International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 15, Issue 01, January 2026)

Digital Surveillance and Democratic Fragility in India

Dr. Abdul Razak Kunnathodi
Assistant Professor, Department of Sociology, SGO University, Kollam

***Abstract*-- Digital surveillance has emerged as a central feature of governance in contemporary India, reshaping the relationship between the state, technology, and democratic citizenship. This article critically examines the expansion of surveillance infrastructures across social media platforms, public administration, labour management, and public health systems, highlighting how data-driven monitoring has become normalized within everyday governance practices. Drawing on policy documents, legal developments, and empirical examples, the study analyses the implications of mass, targeted, and lateral surveillance for privacy, freedom of expression, and political dissent. It argues that while surveillance initiatives are often justified in the name of national security, efficiency, and convenience, the absence of robust legal safeguards, transparency, and independent oversight has enabled the consolidation of disproportionate state power. The recognition of privacy as a fundamental right in the *Puttaswamy* judgment and the enactment of the Digital Personal Data Protection Act, 2023 represent important institutional developments; however, their limitations undermine effective protection against surveillance overreach. The article further explores emerging forms of resistance, including sousveillance and civic monitoring, as democratic counterbalances to state-led data extraction. Ultimately, the study contends that without rights-based regulation and accountability mechanisms, digital surveillance risks eroding constitutional freedoms and transforming citizens into data subjects governed through opaque technological systems.**

***Keywords*-- Digital Surveillance, Data Protection, Social Media Monitoring, Democratic Accountability, Surveillance Capitalism**

I. Introduction

Digital surveillance has emerged as one of the most pressing issues of the twenty-first century, reshaping the relationship between the state, technology, and individual rights. At its core, digital surveillance refers to the monitoring of behaviour, activities, and information through electronic systems for purposes such as information gathering, management, security, and control. This includes practices ranging from the use of closed-circuit television (CCTV) cameras in public spaces to the interception of internet traffic and digital communications. While surveillance has existed for centuries, its scale and sophistication have expanded exponentially in the digital age.

India, home to nearly 1.4 billion people, is undergoing rapid digital transformation that has deeply integrated technology into governance, commerce, and everyday life. As the world's second-largest internet market, the country has developed an extensive surveillance architecture composed of interconnected platforms and databases. These systems are often justified in the name of national security, administrative efficiency, and improved service delivery. However, they also raise serious concerns about mass surveillance and the shrinking space for privacy.

The Aadhaar system exemplifies this duality. As the world's largest biometric database, it collects fingerprints, iris scans, and demographic information of residents. Despite a 2014 Supreme Court ruling stating that Aadhaar should not be made mandatory for welfare schemes, it continues to function as a prerequisite for accessing essential services such as pensions, subsidies, and government employment. This blurred boundary between voluntary identification and compelled data submission highlights the tension between technological governance and constitutional rights.

In this context, digital surveillance in India is not merely a technical issue but a critical question of civil liberties, democratic accountability, and personal freedom. The central challenge lies in balancing legitimate security concerns with the fundamental right to privacy, ensuring that technological progress does not erode constitutional safeguards.

II. Proponents Of Surveillance

Surveillance is promoted and utilized by a wide range of actors, each driven by distinct interests. At the community level, citizens increasingly rely on surveillance tools to enhance safety. Neighbourhood CCTV networks, community watch initiatives, and mobile applications for reporting suspicious activity illustrate how monitoring practices are normalized in the pursuit of security.

Governments remain the most prominent proponents of surveillance. State agencies deploy monitoring systems for intelligence gathering, crime prevention, and the protection of public infrastructure. Surveillance is also central to criminal investigations, enabling authorities to track communications, observe behaviour, and collect evidence.

These practices are typically justified through national security and public safety narratives, though they frequently provoke debates about accountability and state overreach.

Surveillance practices extend beyond state actors. Criminal organizations engage in counter-surveillance to evade law enforcement and monitor rival groups. Religious institutions have historically employed monitoring mechanisms to safeguard property and regulate internal activities. Professional fields such as auditing also rely on systematic observation to ensure transparency and regulatory compliance.Together, these actors demonstrate that surveillance is a multifaceted phenomenon spanning state institutions, civil society, professional organizations, and illicit networks, collectively shaping contemporary monitoring regimes.

III. Methods Of Digital Surveillance

Digital surveillance encompasses a wide range of techniques designed to monitor, intercept, and analyse electronic data. Computer surveillance involves tracking internet traffic and extracting sensitive information from personal devices. Intelligence tools such as Magic Lantern and CIPAV have enabled remote access to computers without users' knowledge. At a global scale, agencies such as the U.S. National Security Agency maintain extensive data repositories, while programs such as PRISM facilitate access to data held by major technology companies.

