THE IMPACT OF DIGITAL SURVEILLANCE ON FUNDAMENTAL RIGHTS IN INDIA: A CONSTITUTIONAL ANALYSIS

Muskan, B.A. LL.B, S.S. Jain Subodh Law College, Jaipur

ABSTRACT

The increasing reliance on digital surveillance in India has sparked significant constitutional debates, particularly concerning the fundamental rights guaranteed under Part III of the Indian Constitution. In an era where data has emerged as the new oil, both government agencies and private entities have intensified their data collection and monitoring practices, often justifying them under the pretext of national security, public safety, and economic governance. However, such pervasive surveillance mechanisms pose serious concerns regarding individuals' autonomy, data privacy, freedom of speech, and protection against self-incrimination, all of which are core principles of a democratic society.

A pivotal moment in India's legal history was the landmark Supreme Court ruling in *Justice K.S. Puttaswamy v. Union of India* (2017)[1], which unequivocally established the right to privacy as a fundamental right under Article 21[2] of the Constitution. The judgment affirmed that privacy is intrinsic to an individual's dignity and liberty, forming an essential component of the fundamental right to life and personal liberty. Despite this judicial recognition, the effectiveness of privacy protections in the face of increasing mass surveillance remains contentious. The growing deployment of facial recognition technology, AI-driven predictive policing, and metadata analysis by government agencies has raised pressing concerns about the erosion of individual privacy and the potential for misuse of personal data.

This research paper critically examines the constitutional dimensions of digital surveillance in India, evaluating its far-reaching implications on fundamental rights. It explores the complex interplay between national security imperatives and personal liberties, recognizing the inherent tension between the state's duty to protect its citizens and the obligation to uphold their constitutional freedoms. As technological advancements continue to

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

[2] *21. Protection of life and personal liberty: No person shall be deprived of his life or personal liberty except according to procedure established by law.*

reshape the landscape of surveillance, the paper also delves into the ethical considerations surrounding emerging surveillance technologies such as Artificial Intelligence (AI), Big Data analytics, and biometric-based identification systems like Aadhaar.

Through an in-depth analysis of existing legal frameworks, judicial pronouncements, and comparative international perspectives, this paper aims to provide a comprehensive understanding of the evolving surveillance regime in India. It assesses the adequacy and effectiveness of regulatory instruments such as the Information Technology Act, 2000, the Indian Telegraph Act, 1885, and the proposed Personal Data Protection Bill in safeguarding individual privacy against unauthorized and excessive state surveillance. The study also critiques the lack of institutional oversight, highlighting the urgent need for judicial and parliamentary accountability in surveillance policies.

Furthermore, this research extends beyond legal analysis to examine the broader socio-political ramifications of digital surveillance. It investigates how mass surveillance programs shape public discourse, influence governance, and impact democratic values such as free speech, dissent, and the right to protest. The chilling effect of constant surveillance on journalistic freedom, political activism, and opposition voices is a crucial concern in the context of an increasingly digitized society.

By integrating perspectives from law, technology, and ethics, this paper argues that the unchecked expansion of digital surveillance mechanisms poses a significant threat to constitutional freedoms. It contends that while security concerns are legitimate, they must not serve as a pretext for mass data collection, warrantless monitoring, or suppression of civil liberties. Striking a delicate balance between security imperatives and individual rights is essential to ensure that technological advancements in surveillance do not come at the cost of democratic freedoms. Accordingly, this paper advocates for the implementation of robust legal safeguards, transparency measures, and independent regulatory oversight to prevent abuse and protect the fundamental rights of Indian citizens in the digital age.

Keywords: Digital Surveillance, Right to Privacy, Fundamental Rights, Constitutional Law, Artificial Intelligence, National Security, Freedom of Speech, Data Protection, Surveillance Ethics, Cyber security, Biometric Identification.

I. INTRODUCTION

With rapid technological advancements, surveillance has evolved beyond traditional methods like wiretapping to sophisticated digital monitoring through Artificial Intelligence (AI)-driven systems, Big Data analytics, and biometric identification. Governments worldwide justify these surveillance mechanisms as essential for national security, crime prevention, and administrative efficiency. However, such practices often encroach upon fundamental rights, particularly the right to privacy, freedom of expression, and due process, leading to a critical debate on the balance between state security and individual liberties.

