuum, allowing executive practices to evolve without legislative guidance.

6.2 Surveillance Laws and Executive Discretion

Existing surveillance laws in India grant broad powers to the executive to intercept communications and collect data in the interest of public safety and national security. While these laws contain procedural requirements, their implementation often lacks transparency and accountability. Judicial review is typically limited and occurs ex post facto, reducing its effectiveness as a safeguard.

Digital arrest practices often operate at the intersection of criminal procedure and surveillance law, exploiting ambiguities in both domains. By framing coercive digital measures as “investigative tools” rather than as restraints on liberty, law enforcement agencies circumvent the procedural protections traditionally associated with arrest.

7. Digital Arrest as a Form of Indirect Deprivation of Liberty

The constitutional understanding of liberty must evolve to recognise indirect forms of deprivation. Digital arrest exemplifies a situation where the cumulative effect of surveillance, coercion, and control produces a restraint on liberty comparable to physical detention. The absence of bodily confinement does not diminish the severity of constitutional infringement.

From a constitutional perspective, any state action that substantially restricts an individual’s autonomy must be subjected to strict scrutiny. Digital arrest, by imposing continuous psychological pressure and restricting freedom of movement and expression, meets this threshold. Treating such practices as mere investigative conveniences undermines the spirit of constitutional safeguards.

8. Need for a Re-Conceptualisation of Arrest in the Digital Age

The traditional legal conception of arrest as physical custody is increasingly inadequate in the digital age. A rights-based approach requires recognising arrest as any state action that effectively restrains liberty, regardless of its form. This reconceptualisation is essential to ensure that constitutional protections remain meaningful in the face of technological change.

By expanding the legal understanding of arrest to include digital restraint, courts and legislatures can restore the balance between state power and individual rights. Such an approach would ensure that procedural safeguards, judicial oversight, and accountability mechanisms apply equally to both physical and digital forms of policing.



9. Constitutional Accountability of Police in the Era of Digital Policing

Accountability constitutes the foundational principle that legitimises the exercise of state power in a constitutional democracy. In the context of policing, accountability operates as a safeguard against abuse, arbitrariness, and excess. The advent of digital policing, however, has significantly weakened traditional accountability mechanisms by enabling surveillance and coercion to function invisibly and remotely.

Digital arrest practices pose a unique challenge to constitutional accountability because they frequently escape the formal triggers that activate oversight. Physical arrest ordinarily leads to mandatory documentation, production before a magistrate, and judicial scrutiny. In contrast, digital restraint—through constant monitoring, coercive electronic communication, or remote control—often leaves no visible trail and no immediate opportunity for legal challenge. This structural invisibility allows power to be exercised without responsibility.

From a constitutional standpoint, such unchecked authority undermines the rule of law. Accountability is not merely a procedural requirement but a substantive guarantee that ensures power is exercised for lawful purposes and within constitutional limits. The absence of accountability mechanisms in digital policing therefore represents a serious constitutional deficit.

10. Police Discretion, Technology, and the Risk of Arbitrariness

Discretion is an inherent feature of policing, but constitutional law demands that discretion be structured, guided, and reviewable. Digital technologies, when combined with broad police discretion, significantly amplify the risk of arbitrary action. Surveillance tools enable continuous observation and control without requiring repeated justification, thereby normalising extraordinary measures as routine practices.

The risk of arbitrariness is further heightened by the absence of clear legal thresholds governing digital surveillance. Terms such as “investigative necessity” or “security interest” are frequently invoked without precise definition, allowing subjective interpretation by law enforcement authorities. This creates a fertile ground for selective enforcement and discriminatory targeting.

Article 14 of the Constitution mandates that state action must be non-arbitrary and based on intelligible criteria. Digital arrest practices that operate without objective standards or transparent procedures fail to meet this constitutional requirement. The concentration of unchecked discretion in the hands of law enforcement agencies erodes public trust and weakens democratic accountability.



11. Absence of Effective Remedies and Judicial Oversight

An essential component of constitutional governance is the availability of effective remedies against rights violations. In cases of physical arrest, remedies such as habeas corpus, bail, and judicial review provide immediate relief. Digital arrest, however, often deprives individuals of the opportunity to seek timely redress.

Victims of digital surveillance may not even be aware that their liberty is being curtailed. The covert nature of digital monitoring makes it difficult to establish standing, gather evidence, or demonstrate harm. Even when individuals suspect surveillance, the lack of transparency prevents meaningful legal challenge. Judicial oversight, where it exists, is often *ex post facto* and limited in scope. Courts are typically presented with surveillance-related disputes after the damage to privacy and liberty has already occurred. The absence of prior judicial authorisation for many digital policing practices further weakens constitutional safeguards.

12. Comparative Constitutional Perspectives on Surveillance and Accountability

A comparative examination reveals that constitutional democracies across jurisdictions have grappled with similar challenges posed by digital surveillance. While approaches vary, a common trend is the recognition that technological policing must be accompanied by enhanced safeguards.