Internet infrastructure itself is a critical site of mass surveillance. Submarine fiber-optic cables transmit vast volumes of global data traffic and have been targeted by intelligence agencies for interception. Telecommunications surveillance has also expanded through automated speech-to-text software and mobile tracking technologies such as StingRay devices, which mimic cell towers to locate phones.Visual surveillance through CCTV networks has become ubiquitous in public and private spaces. Alongside camera-based monitoring, social media platforms facilitate network mapping that reveals users' relationships, interests, affiliations, and behavioural patterns. Individuals also participate in self-surveillance by voluntarily sharing personal information online.

Biometric surveillance represents one of the fastest-growing domains. Facial recognition technologies analyse distinctive facial features, while thermal imaging systems detect emotional or physiological states. Data mining and profiling techniques further enable the construction of detailed behavioural and risk profiles. Mobile network infrastructure also contributes to surveillance through the continuous collection of geolocation data.

Radio-frequency identification (RFID) technology extends monitoring into physical environments by enabling the tracking of tagged objects, animals, and individuals. More invasive forms include implantable microchips designed to store personal information. Together, these methods illustrate the convergence of physical and digital monitoring systems into an integrated surveillance ecosystem.

IV. India's Surveillance Ecosystem

India has developed one of the most expansive surveillance infrastructures in the Global South. The Central Monitoring System (CMS) enables government agencies to directly intercept communications across telecom and internet networks. While authorities emphasize efficiency and security, critics argue that limited transparency and oversight create the risk of unchecked intrusion into private life.

The Network Traffic Analysis system (NETRA), developed by the Defence Research and Development Organisation, scans internet traffic to identify suspicious communication patterns. Similarly, the National Intelligence Grid (NATGRID), established after the 2008 Mumbai attacks, integrates data from financial institutions, transport networks, immigration databases, and telecom providers to enhance inter-agency coordination. Despite their stated security objectives, these initiatives consolidate massive volumes of personal data without adequate independent oversight.

Facial recognition technology has emerged as one of the most controversial components of India's surveillance framework. Government initiatives aim to build one of the world's largest facial recognition systems. While presented as tools for law enforcement and public safety, their deployment in public spaces raises concerns about profiling, discrimination, and political targeting.

The Pegasus spyware controversy in 2021 further exposed systemic vulnerabilities. Reports indicated that journalists, activists, lawyers, and opposition leaders were targeted using military-grade spyware. This episode underscored the urgent need for accountability and stronger legal safeguards.India's surveillance practices remain governed largely by outdated legislation such as the Indian Telegraph Act (1885), the Information Technology Act (2000), and provisions of the Code of Criminal Procedure. These frameworks were designed for a pre-digital era and fail to adequately regulate contemporary surveillance technologies, leaving critical gaps in legal protection.

V. MASS SURVEILLANCE: SECURITY, GOVERNANCE, AND SOCIAL CONTROL

Security based Surveillance

India's security infrastructure includes large-scale systems such as CMS, NETRA, and NATGRID, as well as the Automated Facial Recognition System (AFRS). Law enforcement agencies often justify facial recognition technology using broad and ambiguous categories such as "suspicious individuals" or "habitual protesters," granting wide discretionary power.

During protests against the Citizenship Amendment Act in 2019 and the farmers' movement in 2020–2021, facial recognition tools and drones were reportedly used to monitor crowds. Following the 2020 Delhi riots, facial recognition systems with low accuracy rates were deployed, raising the risk of wrongful identification and judicial errors.Mass communication surveillance has also intensified. RTI data from 2014 indicated that more than 100,000 phone interception orders were issued annually by the central government alone, raising serious concerns regarding proportionality and transparency.

Governance based Surveillance

Surveillance has become embedded within governance structures, particularly through Aadhaar. Although introduced to streamline welfare delivery, the extensive linking of Aadhaar with banking, telecommunications, and public services has enabled continuous state monitoring of citizens' activities.

Empirical evidence demonstrates exclusionary consequences. Surveys conducted by CSDS–Lokniti in 2019 reported denial of food rations to low-income households due to biometric authentication failures or Aadhaar-related issues. Concerns were also raised about proposals to link Aadhaar with the National Register of Citizens, potentially enabling mass disenfranchisement. Data security remains a major challenge. Reports of large-scale Aadhaar data exposure in 2017 revealed weak safeguards protecting sensitive personal information. Similar concerns surround emerging initiatives such as the National Digital Health ID, which consolidate highly sensitive health data.

