INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 5 AND ISSUE 5 OF 2025

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 5 and Issue 5 of 2025 (Access Full Issue on - https://ijlr.iledu.in/volume-5-and-issue-5-of-2025/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 5 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

"BIG DATA SURVEILLANCE AND ITS IMPACT ON FUNDAMENTAL RIGHTS UNDER THE INDIAN CONSTITUTION"

AUTHOR – SHREYANSHI* & DR. JYOTSNA SINGH**

* LL.M (CONSTITUTIONAL LAW) SCHOLAR AT AMITY LAW SCHOOL, AMITY UNIVERSITY UTTAR PRADESH LUCKNOW CAMPUS

** ASSISTANT PROFESSOR AMITY LAW SCHOOL, AMITY UNIVERSITY UTTAR PRADESH LUCKNOW CAMPUS

BEST CITATION - SHREYANSHI & DR. JYOTSNA SINGH, "BIG DATA SURVEILLANCE AND ITS IMPACT ON FUNDAMENTAL RIGHTS UNDER THE INDIAN CONSTITUTION", *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 5 (5) OF 2025, PG. 66-75, APIS – 3920 – 0001 & ISSN - 2583-2344

ABSTRACT

The exponential growth of **Big Data technologies** has significantly reshaped the landscape of **personal data management**. In India, the widespread use of **Big Data surveillance systems** by both state agencies and private corporations has raised complex constitutional questions regarding the protection of **fundamental rights** guaranteed by the Indian Constitution. This paper examines the constitutional implications of Big Data surveillance, particularly with respect to the **Right to Privacy** under Article 21, **Freedom of Speech and Expression** under Article 19(1)(a), and protection from arbitrary state action under Article 14.

The **use of surveillance tools** such as biometric identification systems (e.g., **Aadhaar**), facial recognition technologies, and real-time monitoring mechanisms raise concerns regarding **privacy violations**, **freedom of expression**, and **state overreach**. The **Right to Privacy**, as established by the **Supreme Court of India** in *Justice K.S. Puttaswamy v. Union of India*, and **Article 19** on free speech, are often at odds with the increasing intrusion of digital surveillance technologies. The paper critically assesses the impact of Big Data on these fundamental rights, emphasizing the need for stronger **legal safeguards** and **democratic oversight**.

In addition to examining legal gaps, the paper highlights the **absence of comprehensive data protection laws** and **transparent regulations** for surveillance programs. Given the absence of a unified **data protection framework** in India, this study advocates for the establishment of **institutional mechanisms** that balance the goals of **national security** with the **protection of individual freedoms**. The paper concludes by calling for an urgent legal reform to address **the challenges posed by Big Data** and proposes a framework that respects **constitutional rights** while enabling **responsible digital governance**.

Keywords: Big Data, Surveillance, Privacy, Fundamental Rights, Indian Constitution, Freedom of Expression, State Accountability, Legal Safeguards, Data Protection, Democratic Oversight.

INTRODUCTION –

In the contemporary digital age, **data** has emerged as one of the most valuable resources, often compared to oil due to its vast potential in driving economic growth and shaping policy decisions. The integration of **Big Data** technologies across various sectors—be it government, law enforcement, healthcare, or private corporations—has resulted in the unprecedented collection and analysis of personal data. This data is harvested from numerous sources, including **social media platforms**, **mobile devices**, **biometric systems**, **financial transactions**, and widespread

surveillance networks.

While the use of Big Data offers undeniable advantages in streamlining services, improving governance, and enhancing security measures, it also brings about profound constitutional challenges. These challenges primarily revolve around **privacy concerns**, the **misuse of personal data**, and the potential for state overreach. In particular, the increasing reliance on **data surveillance systems** poses significant risks to individual autonomy and freedoms. Personal data, once collected, can be processed, stored, and accessed by authorities or corporations, sometimes without sufficient oversight or accountability. As a result, there is a growing need to examine the implications of such surveillance on the **fundamental rights** guaranteed by the **Indian Constitution**.

