IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DATA PROTECTION, CYBER SECURITY, AND STATE SURVEILLANCE BALANCING PRIVACY AND NATIONAL SECURITY IN THE DIGITAL AGE

Dr. Wasim Ahmad. Ms. Hiteshi, Ms Monika Sharma, Ms. Pratiksha

All Assistant Professors

School of Law

Starex University, Gurugram

Abstract

The rapid expansion of digital technologies has transformed governance, enabling States to deploy surveillance tools such as real-time interception, bulk data collection, and algorithmic analytics for cyber security and law enforcement. However, these practices raise serious concerns regarding the protection of individual privacy and civil liberties. In India, this tension is particularly significant following the Supreme Court's landmark decision in *K.S. Puttaswamy v Union of India*, which recognised the right to privacy as a fundamental right under Article 21 and established the tests of legality, legitimate aim, necessity, and proportionality.

This Conference paper critically examines the conflict between privacy and State surveillance within India's legal framework, highlighting structural deficiencies in existing laws such as the Indian Telegraph Act, 1885 and the Information Technology Act, 2000. It further evaluates the role of the Digital Personal Data Protection Act, 2023, noting that while it introduces a comprehensive data protection regime, its broad exemptions for State activities limit its effectiveness in regulating surveillance.

1. Introduction

The digital revolution has fundamentally altered how modern States govern, communicate and secure their populations. Increasingly, governments rely on digital-surveillance architectures, real-time interception, large-scale data retention and algorithmic analytics to combat cyber threats, terrorism and organised crime. While these tools promise efficiency and preventive capacity, they also intrude deeply into the informational, bodily and decisional spheres that constitute individual autonomy and dignity.[1]

In India, this tension is particularly acute because constitutional freedoms especially the right to privacy under Article 21 must be reconciled with an expanded security and governance apparatus that operates through both law and executive practice.[2] The Supreme Court's recognition of privacy as a fundamental right in K.S. Puttaswamy v Union of India has significantly raised the threshold for justifying State

surveillance, insisting that any restriction must satisfy tests of legality, legitimate aim, necessity and proportionality.[3] Yet the existing surveillance and cyber-security framework remains fragmented, executive-driven and only partially aligned with these constitutional requirements.[4] This paper examines the conceptual and legal conflict between privacy and surveillance in India's cyber-security regime, assesses the impact of the Digital Personal Data Protection Act 2023 and proposes reforms to ensure that security measures operate within a rights-based constitutional order.[5]

2. Conceptual Framework: Privacy vs Surveillance

2.1 Right to privacy

The right to privacy is widely understood as intrinsic to human dignity and personal liberty. Philosophically, it protects three interrelated interests: informational privacy (control over personal data and communications), bodily privacy (freedom from intrusive physical or technological surveillance) and decisional autonomy (freedom to make intimate and political choices without undue interference).

In K.S. Puttaswamy v Union of India, a nine-judge Bench of the Supreme Court unanimously held that privacy is a constitutionally protected fundamental right under Article 21 and as part of the freedoms guaranteed by Part III. The Court traced privacy to concepts of dignity, bodily integrity and personal autonomy, and explicitly overruled earlier decisions that had denied fundamental-right status to privacy. Importantly, the Bench articulated a three-pronged test for any State action that limits privacy: there must be (i) a law (legality), (ii) a legitimate State aim, and (iii) a proportionate means employed, including rational connection and minimal impairment, subject to procedural safeguards. Privacy, therefore, is not absolute, but any restriction must be narrowly tailored and justifiable in a constitutional democracy.

2.2 State surveillance

State surveillance in the digital age encompasses interception of communications, monitoring of online activities, bulk and targeted data collection, metadata analysis, profiling and increasingly, algorithmically driven risk-assessment systems. In principle, such measures are justified on grounds of national security, public order, prevention and investigation of offences and protection of critical infrastructure. However, unchecked or opaque surveillance architectures risk normalising a culture of suspicion, chilling free expression and association, enabling discrimination and undermining the very democratic accountability that security is meant to protect.[6]

Academic and civil-society critiques of India's interception and monitoring regime highlight the breadth of executive powers, the absence of prior judicial authorisation, weak ex post review and limited access to remedies for individuals subjected to unlawful or disproportionate surveillance.[7] The challenge, therefore, is to develop a framework in which surveillance remains available as a legitimate tool of cyber security but is constrained by robust constitutional, statutory and institutional safeguards.