Social Media Surveillance

In India, social media platforms have become major sites of surveillance, enabling both government agencies and private corporations to monitor users' activities with relative ease. As of 2023, the absence of a comprehensive data privacy and protection framework has left citizens' online information vulnerable to misuse.

Canadian political communication scholar Vincent Mosco describes this condition as the emergence of a "surveillance state" reinforced by surveillance capitalism, in which corporations use big-data analytics to track, profile, and monetise user behaviour. Similarly, Freedom House's *Freedom on the Net* (2019) report observed that governments worldwide increasingly rely on social media platforms to monitor citizens' opinions and political expression.

One of the most common techniques of social media surveillance is keyword and hashtag tracking. By monitoring specific terms, trending topics, and online conversations, authorities can analyse public discourse, identify emerging movements, and assess popular sentiment. Facebook's Transparency Report (2019) revealed that India ranked second only to the United States in government requests for user data. Although the Supreme Court blocked the proposed Social Media Communication Hub in 2018which aimed to centralise monitoring of citizens' online activitieslarge-scale surveillance continues through alternative mechanisms. Currently, around forty government departments reportedly have access to the Advanced Application for Social Media Analytics (AASMA), which collects live data from multiple platforms and enables real-time behavioural analysis.

The expansion of social media surveillance has been accompanied by increased restrictions on online expression. Arrests related to satire, political criticism, and dissenting opinions have become more frequent, reflecting the growing use of legal provisions to regulate digital speech. Several states have invoked sections of the Information Technology Act, including Section 66A to prosecute individuals for online posts and Section 69A to block websites, accounts, or content deemed "unlawful." These practices illustrate how legal frameworks originally designed for cybersecurity are increasingly employed to control online narratives and curb freedom of expression.

A particularly concerning development within this ecosystem is the rise of lateral surveillance, in which citizens themselves are encouraged to monitor and report one another. In February 2021, the Ministry of Home Affairs launched a programme under the Indian Cyber Crime Coordination Centre (I4C) inviting volunteers to register as Cyber Awareness Promoters, Cyber Experts, and Unlawful Content Flaggers. While the initiative was presented as a measure to strengthen cyber safety, it effectively institutionalised participatory surveillance.

Critics argue that such a framework may be exploited for political purposes, allowing individuals aligned with dominant political interests to target journalists, activists, and government critics. The structure bears similarities to China's grid-management system, which relies on decentralised community monitoring. According to data reported by Purohit (2021), 96 per cent of cases filed against 405 individuals for criticising politicians and governments over the past decade were registered after the Modi government assumed office in 2014. This trend highlights how social media monitoring and citizen-led reporting mechanisms can be weaponised to suppress dissent and reinforce existing power hierarchies.

Pandemic Surveillance: Digi Yatra and Arogya Setu

The COVID-19 pandemic accelerated the adoption of digital health surveillance tools, including geo-tagged smartphone applications and biometric monitoring systems. Among these, the Arogya Setu app became one of India's most widely used platforms for tracking COVID-19 exposure. Globally, approximately 120 contact-tracing applications were deployed across 71 countries, reflecting a broader shift toward technology-driven public health governance. In the Indian context, however, the deployment of such tools raised significant concerns regarding privacy, transparency, and data protection.

In March 2021, an RTI application filed by lawyer Saurav Das revealed that the Jammu and Kashmir administration had shared data collected through the Arogya Setu app with police authorities. This disclosure indicated a violation of the principle of purpose limitation, as data collected for public health purposes was repurposed for law enforcement. Such practices intensified public anxieties regarding the long-term storage and secondary use of sensitive personal information generated during the pandemic.

Another major development during this period was the introduction of Digi Yatra at airports in Delhi, Bengaluru, and Varanasi. The system integrates Aadhaar-based identification with facial recognition technology to facilitate contactless airport check-ins and boarding. While Digi Yatra has been promoted as a convenience-oriented innovation, it also represents a significant expansion of biometric surveillance in public spaces, raising questions about informed consent, data security, and the potential for profiling and misuse.

Attendance Applications and Workers' Surveillance

Surveillance has also intensified in the domain of labour management. In several municipalities, sanitation and public-sector workers are required to use GPS-enabled smartwatches equipped with cameras and audio-recording features. Although these technologies are framed as tools to improve efficiency and ensure attendance, they effectively subject workers to continuous monitoring, raising ethical and legal concerns regarding workplace privacy and dignity.