The Indian Constitution enshrines certain **fundamental rights**, such as the **right to privacy**, **freedom of expression**, and **protection against arbitrary state action**, which are increasingly coming into conflict with the pervasive use of surveillance technologies. The **Right to Privacy**, declared a fundamental right by the **Supreme Court of India** in the landmark judgment of *Justice K.S. Puttaswamy v. Union of India*, underscores the importance of protecting individuals' personal space in the digital realm. Similarly, **freedom of expression** and **freedom of association**—critical pillars of a democratic society—are also at risk of being undermined through the misuse of surveillance tools.

This paper seeks to explore the intersection of **Big Data surveillance** and **constitutional law** in India. Specifically, it will focus on the impact of **Big Data surveillance** on **fundamental rights**, considering the evolving legal landscape, the challenges posed by such technologies, and the constitutional safeguards necessary to protect individual freedoms. Through this analysis, the paper aims to assess the balance between **national security interests** and **individual rights** while proposing reforms that ensure robust **legal safeguards** and **democratic oversight** in the age of Big Data.

2. Conceptual Framework of Big Data Surveillance

2.1 What is Big Data?

Big Data refers to the enormous volume of structured and unstructured data generated from a variety of digital sources, including social media platforms, mobile applications, surveillance systems, online transactions, financial data, GPS systems, and government databases like Aadhaar. Unlike traditional data, Big Data is characterized by its sheer volume, velocity, and variety—often referred to as the "3Vs." Additionally, Big Data involves a wide range of data types: textual, numerical, audio, video, and biometric data, making it far more complex to analyze and manage.

The significance of Big Data lies not only in its size but also in the ability to derive valuable insights from it using advanced analytical tools. Through data mining, machine learning algorithms, and predictive analytics, organizations and governments can discern patterns, trends, correlations, and associations that were previously hidden. These insights can be used to improve decision-making, optimize resource allocation, enhance services, and even predict future outcomes. In the context of governance and law enforcement, Big Data provides a tool for enhancing national security, crime prevention, and the provision of public services.

However, despite these benefits, the rapid growth and integration of Big Data into various sectors have given rise to significant concerns related to privacy, autonomy, and security. The scale of data collection and its potential for misuse pose a challenge to protecting individuals' rights, especially when surveillance becomes ubiquitous and invasive.[183]

2.2 Big Data Surveillance

[183] David Loshin, *Big Data Analytics: From Strategic Planning to Enterprise Integration with Tools, Techniques, NoSQL, and Graph* (Elsevier, 2013).

Big Data Surveillance refers to the use of data collection and analytical tools to monitor and profile individuals or groups on a massive scale, often without explicit consent. Unlike traditional forms of surveillance, which may involve the physical monitoring of individuals, Big Data Surveillance employs advanced computational techniques to observe behavior and predict actions based on large-scale data sets. It is characterized by its ability to collect, analyze, and store data from a wide range of sources in real-time, allowing for continuous monitoring of individuals and communities.[184]

Key elements of Big Data Surveillance include:

1. **Real-time Monitoring**: Data streams are constantly monitored, allowing authorities to track individuals' movements, communications, behaviors, and interactions in real-time. For instance, CCTV cameras equipped with facial recognition technology can identify and track individuals across public spaces.[185]
2. **Data Mining and Profiling**: Data mining techniques are employed to uncover patterns and correlations from vast amounts of data. By analyzing online activities, social media posts, and transaction records, authorities or corporations can build comprehensive profiles of individuals, including their preferences, habits, and potential risks. This form of surveillance does not require a specific focus on any individual but rather aggregates data to identify trends or outliers.[186]
3. **Predictive Analytics**: By using Big Data to predict behaviors, authorities can identify individuals who may be at risk of engaging in criminal activities or pose a threat to national security. Predictive policing, for example, uses historical crime data and machine learning algorithms to predict when and where crimes are likely to occur, enabling law enforcement to allocate resources preemptively. However, this approach raises concerns about bias and fairness, as predictive algorithms may reinforce existing societal inequalities.
4. **Facial Recognition and Biometric Surveillance**: Biometric technologies, such as facial recognition systems, fingerprint scanners, and iris scans, are increasingly used for surveillance purposes. These technologies can be integrated into CCTV networks, airports, and public spaces to identify individuals in real-time. While such systems can enhance security, they also raise privacy concerns, as they allow for the continuous identification of individuals without their knowledge or consent.
5. **Metadata Analysis**: In addition to analyzing content, Big Data Surveillance involves examining metadata—the data about data—such as the time, location, and frequency of communications or transactions. By aggregating metadata from mobile phones, emails, social media platforms, and online searches, authorities can gain insights into individuals' social networks, relationships, and behaviors.
6. **Mass Communication Surveillance**: Big Data techniques are used to monitor mass communication channels, including phone calls, emails, social media posts, and online activity. While this may be justified under national security or law enforcement frameworks, it often leads to a chilling effect on free speech, as individuals may self-censor their behavior out of fear of being watched.[187]

[184] European Commission, "Big Data: A New Frontier for Innovation, Competition, and Research" (2014), https://ec.europa.eu/digital-strategy/our-policies/big-data_en.
[185] Wadhwa, R. "Real-time Data Mining and Its Applications in National Security," *International Journal of Computer Science* (2018), 12(3), pp. 192-198.
[186] Gellman, Robert, "Privacy in the Age of Big Data: The Challenge to the Rule of Law," *Privacy and Data Security Law Journal* (2017), 24(2), pp. 13-17.
[187] Schneier, Bruce, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (W.W. Norton & Company, 2015), pp. 112-118.

Big Data Surveillance has expanded significantly in recent years, facilitated by advancements in computing power, storage capacity, and sophisticated algorithms. While it offers significant advantages in terms of security, governance, and efficiency, the widespread use of these technologies also raises profound questions about their impact on personal freedoms and constitutional rights. These concerns are particularly relevant in the context of India, where the right to privacy, freedom of expression, and protection from arbitrary state action are enshrined in the Constitution.

The risk of overreach by the state or misuse by private corporations is high, and the lack of transparency, accountability, and proper legal safeguards makes it difficult to ensure that these technologies are being used ethically and in compliance with constitutional principles. The need for oversight, regulation, and clear legal frameworks becomes imperative as Big Data Surveillance continues to evolve and expand.

3. Constitutional Framework in India

3.1 Right to Privacy (Article 21)

The Right to Privacy, as enshrined under Article 21 of the Indian Constitution, protects an individual's personal liberty. The landmark judgment of *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) affirmed the Right to Privacy as a fundamental right, expanding the scope of Article 21. The Supreme Court recognized that privacy is a crucial aspect of human dignity, encompassing informational privacy, which includes the protection of personal data from arbitrary state interference. This judgment specifically highlighted the need for stringent safeguards against unjustified encroachments on privacy, including the growing trend of Big Data surveillance.

In its ruling, the Court observed that surveillance mechanisms, especially those involving the collection and analysis of personal data, must meet the twin tests of necessity and proportionality. Therefore, any intrusion on privacy must be justified by a legitimate purpose, such as national security or public order, and should not exceed the scope necessary to achieve that objective. As Big Data surveillance increasingly threatens privacy through mass data collection and surveillance practices, the Right to Privacy remains a critical constitutional safeguard against state overreach.[188]

3.2 Freedom of Expression (Article 19(1)(a))

Article 19(1)(a) guarantees the right to freedom of speech and expression, a vital component of India's democratic framework. Excessive surveillance can lead to a chilling effect, wherein individuals may avoid expressing themselves freely out of fear that their communications and activities are being monitored. In the context of Big Data surveillance, the monitoring of communications, both online and offline, can restrict individuals' ability to express their opinions without fear of reprisal.