3. Conflict Between Privacy and Surveillance Laws

India's surveillance laws and practices reveal several structural tensions with the constitutional conception of privacy. First, interception and monitoring powers in telecommunication and information-technology statutes confer broad discretions on the executive, often couched in open-ended terms such as "sovereignty and integrity of India", "security of the State", "public order" or "prevention of incitement to an offence". Secondly, there is limited transparency: orders for interception or decryption are typically secret, with only internal review committees and no routine public reporting, which impedes democratic oversight. Thirdly, affected citizens have few effective remedies because they may never know they were surveilled, and statutory frameworks provide no clear mechanisms for individual challenge or compensation.

From a constitutional perspective, the central issue is whether existing and proposed surveillance measures satisfy the proportionality test elaborated in Puttaswamy. This requires asking in each case:

(i) Legality – Is there a clear, accessible law authorising the surveillance, with precise scope and limits?[8]
(ii) Legitimate aim – Does the measure pursue a genuine State interest such as national security or prevention of serious crime, rather than vague or political objectives?
(iii) Necessity and proportionality – Is the measure strictly necessary for that aim, or could less intrusive means suffice? Are the duration, scope, data categories and persons targeted proportionate?
(iv) Procedural safeguards – Are there independent authorisation, periodic review, logging, data-minimisation, audit and ex post remedies, including judicial oversight?

Much of India's current interception and decryption practice, as commentators argue, falls short on at least the last two elements, particularly in the context of bulk or programmatic surveillance for cyber-security and threat-intelligence purposes.

4. India's Data Protection Framework

4.1 Digital Personal Data Protection Act 2023

The Digital Personal Data Protection Act 2023 (DPDPA) is India's first comprehensive personal-data statute, intended to regulate the collection and processing of digital personal data, define rights of data principals and obligations of data fiduciaries, and establish a Data Protection Board with enforcement powers. The Act is built around consent-based processing, purpose limitation, storage limitation, data-security obligations and penalties for non-compliance.[9]

For individuals, the DPDPA recognises rights such as access to personal data, correction and erasure, grievance redress and the right to nominate another person to exercise rights in certain circumstances. For data fiduciaries, it mandates reasonable security practices, breach reporting and compliance with directions of the Data Protection Board. PRS analysis notes, however, that the Act grants wide exemptions to the State and government-controlled entities, allowing processing in the interests of national security, public order and other grounds, with many core obligations and rights disapplied in such contexts.[10]

4.2 Limitations in the context of surveillance

Critics argue that broad exemptions to State processing, coupled with the lack of a strong, structurally independent data-protection authority, limit the DPDPA's capacity to meaningfully restrain surveillance. Under the Act, the central government can exempt its instrumentalities from significant obligations where processing is for notified purposes such as national security or public order, effectively creating wide carve-outs in precisely those areas where surveillance risks are highest. Moreover, there is no explicit requirement that surveillance-related processing comply with the proportionality test or obtain prior judicial authorisation, and the Board's independence has been questioned due to the extent of executive control over appointments and functions.[11]

Consequently, while the DPDPA improves the general data-protection landscape, it does not yet establish a comprehensive rights-protective regime for surveillance and cyber-security operations, leaving privacy protection to be mediated by older interception laws and constitutional litigation.

5. Cyber Security vs Civil Liberties

Cyber-security measures often rely on practices such as mandatory data retention, large-scale traffic monitoring, decryption orders and regulation of encryption standards. These tools can assist in detecting malware, preventing cyber-attacks, tracing perpetrators and securing critical infrastructure.[12] However, without clear statutory limits, necessity tests and oversight, such measures may infringe privacy, restrict freedom of speech and association, and facilitate profiling or discrimination, especially against vulnerable communities and political dissenters.

Comparative literature on cyber security and rights cautions that mass surveillance or indiscriminate data retention is rarely justifiable under proportionality analysis, and that targeted, intelligence-led surveillance should be the norm.[13] In India, concerns have been raised that current and proposed frameworks tilt towards expansive preventive surveillance, with insufficient embedding of rights-based safeguards, transparency obligations and avenues for challenge. Ultimately, cyber security cannot be constitutionally sustainable if it systematically undermines the very civil liberties that the Constitution is designed to protect.

6. Surveillance Mechanisms and Legal Challenges

6.1 Legal framework in India

The traditional statutory bases for surveillance in India are section 5(2) of the Indian Telegraph Act 1885, which permits interception of messages on specified grounds, and provisions of the Information Technology Act 2000, particularly section 69, which authorises interception, monitoring and decryption of information through computer resources. These are supplemented by detailed rules on interception, monitoring and blocking, as well as executive orders and guidelines for lawful interception and monitoring systems.