In jurisdictions such as the United Kingdom and the European Union, surveillance powers are increasingly subjected to independent oversight, proportionality review, and statutory authorisation. Judicial warrants, independent supervisory bodies, and data protection authorities play a crucial role in ensuring accountability. These mechanisms reflect an understanding that digital surveillance poses systemic risks to liberty and therefore demands stricter controls.

The Indian framework, by contrast, remains fragmented and executive-driven. While constitutional principles provide a strong normative foundation, their translation into enforceable statutory safeguards remains incomplete. The absence of independent oversight institutions dedicated to policing surveillance represents a significant lacuna in India's accountability architecture.

13. Towards a Rights-Based Framework for Regulating Digital Arrest

The regulation of digital arrest requires a fundamental shift from an executive-centric model to a rights-based constitutional framework. Such a framework must recognise that digital restraint constitutes a



serious interference with personal liberty and must therefore be subjected to the same standards as physical arrest.

A rights-based approach would entail clear legislative authorisation for digital surveillance practices, accompanied by narrowly defined purposes and strict procedural safeguards. Judicial oversight must be incorporated at the authorisation stage rather than being confined to post facto review. Transparency measures, including disclosure obligations and audit mechanisms, are essential to prevent abuse.

Furthermore, accountability must extend beyond formal legality to encompass substantive justification. Law enforcement agencies must demonstrate not only that surveillance is lawful but also that it is necessary, proportionate, and least intrusive. This approach aligns with constitutional principles and reinforces public confidence in the legitimacy of policing practices.

14. Normative Foundations: Liberty, Dignity, and the Rule of Law

At a deeper level, the challenge of digital arrest is normative rather than merely technical. It raises fundamental questions about the nature of liberty, dignity, and state power in a digital society. Liberty cannot be reduced to the absence of physical confinement; it encompasses the freedom to act, communicate, and exist without constant state monitoring.

Human dignity, a core constitutional value, is compromised when individuals are subjected to pervasive surveillance without justification or recourse. The normalisation of digital arrest risks transforming citizens into subjects of continuous observation, undermining the democratic promise of autonomy and self-determination.

The rule of law demands that power be exercised transparently, predictably, and accountably. Digital policing practices that operate in legal grey zones threaten to replace rule of law with rule by technology. Addressing this challenge requires reaffirming constitutional values as the guiding principles of technological governance.

15. Proposed Constitutional Accountability Model for Digital Arrest

In order to address the constitutional challenges posed by digital arrest and technology-enabled police surveillance, this paper proposes a structured constitutional accountability model grounded in fundamental rights, rule of law, and democratic oversight. The model is premised on the recognition that digital restraint constitutes a substantive interference with personal liberty and therefore must be regulated with the same rigor as physical arrest.



15.1 Legal Recognition of Digital Arrest

The first step towards accountability is the formal legal recognition of digital arrest as a constitutionally significant event. Legislatures must acknowledge that sustained digital surveillance, coercive online communication, and enforced digital compliance can amount to deprivation of liberty. Such recognition would ensure that constitutional safeguards are triggered whenever digital policing practices cross the threshold of permissible investigation.

15.2 Statutory Authorisation and Clear Thresholds

Digital arrest practices must be grounded in explicit statutory authorisation. Laws governing criminal procedure and surveillance should clearly define the circumstances under which digital monitoring may be employed, the duration for which it may continue, and the safeguards applicable to its use. Vague standards such as “investigative necessity” must be replaced with objective and narrowly tailored criteria to prevent abuse.

15.3 Prior Judicial Oversight

A central component of the proposed model is prior judicial oversight. Any form of continuous digital surveillance or coercive digital control should require authorisation from an independent judicial authority. Such oversight ensures that surveillance measures are subjected to proportionality analysis before being implemented, thereby reducing the risk of arbitrary state action.

15.4 Transparency and Disclosure

Transparency is essential for meaningful accountability. Individuals subjected to digital surveillance should, subject to legitimate security exceptions, be informed of such measures once the purpose of surveillance is fulfilled. Disclosure obligations enable affected persons to seek legal remedies and deter misuse of power.

15.5 Remedies and Institutional Accountability

Effective remedies must be available for violations arising from unlawful digital arrest. Courts should recognise digital restraint as a ground for constitutional remedies, including compensation and exclusion of unlawfully obtained evidence. In addition, independent oversight bodies should be established to audit surveillance practices and ensure compliance with constitutional standards.



16. Legislative and Judicial Reform Proposals

16.1 Reform of Criminal Procedure Laws

Criminal procedure laws must be updated to reflect the realities of digital policing. Provisions governing arrest, investigation, and surveillance should be harmonised to ensure that technological practices do not bypass procedural safeguards. Clear reporting requirements and documentation of digital surveillance activities should be mandated.