The pervasive use of surveillance tools, such as internet monitoring, social media tracking, and content censorship, may make individuals hesitant to voice dissent or engage in political discourse, ultimately undermining the exercise of their fundamental right to free expression. The Right to Freedom of Speech, therefore, requires safeguards against state surveillance that could stifle the diversity of thought and discourse essential in a democratic society.[189]

3.3 Right to Equality (Article 14)

Article 14 guarantees equality before the law and equal protection of the laws, ensuring that no person is discriminated against on arbitrary grounds. In the context of Big Data surveillance, discriminatory practices may arise, such as biased data collection and profiling based on race, religion, or other demographic factors. Algorithmic bias, inherent in data analysis processes, can perpetuate systemic

[188] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1. Mehta, Prashant. "The Right to Privacy in India: A Critique of Its Judicial Development," *Journal of Indian Law Institute* (2018).
[189] Article 19(1)(a), *Constitution of India*. Desai, Harsh. "Chilling Effects of Surveillance on Freedom of Expression in India," *National Law Review* (2019).

inequalities, leading to disproportionate surveillance or targeting of certain communities.

For instance, Big Data surveillance systems may prioritize monitoring particular social groups or geographic regions, leading to discriminatory outcomes. This practice not only violates the Right to Equality but also creates an environment where individuals or communities feel unjustly targeted, further marginalizing them in society. Hence, a legal framework for Big Data surveillance must incorporate anti-discrimination provisions to ensure fairness and equality in its application.[190]

4. Existing Surveillance Framework in India

4.1 Legal Provisions

Information Technology Act, 2000
The Information Technology Act, 2000 (IT Act) plays a pivotal role in regulating digital activities and online surveillance in India. Section 69 of the IT Act grants the government the power to intercept, monitor, and decrypt any information generated, transmitted, or stored through computer resources. This provision is often invoked to justify surveillance activities in the interest of national security, public order, or prevention of cybercrime. While these powers are intended to enhance security, they raise significant concerns regarding privacy and the potential for misuse.[191]

Telegraph Act, 1885
The Telegraph Act, 1885, remains another key legislative framework used for surveillance in India. Section 5(2) of the Act allows the government to intercept messages and communications in the interest of public safety and national security. The Act, however, does not provide a clear distinction between legal and illegal surveillance, leaving room for potential overreach. Given that much of modern communication happens digitally, the applicability of such laws to contemporary surveillance practices has come under scrutiny.[192]

4.2 Major Surveillance Projects

Aadhaar (UIDAI)
The Aadhaar project, which issues a unique biometric identification number to every Indian resident, is one of the largest biometric databases in the world. Originally launched for efficient delivery of welfare schemes, Aadhaar is increasingly being integrated into surveillance infrastructure. The database can be accessed by various government departments and private agencies, raising concerns about its potential use for mass surveillance and the unauthorized collection of personal data. The Supreme Court in *K.S. Puttaswamy v. Union of India* (2017) recognized the need for strict data protection and consent protocols surrounding Aadhaar, but its continued expansion raises questions about privacy violations.[193]

NATGRID (National Intelligence Grid)
NATGRID is a government project designed to facilitate the aggregation of data from various law enforcement and intelligence agencies, enabling real-time surveillance and analysis of individuals' activities. The project connects databases across sectors like immigration, banking, and telecommunications to track and monitor potential security threats. While it is justified as a counterterrorism measure, NATGRID raises serious concerns about the scope of surveillance and the lack of clear legal safeguards for individuals' rights.[194]

CMS (Central Monitoring System)
The Central Monitoring System (CMS) is a government-run system that allows for real-time interception of phone calls and internet activities. It is designed to monitor and track communications for national security

