ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 5| May 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

THE NEED FOR A DEDICATED SURVEILLANCE LAW IN INDIA POST-DPDP ACT AND NEW CRIMINAL LAWS

Nikita Sehrawat
Research Scholar, Department of Law, Kurukshetra University, Kurukshetra, Haryana

ABSTRACT

The recent enactment of India's Digital Personal Data Protection Act (DPDP Act) 2023 and the overhaul of its criminal justice system through the Bharatiya Nyaya Sanhita (BNS) 2023, Bharatiya Nagarik Suraksha Sanhita (BNSS) 2023, and Bharatiya Sakshya Adhiniyam (BSA) 2023 mark a significant legislative leap. While the DPDP Act introduces a framework for data protection and the new criminal laws modernize investigative procedures, a critical lacuna remains: the absence of a comprehensive, dedicated surveillance law. This paper argues that despite these legislative advancements, India's surveillance regime remains fragmented, opaque, and prone to potential misuse, posing a persistent threat to the fundamental right to privacy enshrined in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017). It will analyze the shortcomings of existing legal provisions, the broad exemptions granted to the state under the DPDP Act, and the expanded digital powers of law enforcement under the new criminal laws. The paper will highlight the need for a separate, overarching surveillance law grounded in principles of legality, necessity, and proportionality, establishing robust oversight mechanisms, accountability frameworks, and redressal avenues to safeguard individual liberties in the digital age.

KEYWORDS: *Data Privacy, Surveillance Law, Criminal Investigations, DPDP Act, Bharatiya Nyaya Sanhita (BNS), Bharatiya Nagarik Suraksha Sanhita (BNSS), Bharatiya Sakshya Adhiniyam (BSA), Right to Privacy, Digital Evidence, India.*

INTRODUCTION

India stands at a pivotal juncture in its legal and technological evolution. The very fabric of its justice system and the contours of its citizens' fundamental rights are undergoing a profound transformation. The recent past has witnessed landmark changes, from the Supreme Court's emphatic and unequivocal declaration of privacy as a fundamental right in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) – a ruling that fundamentally reshaped constitutional jurisprudence – to the long-awaited enactment of the Digital Personal Data Protection Act (DPDP Act) in 2023. This Act, after years of deliberation, finally provides a foundational legal framework for safeguarding personal data in the digital realm. Concurrently, the nation's antiquated, colonial-era criminal laws, which had governed police investigation, evidence, and substantive crimes for over a century, have been comprehensively replaced by the Bharatiya Nyaya Sanhita (BNS), Bharatiya Nagarik Suraksha Sanhita (BNSS), and Bharatiya Sakshya Adhiniyam (BSA), all of which came into effect from July 1, 2024. These new statutes represent a monumental effort to modernize India's criminal justice system, streamline investigations, and crucially, embrace the ubiquity of digital technologies in both criminal activity and law enforcement.

The shift towards a "digital-first" approach in criminal law, coupled with the recognition of privacy as a fundamental right and the establishment of a data protection framework, signals India's ambition to be a leading digital economy that also respects individual liberties. However, beneath the surface of these commendable legislative developments lies a critical and unresolved tension. While the new laws enhance the state's capacity to collect, process, and utilize digital information for crime prevention and investigation, a crucial element remains conspicuously absent: a dedicated, comprehensive law governing state surveillance. The current landscape is characterized by a patchwork of archaic laws (such as the Indian Telegraph Act, 1885), administrative rules, and judicial pronouncements that simply fail to adequately address the complexities, scale, and invasiveness of modern digital surveillance technologies. Technologies like facial recognition, DNA databases, network interception, and advanced data analytics, increasingly employed by law enforcement, operate in a grey area, largely unconstrained by a specific and robust legal framework.

This paper contends that without a specific, overarching, and robust surveillance law, the fundamental right to privacy, even with the protective umbrella of the DPDP Act and the modernized criminal laws, remains profoundly vulnerable to arbitrary state intrusion. The current framework creates an imbalanced scenario where law enforcement agencies are equipped with expanded digital powers under the BNSS and BSA, yet the safeguards and oversight mechanisms mandated by a comprehensive surveillance law are missing. This legislative lacuna poses a persistent threat to individual liberties, undermines democratic principles, and ultimately leaves India's digital justice framework incomplete. This research will delve into the inadequacies of the existing legal provisions, scrutinize the broad exemptions granted to government agencies under the DPDP Act, and analyze how the expanded digital powers of law enforcement under the new criminal laws exacerbate the need for a dedicated surveillance

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 5| May 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

regime. The core argument will be that a separate, overarching surveillance law, firmly grounded in the principles of legality, necessity, and proportionality as articulated by the Supreme Court, and equipped with robust oversight mechanisms, accountability frameworks, and effective redressed avenues, is imperative to truly safeguard privacy in India's evolving digital landscape.