Section 69 of the IT Act, modelled largely on section 5(2) of the Telegraph Act, empowers the government to direct any agency or intermediary to intercept, monitor or decrypt information for reasons including sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States, public order or for preventing incitement to an offence. Civil-society analyses emphasise that these provisions, though subject to executive review committees, lack prior judicial scrutiny, do not envisage independent authorisation or audit, and leave significant discretion in the hands of the executive.

6.2 Challenges

Key challenges in the present framework include:

(a) Lack of transparency: Interception orders and decryption directions are confidential, and there is no requirement for systematic public reporting on the volume, nature or outcomes of surveillance activities.

(b) Absence of independent oversight: Authorisation and review are internal to the executive, with no standing role for the judiciary or independent regulators in ex ante scrutiny of surveillance requests.

(c) Risk of mass surveillance: The architecture of centralised monitoring systems and broad interception powers has generated fears that surveillance may extend beyond targeted suspects to large segments of the population, contrary to the spirit of Puttaswamy's proportionality doctrine.

These structural weaknesses heighten the risk of arbitrary, politically motivated or discriminatory surveillance and undermine public trust in digital-governance initiatives.

7. Judicial Approach to Privacy and Surveillance

The judiciary has emerged as a key institution in articulating and enforcing privacy protections against unrestrained surveillance. In Puttaswamy, the Supreme Court located privacy within the core of Article 21 and made proportionality the central test for assessing intrusions. The judgment emphasised that any surveillance-related law or executive action must be backed by a valid statute, pursue a legitimate aim, use proportionate means and be subject to robust procedural safeguards, including oversight and remedies.

Subsequent decisions have applied privacy and proportionality analysis in varied contexts such as linking Aadhaar to certain services, the retention of biometric data and aspects of data collection but a comprehensive surveillance case testing the full architecture of interception and monitoring has not yet been adjudicated at the same level.[14] Nonetheless, Puttaswamy has influenced data-protection debates and

legislative drafting, with courts and commentators invoking it to criticise overbroad exemptions and inadequate safeguards in new digital-governance statutes.[15]

The judicial approach thus offers a constitutional compass but has not yet been fully translated into detailed statutory reforms that would re-design surveillance powers in line with privacy and proportionality requirements.

8. Comparative Perspectives

8.1 European Union

The European Union offers an instructive model in which strong data-protection norms coexist with security and law-enforcement powers. The General Data Protection Regulation (GDPR) establishes robust rights for data subjects, stringent obligations for controllers and processors and mandates independent supervisory authorities in each Member State with investigative, corrective and advisory powers. These authorities oversee compliance, handle complaints and cooperate in cross-border cases, providing an institutional check on disproportionate data-processing, including by public authorities. [16]

At the same time, security-related surveillance is addressed through specific instruments and subject to rule-of-law constraints, with the Court of Justice of the EU repeatedly striking down indiscriminate bulk-data retention measures as incompatible with fundamental rights.[17] European scholarship and policy emphasise that surveillance must be targeted, time-bound and subject to independent oversight, and that data-protection authorities, courts and parliaments all have roles in maintaining this balance.

8.2 United States

The United States historically follows a more security-focused, sectoral approach to privacy, with different statutes governing health, financial and children's data, and significant surveillance authorities vested in intelligence and law-enforcement agencies. Constitutional review under the Fourth Amendment and statutory frameworks such as the Foreign Intelligence Surveillance Act provide some judicial oversight, but bulk-collection programmes and metadata surveillance have generated substantial civil-liberties concerns.

Recent reforms and debates have attempted to recalibrate this balance by increasing transparency, tightening standards for collection and expanding independent review, yet critics argue that national-security considerations still often prevail over privacy and data-protection concerns.[18] Lessons from both the EU and US highlight the importance of independent regulators, clear statutory limits and meaningful judicial review in structuring surveillance powers.

9. Recommendations

(a) Judicial authorisation for surveillance: Interception, monitoring and decryption orders especially those of significant scope or duration should require prior or prompt judicial authorisation, at least at a preliminary level, with detailed reasons recorded and subject to periodic review.[19]

(b) Limiting State exemptions under data-protection law: Exemptions for State processing in the DPDPA should be narrowly drafted, subject to necessity and proportionality tests and constrained by independent oversight, rather than broad carve-outs that exclude entire categories of processing from core safeguards.

(c) Establishing independent oversight bodies: A structurally independent data-protection authority and a dedicated surveillance-oversight mechanism comprising judicial and expert members should be responsible for authorising, reviewing and auditing surveillance activities, with powers to order cessation, deletion and compensation where necessary.