In January, the central government announced the mandatory implementation of the National Mobile Monitoring Software (NMMS) app for workers under the Mahatma Gandhi National Rural Employment Guarantee Scheme (MGNREGS). While the application had already been introduced in select states, the nationwide mandate institutionalised a system of pervasive digital tracking for rural labourers. Critics argue that such measures disproportionately affect vulnerable populations with limited digital access and autonomy, further expanding the surveillance capacity of the state while deepening existing social inequalities.

VI. Privacy As A Fundamental Right And Human Rights Protection

Trading privacy for promises of improved governance or convenience carries serious long-term consequences. Digital surveillance is significantly more intrusive than traditional monitoring because it enables continuous tracking of individuals' activities, social relationships, movements, emotional patterns, and even biometric indicators. In an era of expanding biometric infrastructures, data breaches, system errors, or deliberate manipulation can result in grave harms, including identity denial and exclusion from essential public services.

On 24 August 2017, the Supreme Court of India, in the landmark *Justice K. S. Puttaswamy (Retd.) vs. Union of India* judgment, recognised the right to privacy as a fundamental right protected under Article 21 and Part III of the Constitution. This ruling reaffirmed the central role of privacy in safeguarding personal liberty, dignity, and democratic freedoms. However, surveillance practices continue to disproportionately affect marginalised communities, weakening the right to dissent and constraining freedom of expression.

A major concern is the lack of transparency and accountability in existing surveillance programmes. Systems such as the Central Monitoring System (CMS) and NETRA facilitate large-scale data interception by treating the entire population as potential suspects. This indiscriminate approach undermines public trust and erodes democratic oversight. High-profile data breaches, including the Aadhaar leak of 2019, further demonstrate the risks associated with centralised databases that store sensitive personal information. The opaque and expansive nature of these infrastructures discourages political participation, silences dissent, and weakens civil society's capacity to hold authorities accountable.

Protecting human rights requires strict legal limits on how intelligence and law enforcement agencies collect and access personal data. Surveillance should be targeted, proportionate, and based on clearly defined legal standards rather than broad or speculative monitoring. Access must be restricted to specific records and communications to minimise unnecessary intrusions into individual privacy.

An essential safeguard is the clear separation of powers in data usage. Information gathered under national security provisions must not be repurposed for routine administrative or policing functions. Strong protections are also required for freedom of association, particularly against intrusive social network analysis that can expose personal relationships and political affiliations. Privacy-by-design principles, including built-in technological and operational safeguards, should be integrated into surveillance systems from their inception.

Illegal surveillance must be criminalised, accompanied by accessible legal remedies for victims. Evidence obtained unlawfully should be inadmissible in court, and whistle-blowers who expose abuses must be protected rather than penalised. These measures are necessary to ensure institutional accountability and reinforce public confidence in democratic governance.

Beyond state institutions, resistance to intrusive monitoring has also emerged through civil society initiatives. Practices such as sousveillance“watching from below”and equiveillance, where less powerful groups use monitoring tools to counter institutional power, have gained prominence. Citizens recording police actions, documenting public officials' behaviour, or using digital platforms to expose misconduct illustrate how grassroots monitoring can function as a democratic counterbalance to unchecked surveillance.

VII. DPDP Act, 2023: Progress And Limitations

The Digital Personal Data Protection (DPDP) Act, 2023 represents a significant development in India's data governance framework. While it introduces formal regulatory mechanisms for personal data processing, several provisions have generated concern among scholars and digital rights advocates.

One of the most controversial aspects of the Act is Section 17, which permits the government to process personal data without consent for broadly defined purposes such as “public order” and “national security.” The vagueness of these terms grants the state wide discretionary powers and risks normalising surveillance practices without adequate safeguards. Such exemptions undermine the core objective of data protection by weakening individual consent and accountability mechanisms.

The Act also lacks robust independent oversight and effective judicial review. Without autonomous regulatory authorities capable of scrutinising state surveillance practices, the potential for abuse remains high. Meaningful accountability requires that all surveillance activities be subject to transparent review processes, including judicial authorisation and parliamentary oversight.

Strengthening privacy protections further requires the integration of encryption, anonymisation, and other privacy-preserving technologies into data management systems. Involving civil society organisations, privacy experts, and digital rights advocates in policymaking can enhance institutional transparency and foster greater public trust in regulatory frameworks.

VIII. Conclusion

This study demonstrates that digital surveillance in India has evolved from a limited security mechanism into a comprehensive system of governance, social regulation, and political control. What distinguishes the contemporary surveillance ecosystem is not only its technological sophistication but also its normalization across everyday domains, including welfare delivery, labour administration, social media regulation, public health management, and civic participation. Surveillance has become infrastructural, routine, and deeply embedded in state–citizen relations.