[190] *Ravindra K. S. v. Union of India*, W.P. (C) No. 938/2019 (Supreme Court of India). Raj, Arvind. "Algorithmic Bias and Equality: Big Data and Discriminatory Surveillance Practices," *Indian Constitutional Law Review* (2020).
[191] Sharma, Kunal. "The Information Technology Act: A Critical Review of Surveillance Powers," *Journal of Cyber Law* (2019).
[192] Chandra, P. "National Security and Privacy: A Reassessment of Surveillance Laws in India," *Indian Law Journal* (2018).
[193] Agarwal, Neha. "The Aadhaar Controversy and Data Protection: An Analysis," *Indian Journal of Privacy Law* (2020).
[194] Rai, Suman. "NATGRID: Surveillance and Its Implications for Privacy in India," *National Security Law Review* (2019).

purposes. While it is aimed at strengthening law enforcement capabilities, CMS's lack of transparency and accountability mechanisms have raised fears about potential misuse and the erosion of privacy rights.[195]

5. Issues and Concerns

5.1 Lack of Data Protection Legislation

Despite the rapid digitization and datafication of society, India continues to operate without a comprehensive and enforceable data protection framework. Although the **Personal Data Protection Bill, 2019** aimed to create a robust structure for data protection, it was widely criticized for granting broad exemptions to the State under the guise of "national security" and "public order." Eventually, it was withdrawn and replaced by the **Digital Personal Data Protection Act, 2023**. However, this new Act has also raised concerns for being vague in key definitions and lacking adequate safeguards.

One of the critical loopholes in the 2023 Act is **Clause 17(2)**, which empowers the government to exempt any of its agencies from the application of the law in the interest of sovereignty, integrity, and public order—without clearly defined procedural safeguards or judicial review. This opens the door to unaccountable data processing by state authorities. Furthermore, the Act does not provide for an independent **Data Protection Authority** but establishes a government-appointed **Data Protection Board**, compromising institutional autonomy and public trust.[196]

5.2 Absence of Judicial Oversight

Judicial oversight is a crucial element in any surveillance regime to ensure checks and balances between state power and individual liberties. However, in India, most surveillance activities, particularly those conducted under the **Information Technology Act, 2000** and the **Indian Telegraph Act, 1885**, are authorized by executive orders without any mandatory judicial scrutiny. This executive-centric mechanism, where surveillance orders are approved by government committees, lacks transparency and independence.

The **Central Monitoring System (CMS)** and **NATGRID** function without legislative backing or mechanisms for judicial review. As pointed out by civil society and legal experts, this structure facilitates mass surveillance with minimal public accountability.[197] In the absence of a "warrant" or court order requirement—unlike in jurisdictions like the United States or the European Union—India's surveillance framework fails to meet global best practices.

5.3 Disproportionate and Arbitrary Surveillance

Mass surveillance, by its very nature, involves the indiscriminate collection of data from large segments of the population, regardless of individual suspicion. This practice violates the **principle of proportionality**, which was articulated by the Supreme Court in **Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)**. The Court held that any restriction on privacy must pass a four-pronged test: legality, necessity, proportionality, and procedural safeguards.

Projects such as **Aadhaar**, when linked to services like SIM cards, banking, and welfare schemes, have led to a system of constant tracking. Likewise, the implementation of **facial recognition technology (FRT)** in public spaces—without informed consent or regulatory oversight—raises the danger of overreach, targeting, and profiling, particularly of dissenters, minorities, and activists. There is an urgent need to ensure that surveillance is not conducted in a manner that is **arbitrary, opaque, or discriminatory**.[198]

---

[195] Kumar, Ramesh. "Surveillance Technologies in India: The Case of CMS and Its Legal Implications," *Indian Cyber Law Journal* (2018).
[196] *The Digital Personal Data Protection Act, 2023*, available at: https://www.meity.gov.in/digital-personal-data-protection-act-2023
[197] Internet Freedom Foundation, *Surveillance and the Central Monitoring System*, available at: https://internetfreedom.in
[198] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, para 180–189.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 5 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