16.2 Development of Surveillance-Specific Legislation

India lacks a comprehensive legal framework governing police surveillance in the digital age. Enacting dedicated legislation that balances security interests with constitutional rights would provide clarity and predictability. Such legislation should incorporate principles of necessity, proportionality, and accountability as binding legal standards.

16.3 Judicial Doctrinal Evolution

The judiciary must continue to evolve constitutional doctrine to address indirect forms of liberty deprivation. Courts should adopt a functional approach to arrest, focusing on the effect of state action rather than its form. Recognising digital arrest within Article 21 jurisprudence would strengthen constitutional protections and adapt them to contemporary realities.

17. Synthesis of Findings

This study demonstrates that digital arrest represents a significant constitutional challenge that existing legal frameworks are ill-equipped to address. The absence of clear statutory standards, judicial oversight, and accountability mechanisms allows digital policing practices to operate in a constitutional grey zone. Judicial jurisprudence on privacy and due process provides valuable normative guidance but remains underutilised in regulating everyday policing practices.

The analysis reveals that digital arrest blurs the boundary between investigation and detention, enabling state control without triggering traditional safeguards. Such practices disproportionately affect vulnerable populations and risk normalising arbitrary surveillance. Without a rights-based regulatory framework, technological efficiency threatens to override constitutional legality.

18. Conclusion

The transformation of policing through digital technologies necessitates a corresponding evolution in constitutional law. Digital arrest, though lacking formal legal recognition, has emerged as a tangible reality

that reshapes the relationship between the state and the individual. Treating liberty as contingent upon physical detention alone is no longer sufficient in an era of pervasive digital control.

This paper argues that constitutional accountability must extend to all forms of liberty deprivation, including those effected through technological means. By reconceptualising arrest, strengthening statutory safeguards, and reinforcing judicial oversight, India can ensure that digital policing operates within constitutional limits. Upholding personal liberty, dignity, and the rule of law in the digital age is not merely a legal necessity but a democratic imperative.

Contribution to Knowledge

This research makes three original contributions to constitutional and criminal law scholarship in India: It conceptualises digital arrest as a distinct form of liberty deprivation requiring constitutional scrutiny. It integrates privacy jurisprudence with arrest and surveillance law to develop a unified analytical framework. It proposes a rights-based constitutional accountability model tailored to technology-enabled policing. By addressing a largely under-explored intersection of criminal procedure, surveillance, and constitutional rights, the study advances scholarly understanding and provides a foundation for future legal reform.

References

A. Constitutional & Judicial Sources (India)

Constitution of India (as amended).

Supreme Court of India, *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.

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

Supreme Court of India, *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301.

Supreme Court of India, *Selvi v. State of Karnataka*, (2010) 7 SCC 263.

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

Supreme Court of India, *D.K. Basu v. State of West Bengal*, (1997) 1 SCC 416.

B. Statutes & Legislative Materials

Bharatiya Nagarik Suraksha Sanhita, 2023.

Information Technology Act, 2000.

Ministry of Home Affairs. Telegraph Rules & Interception Guidelines.



C. International & Comparative Judicial Sources

European Court of Human Rights, *Roman Zakharov v. Russia*, (2015) ECHR.

Court of Justice of the European Union, *Digital Rights Ireland Ltd v. Minister for Communications*, (2014).

UK Supreme Court, *R (Davis) v. Secretary of State for the Home Department*, [2015] UKSC 54.

D. Peer-Reviewed Journal Articles (Scopus / WoS Indexed)

Bennett, C. J., & Raab, C. D. (2018). *The governance of privacy: Policy instruments in global perspective*. MIT Press.

De Hert, P., & Gutwirth, S. (2009). Privacy, data protection and law enforcement. *Computer Law & Security Review*, 25(1), 13–24.

(Scopus Indexed)

Richards, N. M. (2013). The dangers of surveillance. *Harvard Law Review*, 126(7), 1934–1965.

(WoS Indexed)

Cohen, J. E. (2012). What privacy is for. *Harvard Law Review*, 126(7), 1904–1933.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3), 477–560.

Lyon, D. (2018). *The culture of surveillance*. Polity Press.

Kuner, C., Bygrave, L., & Docksey, C. (2020). *The EU General Data Protection Regulation (GDPR): A commentary*. Oxford University Press.

E. Indian Academic & Policy Literature

Bhatia, G. (2019). *Offend, shock, or disturb: Free speech under the Indian Constitution*. Oxford University Press.

Sathe, S. P. (2017). *Judicial activism in India: Transgressing borders and enforcing limits*. Oxford University Press.

Bhandari, V. (2021). Surveillance, privacy, and the Indian Constitution. *NUJS Law Review*, 14(2), 205–234.

Vidhi Centre for Legal Policy. (2020). *Privacy and surveillance reform in India*. New Delhi.

Law Commission of India. (2017). Report No. 267: Hate Speech (contextual relevance to chilling effect).