In India, digital surveillance has gained prominence through state-led initiatives such as the Central Monitoring System (CMS), the Aadhaar biometric identification program, and the National Intelligence Grid (NATGRID). Additionally, concerns regarding unauthorized surveillance and state overreach have intensified following allegations of Pegasus spyware being used against journalists, activists, and opposition leaders. The lack of transparency and accountability in these surveillance practices has raised alarms about potential misuse and the weakening of democratic values.

A major turning point in the legal discourse on surveillance was the Supreme Court's landmark ruling in *K.S. Puttaswamy v. Union of India* (2017), which recognized the right to privacy as a fundamental right under Article 21 of the Indian Constitution. Despite this ruling, several existing laws, including the Information Technology Act, 2000, the Indian Telegraph Act, 1885, and the Unlawful Activities (Prevention) Act, 1967, continue to grant broad surveillance powers to the state with minimal oversight. The absence of a comprehensive data protection law exacerbates the risks of mass surveillance and potential violations of civil liberties.

The ethical ramifications of digital surveillance are also significant. Technologies like AI-based facial recognition and predictive policing disproportionately impact marginalized communities, raising concerns about bias, discrimination, and profiling. Additionally, constant surveillance creates a chilling effect on free speech, journalism, and dissent, discouraging citizens from expressing critical views against the government.

Given the intersection of law, technology, and ethics, there is an urgent need to scrutinize India's existing legal framework and strengthen judicial oversight to ensure surveillance mechanisms comply with constitutional principles. Reforms should include greater

transparency in government surveillance programs, judicial authorization for data interception, and an independent regulatory body to oversee surveillance practices. A well-defined Personal Data Protection law with strict safeguards against mass data collection and misuse is crucial to maintaining a rights-based approach to governance.

II. CONSTITUTIONAL FRAMEWORK AND FUNDAMENTAL RIGHTS

1. Right to Privacy: Article 21 and the Puttaswamy Judgment

The right to privacy, recognized as a fundamental right under Article 21, was solidified by the Supreme Court in *Justice K.S. Puttaswamy v. Union of India* (2017). The Court held that privacy is not an absolute right but can only be restricted by a just, fair, and reasonable law that serves a legitimate state interest. However, in the absence of comprehensive data protection and surveillance regulations, digital monitoring systems continue to operate in a legal gray area, often exceeding their intended purpose.

India's surveillance infrastructure includes programs such as:

- **Centralized Monitoring System (CMS):** Allows government agencies to intercept digital and telephonic communications without independent judicial oversight.
- **Network Traffic Analysis (NETRA):** Monitors online activities and keywords in real-time.
- **National Intelligence Grid (NATGRID):** Integrates databases from various agencies to track individuals' financial, travel, and communication details.

The Supreme Court's ruling in *Anuradha Bhasin v. Union of India* (2020) [3]reaffirmed that internet restrictions must meet the test of proportionality and necessity. However, large-scale data collection by state agencies—without meaningful legal safeguards—dilutes privacy protections, creating an imbalance between national security and individual liberties.

The Personal Data Protection Bill, 2019, which sought to regulate data collection and surveillance practices, has been replaced by the Digital Personal Data Protection Act, 2023.

[3] *Anuradha Bhasin v. Union of India, A.I.R. 2020 S.C. 1308 (India)*

However, critics argue that it grants excessive power to the state for data access and surveillance, weakening citizens' right to privacy.

2. Freedom of Speech and Expression (Article 19(1)(a))

Surveillance has a profound impact on freedom of speech and expression, a cornerstone of democracy protected under Article 19(1)(a). [4]Mass surveillance leads to self-censorship, where individuals, journalists, and activists refrain from expressing dissenting views due to fear of retaliation.

The Pegasus spyware case revealed how the government allegedly used cyber-surveillance to track opposition leaders, activists, and journalists, raising concerns about political suppression and erosion of press freedom. This case highlighted how state surveillance can be weaponized against dissent, violating democratic principles.

Key judicial precedents reinforcing free speech protections include:

- *Shreya Singhal v. Union of India* (2015): [5]Struck down Section 66A [6]of the IT Act, ruling that vague provisions restricting free speech violate constitutional rights.

- *S. Rangarajan v. P. Jagjivan Ram* (1989): [7]Held that restrictions on speech must be reasonable and necessary, rather than arbitrary.