(d) Enhancing transparency and accountability: Aggregated transparency reports on interception, monitoring and decryption orders should be published, alongside robust internal logging, ex post audits and parliamentary scrutiny.

(e) Adopting global best practices: India should draw on comparative experiences under the GDPR and leading constitutional jurisprudence to embed necessity, proportionality, data minimisation, purpose limitation and independent supervision into all cyber-security and surveillance programmes.

10. Conclusion

The evolution of India's digital state has brought the question of how to balance privacy and national security to the centre of constitutional debate. Cyber threats, terrorism, disinformation, and organised crime are real and evolving dangers. They demand sophisticated tools: real-time monitoring, rapid data-sharing, predictive analytics, and robust cyber-defence capabilities. Yet the same technologies that empower the State to respond to these threats also enable unprecedented insight into citizens' lives, movements, relationships, and thoughts. The core concern is that, without carefully designed limits, the architecture built to protect democracy can quietly erode its foundational values.

India's constitutional jurisprudence has already travelled a long distance towards recognising the centrality of privacy in this new environment. By locating privacy within Article 21 and tying it to dignity, bodily integrity, and decisional autonomy, the Supreme Court has moved beyond narrow, spatial conceptions ("privacy inside one's home") towards a more substantive understanding of what it means to live as a free person under a Constitution. The articulation of the tests of legality, legitimate aim, necessity, and proportionality provides not just a doctrinal tool, but a normative yardstick: state action that interferes with privacy must be authorised by clear law, must pursue a genuine public purpose, must be strictly needed for that purpose, and must be accompanied by safeguards and remedies.

However, there is a noticeable gap between this constitutional vision and the statutory reality of India's surveillance and cyber-security regime. Much of the existing legal framework whether under the Telegraph Act, the Information Technology Act, or their subordinate rules was conceived before privacy was recognised as a fundamental right, and before the magnitude of data-driven governance was fully appreciated. These laws often grant broad discretionary powers to the executive, couched in expansive language like "security of the State" or "public order", with relatively little involvement of independent bodies at the point of authorisation or review. Orders for interception, monitoring, and decryption operate largely in secrecy, with minimal public reporting. For many citizens, surveillance is not something they can contest; it is something they might never know has occurred.

The Digital Personal Data Protection Act marks a significant step towards organising India's data-protection landscape, but it is not yet a complete answer to the surveillance problem. Its rights and obligations are meaningful in the general context of personal-data processing by private and public entities, but the wide exemptions it permits for State processing on security and public-order grounds create precisely the sort of blind spots where the risk of overreach is greatest. If large swathes of State activity can be insulated from core data-protection duties on the simple assertion of security needs, the promise of rights for individuals becomes contingent, especially in the most sensitive areas.

In this sense, India's present regime can be seen as structurally asymmetric. On the one hand, it proclaims a strong constitutional right to privacy and obliges the State to justify intrusions through a rigorous proportionality analysis. On the other hand, the day-to-day operation of surveillance and cyber-security measures is governed by frameworks that do not fully internalise these requirements, and that leave many critical decisions in the hands of the very agencies whose powers ought to be checked. This is not to deny the complexity of the task: cyber-security demands rapid action, technical expertise, and in some cases a degree of operational secrecy. But constitutionalism demands that such action be embedded in a system of independent authorisation, transparent rules, and accountability ex post.

The comparative experience of other democracies illustrates that this is not an impossible balance to strike. The European Union's model, for example, shows how independent supervisory authorities with clearly defined powers, combined with strong data-protection norms and judicial review, can discipline security and surveillance measures without paralysing them. Courts have struck down indiscriminate bulk-retention measures but left room for targeted, intelligence-led surveillance supported by proper safeguards. The lesson is that the question is not whether to have surveillance, but how to design surveillance in a way that is precise, limited, and controlled.

In the Indian context, moving towards such a model would involve several interrelated reforms. Surveillance powers should be based on clear statutes that define their scope, thresholds, and duration, rather than on open-textured executive regulations. Authorisation, particularly for intrusive or large-scale measures, should involve an element of judicial or independent scrutiny at the outset, rather than relying entirely on internal executive procedures. Oversight should not be left to occasional committee reviews behind closed doors, but should include regular audits, independent inspections, and structured reporting to Parliament or another democratic body.

Equally important is the creation or strengthening of independent institutions. A data-protection authority that is genuinely autonomous from the executive, equipped with technical capacity and legal powers, can serve as a counterweight to unilateral security claims. A dedicated surveillance-oversight mechanism with judicial and expert participation could monitor trends, investigate complaints, and recommend reforms. Such bodies do not eliminate security risks, but they provide an organised, institutionalised way of ensuring that the response to those risks remains anchored in the rule of law.