THE FRAGMENTED AND ARCHAIC SURVEILLANCE LANDSCAPE PRE-NEW LAWS

Prior to the recent legislative changes, India's surveillance regime operated under provisions primarily derived from two colonial-era statutes: The Indian Telegraph Act, 1885, and Section 69 of the Information Technology Act, 2000.

- **The Indian Telegraph Act, 1885:** This century-old law provides the basis for intercepting telephone communications. Its provisions, along with the Telegraph Rules, 1951, grant the Central and State governments the power to intercept messages in specific circumstances, generally related to public safety or national security. However, these provisions lack granular detail on proportionality, necessity, and independent oversight. The process often relies on executive discretion rather than stringent judicial authorization.
- **Information Technology Act, 2000 (Section 69):** This section empowers the government to intercept, monitor, or decrypt any information generated, transmitted, received, or stored in any computer resource. Similar to the Telegraph Act, it cites grounds of national security, public order, and prevention of cognizable offenses. While the IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, provide some procedural safeguards, they have been criticized for lacking independent oversight and transparency.

The significant shortcomings of this fragmented framework were starkly highlighted by the *Puttaswamy* judgment, which declared privacy a fundamental right and mandated that any state intrusion must satisfy the triple test of legality, legitimate aim, and proportionality. Existing surveillance laws struggled to meet these constitutional benchmarks, leading to widespread calls for comprehensive reform. The Pegasus spyware controversy, revealing potential state surveillance of journalists, activists, and opposition leaders, further exacerbated these concerns, underscoring the severe lack of accountability and transparency.

THE DPDP ACT 2023: A PARTIAL STEP FOR PRIVACY

The Digital Personal Data Protection Act (DPDP Act) 2023 is India's first comprehensive data protection law, aiming to regulate the processing of digital personal data. It introduces concepts like Data Fiduciary, Data Principal, consent, and various data protection obligations. While a welcome development, its effectiveness in curbing state surveillance is significantly diluted by broad exemptions.

- **Section 17(2) of the DPDP Act:** This crucial provision exempts certain government agencies from many core obligations of the Act, including the requirements of consent, purpose limitation, data minimization, and the right to erasure, among others. The grounds for these exemptions include "prevention, detection, investigation or prosecution of any offence or for the enforcement of any legal right or claim," "national security," "public order," and "preventing incitement to the commission of any cognizable offence."
- **Concerns with Exemptions:** Critics argue that these exemptions are excessively broad and grant the government considerable leeway to process personal data without the strictures imposed on private entities. The vagueness of terms like "public order" creates a wide interpretative window that could be exploited for surveillance purposes. Furthermore, the Act does not establish an independent oversight body for government data processing activities, leaving a significant accountability gap. The Data Protection Board of India, established under the Act, primarily focuses on compliance by data fiduciaries, not on monitoring state surveillance.
- **The Unaddressed Core of Surveillance:** Crucially, the DPDP Act is a general data protection law; it does not explicitly define or regulate the *methods* of surveillance, the *criteria* for authorizing it, or the *specific procedural safeguards* required before deploying intrusive technologies. It assumes existing legal frameworks for surveillance remain valid, yet those frameworks are precisely what are under scrutiny for their inadequacy.

Therefore, while the DPDP Act marks a move towards recognizing data privacy, it leaves the door open for extensive state surveillance by exempting government agencies without instituting corresponding, robust oversight mechanisms. The balance, in this critical area, arguably tilts heavily in favor of the state.

NEW CRIMINAL LAWS (BNS, BNSS, BSA): EXPANDING DIGITAL POWERS WITHOUT CORRESPONDING PRIVACY SAFEGUARDS

The BNS, BNSS, and BSA, effective July 1, 2024, introduce significant changes to India's criminal justice system, particularly in the realm of digital evidence and investigation. While aiming for efficiency and modernization, these laws also expand the digital powers of law enforcement without adequately addressing the concomitant privacy implications through a dedicated surveillance framework.