The expansion of security-driven, governance-oriented, and lateral surveillance reflects a broader shift toward dragnet monitoring, in which individuals are classified, profiled, and governed through data rather than democratic consent.

While the state frequently justifies these practices in the name of efficiency, public safety, and convenience, the absence of strong legal safeguards, proportionality, and independent oversight has produced a system that disproportionately impacts marginalised populations, restricts political dissent, and weakens constitutional protections.

Although the recognition of privacy as a fundamental right in the *Puttaswamy* judgment marked a constitutional milestone, its practical implementation remains limited. Legislative initiatives such as the DPDP Act, 2023, while symbolically significant, do not adequately constrain state surveillance powers or address the structural imbalance between citizens and data-collecting institutions. Without meaningful reforms, surveillance technologies risk entrenching authoritarian tendencies within democratic governance structures.

Ultimately, the central challenge is not whether surveillance should exist, but how it should be regulated, limited, and democratically controlled. A rights-based surveillance framework must be transparent, accountable, legally constrained, and subject to continuous public scrutiny. In the absence of such safeguards, digital surveillance threatens to hollow out democratic citizenship by transforming rights-bearing individuals into data subjects governed through opaque and unaccountable systems of control.

REFERENCES

[1] J. Bailey, J. Burkell, and V. Steeves, “AI technologies, like police facial recognition, discriminate against people of colour,” Gizmodo Australia, Aug. 2020. [Online]. Available: https://www.gizmodo.com.au/2020/08/ai-technologies-like-police-facial-recognition-discriminate-against-people-of-colour/. Accessed: Feb. 17, 2021.

[2] V. Bhandari, “Facial recognition: Why we should worry the use of big tech for law enforcement,” in The Future of Democracy in the Shadow of Big and Emerging Tech, K. Bhardwaj, S. Rakshita, and S. Bhardwaj, Eds. New Delhi, India: National Law University Delhi Press, 2021, pp. 97–112.

[3] G. Bhatia, “India’s growing surveillance state,” Foreign Affairs, Feb. 2020. [Online]. Available: https://www.foreignaffairs.com/articles/india/2020-02-19/indias-growing-surveillance-state. Accessed: Feb. 21, 2020.

[4] R. Chandran, “Privacy concerns as India pushes digital health plan ID,” Reuters, Sep. 22, 2020. [Online]. Available: https://www.reuters.com/article/india-health-tech-idUKL8N2G536U. Accessed: Feb. 19, 2021.

[5] R. Radhakrishnan, ‘I took Allah’s name and stepped out’: Bodies, data and embodied experiences of surveillance and control during COVID-19 in India,” 2020. [Online]. Available: https://datagovernance.org/files/research/1606371784.pdf. Accessed: Jan. 12, 2021.

[6] S. Sardesai, “When Aadhaar-related problems lead to denial of rations and benefits: What the data show,” The Indian Express, Apr. 2021. [Online]. Available: https://indianexpress.com/article/explained/explained-when-aadhaar-related-problems-lead-to-denial-of-rations-and-benefits-what-the-data-show-7277092/. Accessed: Apr. 18, 2021.

[7] Software Freedom Law Center (SFLC), India’s Surveillance State, 2014. [Online]. Available: https://sflc.in/sites/default/files/wp-content/uploads/2014/09/SFLC-FINAL-SURVEILLANCE-REPORT.pdf. Accessed: Jan. 27, 2021.

[8] K. S. Shrivastava, “Documents show Modi government building 360-degree database to track every Indian,” HuffPost India, Sep. 2020. [Online]. Available: https://www.huffpost.com/archive/in/entry/aadhaar-national-social-registry-database-modi_in_5e6f4d3cc5b6dda30fcd3462. Accessed: Sep. 15, 2020.

[9] C. Fuchs, “How can surveillance be defined?” MATRIZes, vol. 5, no. 1, pp. 109–133, 2011.

[10] O. Gandy, “Engaging rational discrimination: Exploring reasons for placing regulatory constraints on decision support systems,” Ethics and Information Technology, vol. 12, no. 1, pp. 29–42, 2010.

[11] D. Lyon, Surveillance Society: Monitoring Everyday Life. Buckingham, UK: Open University Press, 2001.

[12] A. Marwick, D. Murgia-Diaz, and J. Palfrey, “Youth, privacy, and reputation,” Harvard Public Law Working Paper No. 10–29, 2010.