Transparency, while necessarily limited in some operational details, is another key pillar. Aggregate statistics on the number and types of interception or decryption orders issued, the grounds invoked, and the rate at which applications are accepted or refused can be published without revealing sensitive sources or methods. This allows public debate, academic scrutiny, and media analysis to play their role in a democracy. It also forces policymakers to be explicit about the trade-offs they are making, rather than allowing security concerns to operate as a catch-all justification resistant to examination.

None of these steps requires abandoning or weakening cyber-security goals. On the contrary, rights-compatible security tends to be more robust in the long term because it is less likely to provoke backlash, lose public trust, or be invalidated in court. Systems designed from the outset with proportionality in mind collecting only what is necessary, retaining it only for as long as required, and restricting access to clearly defined purposes are less vulnerable to abuse or mission creep. They also fit more comfortably into an international environment where cross-border data flows and cooperation increasingly depend on perceptions of a country's rights record.

Ultimately, the question is not whether India should be a surveillance state or a secure nation. The false dichotomy between the two obscures the possibility that genuine, sustainable security rests on respect for individual rights and the legitimacy that such respect creates. A framework that subjects surveillance to clear law, independent oversight, and effective remedies does not weaken the State; it clarifies its role, delineates its powers, and grounds its authority in the consent of the governed. In the digital age, where the line between ordinary life and digital infrastructure has all but disappeared, such clarity is not a luxury but a necessity.

If India is able to re-shape its data-protection, cyber-security, and surveillance regimes in line with its own constitutional values, it will not only strengthen protections for its citizens but also set a powerful example for other democracies grappling with similar challenges. The Constitution's promise of liberty and dignity need not be a casualty of the digital era. With deliberate and principled reform, it can instead become the standard by which technological power is measured, guided, and ultimately constrained.

References

1 Global Legal Insights, "Autonomous AI: Who is Responsible When Things Go Wrong?" 2025.[globallegalinsights]

2 "AI Generated Content Regulation in India" Drishti IAS, 24 October 2025.[drishtiias]

3 Gallego-Losada R and others, "The Law and Economics of AI Liability" Computer Law and Security Review 2023.[sciencedirect]

4 "Regulating Artificial Intelligence in India: Legal Frameworks, Governance Challenges and the Path Toward a Digital Constitution" Wisdom J 2026.[wisdomj]

5 "Deepfake Regulation India 2025: MeitY's Comprehensive IT Law Overhaul" Khurana & Khurana, 15 December 2025.[khuranaandkhurana]

6 Sahoo S, "Emerging Technologies and Law: Legal Status of Tackling Crimes Relating to Deepfakes in India" SCC Online Blog 16 March 2023.[scconline]

7 "Liability for Harm Caused by Autonomous AI Systems" International Journal of Science and Technology 2025.[ijsat]

8 "Digital Liability for AI-Generated Malware: Can Code Be a Legal Person?" International Journal of Indian Research in Law 2025.[ijirl]

9 "AI Generated Content Regulation in India" Drishti IAS, 24 October 2025.[drishtiias]

10 "AI Liability – Who Is Accountable When Artificial Intelligence Causes Harm?" Taylor Wessing Insight, 30 January 2025.[taylorwessing]

11 European Parliament, "Artificial Intelligence and Civil Liability: A European Perspective" Study 2025.[europarl.europa]

12 "European Parliament Study Recommends Strict Liability Regime for High-Risk AI Systems" Inside Privacy, 21 August 2025.[insideprivacy]

13 "Who is Responsible When AI Acts Autonomously & Things Go Wrong?" Global Legal Insights AI, Machine Learning and Big Data Laws and Regulations 2025.[globallegalinsights]

14 Nogacki R, "Legal Responsibility for AI Decision-Making: Who Bears Liability When AI Makes a Mistake?" 6 May 2025.[linkedin]

15 "The Case for AI Liability" Institute for Law & AI, 22 June 2025.[law-ai]

16 Tschider C, "Applying Strict Liability to Artificial Intelligence as an Abnormally Dangerous Activity" 2024.[scholarship.law.missouri]

17 "Identify High-Risk AI Systems Under the EU AI Act" Holistic AI Blog, 13 February 2025.[holisticai]

18 "AI Generated Content Regulation in India" Drishti IAS, 24 October 2025.[drishtiias]

19 "Emerging Technologies and Law: Legal Status of Tackling Crimes Relating to Deepfakes in India" SCC Online Blog, 16 March 2023.[scconline]