- **Bharatiya Sakshya Adhiniyam (BSA) 2023:** This Act significantly updates the law of evidence to include electronic records more explicitly. Section 57 of the BSA recognizes electronic or digital records as primary evidence, and Sections 61, 62, and 63 establish conditions for their admissibility, including a certification process. While this legitimizes digital evidence, it doesn't address how such data is collected in

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 5| May 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

the first place, or the privacy impact of extensive data collection for investigative purposes. The focus is on admissibility, not on the legality and proportionality of the initial surveillance act that procured the data.

- **Bharatiya Nagarik Suraksha Sanhita (BNSS) 2023:** The BNSS introduces several provisions that leverage technology for investigation:
  i. **e-FIRs and Electronic Communication (Section 173):** Facilitating electronic registration of FIRs and communication of information. While intended for efficiency, the increased digitization of police records raises questions about data security, access control, and the potential for abuse of such sensitive information.
  ii. **Mandatory Videography of Search and Seizure (Section 105):** This provision mandates audio-video recording of search and seizure operations for offenses punishable with seven or more years of imprisonment. While a positive step for transparency and accountability in police conduct, it also entails the collection of vast amounts of visual and audio data from private spaces. Without clear guidelines on data retention, access, and oversight, this data could pose significant privacy risks, especially if not strictly limited to the purpose of the investigation.
    a. **Electronic Means for Examination of Witnesses and Accused (Sections 54, 180(3), 265, 266, 308):** The BNSS allows for recording witness statements, conducting identification parades, and examining the accused through audio-video electronic means. While beneficial for expediting trials and protecting vulnerable witnesses, the collection and storage of such sensitive personal data (including biometric information) require robust privacy safeguards that are currently lacking.
    b. **Forensic Experts at Crime Scenes (Section 176):** Mandatory forensic visits and evidence collection for serious offenses will inherently involve collection of digital traces. The process requires stringent adherence to privacy principles.
  iii. **Bharatiya Nyaya Sanhita (BNS) 2023:** While primarily focused on substantive offenses, the BNS's modernized definitions of offenses, including those related to cybercrime and organized crime, will necessitate sophisticated digital investigations. The new provisions on 'organized crime' and 'terrorist acts' might also inadvertently be used to justify broader surveillance powers, without a parallel legislative framework to contain potential overreach.

In essence, the new criminal laws significantly empower law enforcement to leverage digital data and technology in investigations. However, they operate within the privacy vacuum created by the broad exemptions in the DPDP Act and the outdated surveillance laws. This creates a scenario where the state has enhanced capabilities to collect and process personal data but lacks a clear, robust, and judicially overseen framework to ensure that such collection is conducted within the strict constitutional limits of necessity and proportionality.

THE CONSTITUTIONAL IMPERATIVE: LEGALITY, NECESSITY, PROPORTIONALITY, AND OVERSIGHT

The *Puttaswamy* judgment unequivocally established the right to privacy as a fundamental right under Article 21 of the Indian Constitution. It laid down a three-fold test for any state action infringing on privacy:

1. **Legality:** The action must be backed by a law.
2. **Legitimate Aim:** The law must serve a legitimate state interest (e.g., national security, public order, crime prevention).
3. **Proportionality:** The measure taken must be necessary and proportionate to the legitimate aim, meaning it should be the least intrusive means to achieve the objective, and there should be a rational nexus between the means adopted and the object sought to be achieved.

Current surveillance practices, relying on the Indian Telegraph Act and IT Act, struggle to meet the proportionality test consistently. The *Puttaswamy* judgment itself pointed towards the need for a comprehensive data protection regime that includes robust safeguards against arbitrary state surveillance. The DPDP Act addresses data protection generally but falls short on specific surveillance regulation. The new criminal laws enhance investigative powers but do not build the necessary privacy infrastructure around them.

A dedicated surveillance law is essential to operationalize these constitutional principles:

- **Clarity on Legality:** It would provide a singular, comprehensive legal basis for all forms of state surveillance, clarifying permissible methods, the types of data that can be collected, and the specific thresholds for authorization.
- **Strict Necessity and Proportionality:** A dedicated law could define "necessity" and "proportionality" in the context of various surveillance methods, requiring judicial or independent oversight to ensure that surveillance is not a default but a measure of last resort, strictly tailored to the legitimate aim. It would also differentiate between targeted surveillance (e.g., specific individual, specific crime) and mass surveillance (e.g., facial recognition databases, bulk data retention).
- **Independent Oversight and Review:** The most glaring omission in the current framework is the lack of independent oversight. A surveillance law must establish a statutory body, preferably with judicial or quasi-judicial powers, to authorize, review, and audit surveillance requests and operations. This body should be distinct from the

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 5| May 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

executive and possess the authority to reject disproportionate requests, ensure compliance with legal procedures, and hold agencies accountable for misuse.