6. Comparative Perspective

6.1 European Union

The **European Union (EU)** is globally regarded as a pioneer in protecting digital rights and data privacy through its landmark regulation—the **General Data Protection Regulation (GDPR)**, which came into effect in May 2018. The GDPR provides a comprehensive legal framework that governs the collection, processing, and storage of personal data. It emphasizes **consent**, **data minimization**, **purpose limitation**, and **user rights**, including the **right to be forgotten**, **data portability**, and **rectification**.[199]

While the GDPR allows for certain exceptions for state surveillance under Articles 23 and 2(2)(d), such surveillance must still adhere to principles of legality, necessity, and proportionality. Moreover, independent **supervisory authorities** such as the *European Data Protection Board (EDPB)* monitor and regulate data processing practices to ensure compliance. The **European Court of Human Rights (ECHR)** and **Court of Justice of the European Union (CJEU)** have also acted as strong checks against indiscriminate surveillance, as seen in judgments like *Digital Rights Ireland* and *Schrems II*[200].

In essence, the EU strikes a balance between state interests and individual rights, ensuring that surveillance does not erode democratic freedoms.

6.2 United States

The **United States** maintains a surveillance regime that is primarily driven by national security concerns, particularly after the 9/11 attacks. Legislation such as the **USA PATRIOT Act**, **Foreign Intelligence Surveillance Act (FISA)**, and **USA Freedom Act** authorize extensive surveillance by agencies like the **National Security Agency (NSA)** and **Federal Bureau of Investigation (FBI)**. However, these laws are coupled with certain **institutional safeguards**.

One such safeguard is the **FISA Court**, a secret court that oversees requests for surveillance warrants against foreign spies inside the United States. While heavily criticized for lack of transparency, it still offers a layer of **judicial oversight** that is absent in India [201].Additionally, the **Fourth Amendment** to the U.S. Constitution protects citizens from unreasonable searches and seizures, forming a constitutional bulwark against arbitrary surveillance.

The **Snowden revelations** in 2013 led to increased scrutiny of U.S. surveillance practices and reforms, including limits on bulk metadata collection under the USA Freedom Act. Unlike India, **civil society organizations** and **whistleblowers** have had significant influence in shaping public discourse and reforms in surveillance laws in the U.S.

7. Judicial Responses and Public Discourse in India

India's judiciary has played a **foundational role** in acknowledging the importance of privacy in the digital age. The landmark judgment in ***Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017)** not only affirmed the **Right to Privacy** as a fundamental right under Article 21 but also introduced the **proportionality test**—mandating that any restriction on privacy must be backed by law, pursue a legitimate aim, and be necessary and proportionate to that aim.[202]

Despite this progressive interpretation, implementation on the ground has been inconsistent. Judicial directives for data protection and surveillance reform have not yet translated into robust statutory frameworks. Furthermore, **public discourse** has gained momentum through controversies such as:

- **Pegasus Spyware Scandal** (2021): The alleged use of Israeli spyware to target journalists, politicians, and activists raised alarms about state-sponsored

[199] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), available at: https://gdpr.eu

[200] *Digital Rights Ireland Ltd v. Minister for Communications*, Case C-293/12, and *Data Protection Commissioner v. Facebook Ireland Ltd*, Case C-311/18 (Schrems II)

[201] Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. §§ 1801–1885c.

[202] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1

digital surveillance. Although the Supreme Court appointed an independent committee to investigate, the findings remain partially undisclosed [203].

- **Facial Recognition in Public Spaces**: Projects like the *Automated Facial Recognition System (AFRS)* have been deployed without public consultation or legal backing, raising fears of mass surveillance and racial profiling.
- **Surveillance of Dissenters**: Instances of activists and opposition figures being monitored have led to concerns about the chilling effect on free speech and democratic participation.