- **Transparency and Accountability:** The law should mandate greater transparency regarding surveillance policies and statistics (e.g., number of interception orders, types of data collected), while balancing legitimate confidentiality requirements. It should also establish clear mechanisms for accountability, including penalties for unauthorized surveillance and a robust redressal system for individuals whose privacy rights have been violated.
- **Data Minimization and Purpose Limitation:** A dedicated law can explicitly impose principles of data minimization (collecting only what is strictly necessary) and purpose limitation (using collected data only for the intended purpose) on law enforcement agencies, going beyond the general provisions of the DPDP Act.
- **Regular Audits and Review:** Mechanisms for regular, independent audits of surveillance systems and practices would ensure ongoing compliance and identify areas for improvement.

INTERNATIONAL BEST PRACTICES AND LESSONS FOR INDIA

Many democratic nations have enacted dedicated surveillance laws that attempt to balance national security with individual rights. Examples include:

- **United Kingdom (Investigatory Powers Act 2016):** Often criticized but comprehensive, it provides a unified framework for all forms of state surveillance, including bulk interception, targeted interception, and equipment interference. It mandates "double-lock" authorization (requiring both ministerial and judicial approval) for many intrusive powers and establishes an independent Investigatory Powers Commissioner for oversight.
- **Germany (various laws including the G10 Act):** German law, influenced by its constitutional court, has strict requirements for surveillance. It emphasizes judicial authorization, necessity, and proportionality, with strong independent oversight.
- **European Union (GDPR and various national laws):** While the GDPR is a general data protection law, EU member states have specific laws governing police and intelligence surveillance, often subject to rigorous judicial review and overseen by strong data protection authorities.

While each country has unique contexts, common themes emerge: independent authorization, strict proportionality, robust oversight, transparency (where possible), and clear accountability. India, having affirmed privacy as a fundamental right, has a constitutional obligation to align its surveillance practices with these globally recognized principles.

CONCLUSION

The DPDP Act and the new criminal laws represent a significant step forward in India's legal landscape. However, by failing to enact a dedicated surveillance law, India has left a critical gap in its framework for protecting fundamental rights in the digital age. The current piecemeal approach, characterized by broad exemptions for state agencies and the lack of independent oversight, creates an environment ripe for potential misuse and undermines the very essence of informational privacy.

A comprehensive surveillance law, grounded in constitutional principles and international best practices, isn't just a legal nicety; it's a democratic imperative. Such a law would provide legal certainty for both law enforcement and citizens, clearly defining the boundaries of state power. It would ensure proportionality and necessity in surveillance operations, actively preventing indiscriminate or overreaching state action. Furthermore, establishing robust independent oversight by a judicial or quasi-judicial body would be crucial in preventing executive overreach. By fostering transparency and accountability, such a law would build public trust in the state's use of powerful technologies and provide effective redressal mechanisms for individuals whose rights are violated.As India embraces the digital future with its new criminal laws, it is crucial that the state also commits to a comprehensive and rights-respecting surveillance framework. Only then can the promises of digital efficiency and citizen protection truly be realized, ensuring that India's journey towards a modern justice system respects and upholds the fundamental right to privacy for all its citizens. The unfinished framework demands
immediate legislative attention to safeguard individual liberties against the increasing power of digital surveillance.

REFERENCES

1. *Bhatia, Gautam. Offend, Shock, or Disturb: Free Speech under the Indian Constitution. Oxford University Press, 2016.*
2. *Solove, Daniel J. Understanding Privacy. Harvard University Press, 2008.*
3. *Mayer-Schönberger, Viktor. Delete: The Virtue of Forgetting in the Digital Age. Princeton University Press, 2009.*
4. *Lessig, Lawrence. Code and Other Laws of Cyberspace, Version 2.0. Basic Books, 2006.*
5. *Ratan, Neer. Criminal Justice System in India. Routledge, 2021.*
6. *Deakin, Simon, et al. Digital Regulation: Law, Economics, and Policy. Oxford University Press, 2024.*
7. *The Missing Piece: Why India Urgently Needs a Comprehensive Surveillance Law."* Indian Journal of Constitutional Law *or* Journal of Law, Technology & Policy
8. *Collier, Adam, and Daniel J. Solove. "Digital Surveillance: A Comparative Analysis of Legal Frameworks."* International Journal of Law and Information Technology.
9. *"Biometric Data in Criminal Justice: A Human Rights Perspective on the New Indian Laws."* Journal of Law and Medicine.