Civil society organizations like the **Internet Freedom Foundation (IFF)** and **Software Freedom Law Center (SFLC)** have been instrumental in pushing for surveillance transparency, yet systemic reform remains elusive.

8. Recommendations

8.1 Enactment of Comprehensive Privacy Legislation

India urgently needs a **robust and enforceable privacy law** that can comprehensively address the challenges posed by Big Data surveillance. While the **Digital Personal Data Protection Act, 2023 (DPDPA)** represents a significant step forward, it still **provides broad exemptions to the State** under Clause 17(2), allowing the government to process personal data without consent in the name of national interest[204]. This raises concerns about unchecked surveillance and undermines the very essence of privacy as established in *Justice K.S. Puttaswamy v. Union of India* (2017).

The law must ensure:

- **Clear definitions** of personal and sensitive data.
- **Mandatory consent** for data collection.
- **Narrow and specific exemptions** for national security, with judicial approval.
- **Independent Data Protection Authority (DPA)** with investigative and enforcement powers.

Such a framework should be modeled on global best practices, particularly the **EU's GDPR**, which balances privacy with legitimate state interests[205].

8.2 Transparent Oversight Mechanism

One of the primary issues with current surveillance practices in India is the **absence of independent oversight mechanisms**. Most surveillance approvals are made by executive authorities, with little or no judicial supervision. This violates the doctrine of separation of powers and fails to protect citizens' fundamental rights.

To remedy this, India should:

- Constitute a **multi-stakeholder oversight body** comprising members from the judiciary, civil society, and technical experts.
- Ensure **mandatory judicial authorization** for intrusive surveillance actions, including phone tapping and facial recognition tracking.
- Mandate **periodic public reporting** of surveillance statistics and transparency audits.

Countries like the **United Kingdom** and the **United States** have independent oversight entities like the **Investigatory Powers Tribunal (UK)** and **Privacy and Civil Liberties Oversight Board (US)**, which could serve as models[206].

8.3 Proportionality and Due Process

The **principle of proportionality**, as emphasized in the *Puttaswamy* judgment,

[203] Supreme Court of India, *Manohar Lal Sharma v. Union of India*, W.P.(C) No. 314/2021.
[204] Digital Personal Data Protection Act, 2023, Clause 17(2), Government of India, Ministry of Electronics and Information Technology
[205] Regulation (EU) 2016/679 – General Data Protection Regulation (GDPR). Available at: https://gdpr.eu
[206] Privacy and Civil Liberties Oversight Board (PCLOB), United States, and Investigatory Powers Tribunal, United Kingdom.

must form the cornerstone of any surveillance regime. Any restriction on fundamental rights must pass the **fourfold test**—legality, legitimate aim, necessity, and proportionality[207].

Recommendations in this regard include:

- Ensuring **legal basis** for all surveillance measures through statute, not executive orders.
- Requiring **specific warrants or orders** that detail scope, duration, and purpose.
- Allowing for **judicial challenge and review mechanisms**, including ex-post facto oversight.

Surveillance must never be disproportionate or arbitrary. Instead, it should be narrowly tailored to achieve specific and justified objectives.

8.4 Citizen Awareness and Digital Literacy

A democratic society thrives when its citizens are **aware of their rights and responsibilities**. Unfortunately, digital literacy and privacy awareness remain low in many parts of India, especially among marginalized communities.

To address this gap:

- Launch **nationwide digital literacy campaigns** focused on data rights, surveillance risks, and cyber hygiene.
- Include **data privacy education** in school and college curricula.
- Encourage **civil society participation** in policy-making and public consultations related to surveillance technologies.

Conclusion

The rapid advancement and integration of Big Data technologies into the domains of governance, law enforcement, and national security have fundamentally altered the nature of surveillance in India. While these technologies offer unparalleled capabilities for predicting threats, improving public service delivery, and enhancing internal security, they also present serious risks to the **core values enshrined in the Indian Constitution**—particularly the **right to privacy**, **freedom of expression**, and **equality before the law**.

The **Justice K.S. Puttaswamy judgment** marked a watershed moment in Indian constitutional jurisprudence by recognizing privacy as a fundamental right. However, the implementation of this right in the era of algorithmic governance and mass surveillance remains deeply inadequate. Surveillance initiatives such as **Aadhaar, NATGRID, and CMS** operate with **limited transparency**, often **without clear legislative mandates**, and are **devoid of robust judicial or parliamentary oversight**. The **Digital Personal Data Protection Act, 2023**, while progressive in certain aspects, still contains broad exemptions that allow the State significant leeway to process personal data without sufficient accountability mechanisms.

Further, **algorithmic bias and discriminatory profiling** through Big Data systems risk exacerbating existing social and economic inequalities. Without meaningful safeguards, such surveillance regimes may disproportionately target vulnerable and marginalized groups, thereby undermining the **principle of equality under Article 14**. The **chilling effect** on speech and expression, too, is no longer a theoretical concern—it is a tangible reality that restricts the democratic fabric of discourse in society.

In light of these challenges, it is imperative that India adopt a **balanced and constitutionally compliant surveillance framework**—one that **respects individual freedoms while ensuring national security**. This necessitates:

- **Comprehensive and rights-based data protection legislation**,
- **Independent oversight bodies with judicial representation**,
- **Enforcement of the proportionality test**, and
- **Public engagement and awareness about digital rights**.

[207] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

Only through such democratic and legally sound reforms can India hope to reconcile the growing demands of security with the **inalienable rights of its citizens**. In the absence of timely intervention and systemic checks, Big Data surveillance could evolve into a tool for digital authoritarianism, fundamentally altering the relationship between the State and the individual. Thus, the future of India's constitutional democracy hinges on how it chooses to govern its data-driven present.

REFERENCE

- *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
- *People's Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 SCC 301.
- *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
- *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.
- Government of India, *Information Technology Act, 2000*, Section 69.
- Government of India, *Indian Telegraph Act, 1885*, Section 5(2).
- Government of India, *Digital Personal Data Protection Act, 2023*.
- Government of India, *Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016*.
- Unique Identification Authority of India. (n.d.). *Aadhaar Project Overview*. Retrieved from https://uidai.gov.in
- Ministry of Home Affairs. (n.d.). *NATGRID Project Overview*. Retrieved from https://www.mha.gov.in
- Department of Telecommunications. (n.d.). *Central Monitoring System (CMS)*. Retrieved from https://dot.gov.in
- Internet Freedom Foundation. (2020). *The Future of Privacy in India*. Retrieved from https://internetfreedom.in
- Privacy International. (2019). *State of Surveillance: India*. Retrieved from https://privacyinternational.org
- Access Now. (2021). *Surveillance and Human Rights: Country Report - India*. Retrieved from https://www.accessnow.org
- Software Freedom Law Center. (2021). *India's Surveillance State*. Retrieved from https://sflc.in
- Centre for Internet and Society. (2020). *Big Data and Privacy in India*. Retrieved from https://cis-india.org
- European Union. (2018). *General Data Protection Regulation (GDPR)*. Retrieved from https://gdpr.eu
- United States Congress. (1978). *Foreign Intelligence Surveillance Act (FISA)*.
- United Nations. (1966). *International Covenant on Civil and Political Rights (ICCPR)*.
- Solove, D. J. (2004). *The Digital Person: Technology and Privacy in the Information Age*. New York University Press.
- Zuboff, S. (2019). *The Age of Surveillance Capitalism*. PublicAffairs.
- Prasad, R. (2019). *Aadhaar: A Biometric History of India's 12-Digit Revolution*. Oxford University Press.