- *Anuradha Bhasin v. Union of India* (2020): Affirmed that internet shutdowns must satisfy the proportionality test and cannot be imposed indefinitely.

[4] *19*(1)*All citizens shall have the right-(a)to freedom of speech and expression;*
[5] **Shreya Singhal v. Union of India***, A.I.R. 2015 S.C. 1523 (India)*
[6] *66A. Punishment for sending offensive messages through communication service, etc.--Any person who sends, by means of a computer resource or a communication device,(a) any information that is grossly offensive or has menacing character; or (b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device;(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine. Explanation.--For the purposes of this section, terms "electronic mail" and "electronic mail message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.*
[7] **S. Rangarajan v. P. Jagjivan Ram***, (1989) 2 S.C.C. 574 (India)*

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, have introduced new compliance obligations for digital platforms. However, critics argue that they empower the government to demand takedown of content without judicial oversight, thereby undermining free expression.

3. Protection Against Self-Incrimination (Article 20(3))

The principle of protection against self-incrimination, enshrined under Article 20(3),[8] ensures that an accused person cannot be forced to provide evidence against them. However, the rise of digital surveillance, AI-driven monitoring, and biometric databases presents new challenges to this protection.

Modern surveillance tools that raise concerns include:

- **Facial recognition systems (FRS):** Used for law enforcement and crowd surveillance without consent.
- **Biometric databases (Aadhaar, DNA profiling):** Increasingly linked to financial and government services, making refusal difficult.
- **Predictive policing and AI-driven surveillance:** Algorithms analyze behavior patterns, raising concerns over profiling and wrongful targeting.

Judicial pronouncements addressing self-incrimination in the digital age include:

- *Selvi v. State of Karnataka* (2010): [9]The Supreme Court held that narco-analysis, polygraph tests, and brain mapping without consent violate Article 20(3). Similar concerns arise with AI-based surveillance that collects personal data without consent.
- *Justice K.S. Puttaswamy v. Union of India* (2017): Warned against excessive biometric data collection that could lead to state overreach and potential self-incrimination risks.

The use of surveillance technologies in criminal investigations raises concerns over due process, as data collected without proper authorization or judicial warrants can be used as

[8] *20*(3)*No person accused of any offence shall be compelled to be a witness against himself.*
[9] *Selvi v. State of Karnataka, (2010) 7 S.C.C. 263 (India)*

evidence against individuals. This undermines the fundamental principle that the state must prove guilt rather than compel individuals to provide incriminating evidence.

III. LEGAL FRAMEWORK GOVERNING DIGITAL SURVEILLANCE

The legal framework governing digital surveillance in India is fragmented and lacks a comprehensive mechanism to regulate state surveillance and data collection. The existing laws primarily focus on national security and crime prevention but fail to provide adequate safeguards against privacy violations and arbitrary state actions. The key legal instruments addressing digital surveillance include the Information Technology Act, 2000, the Indian Telegraph Act, 1885, and the Digital Personal Data Protection Act, 2023. However, these laws often grant sweeping powers to the government, with limited judicial oversight, leading to concerns about misuse and excessive surveillance.

1. The Information Technology Act, 2000, and Its Shortcomings

The Information Technology Act, 2000 (IT Act) is the primary law governing cyber-related offenses, electronic governance, and digital transactions in India. However, it contains several provisions that enable government agencies to conduct digital surveillance with minimal accountability.

Key Provisions Related to Digital Surveillance:

- **Section 69[10]:** Grants the central and state governments the power to intercept, monitor, and decrypt digital communications if it is necessary for national security, public order, or to prevent crime.

[10] *69. Power to issue directions for interception or monitoring or decryption of any information through any computer resource.--(1) Where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do, in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource. (2) The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed. (3) The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (1), extend all facilities and technical assistance to-- (a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or (b) intercept, monitor, or decrypt the information, as the case may be; or (c) provide information stored in computer*

- **Shortcoming:** No requirement for prior judicial approval, allowing government agencies to monitor personal communications without oversight.

- **Section 69A[11]:** Empowers the government to block online content in the interest of national security or public order.
    - **Example:** Used to justify the internet shutdown in Jammu & Kashmir following the abrogation of Article 370 in 2019.

- **Section 66E[12]:** Criminalizes the violation of privacy, but the law is vague and does not impose accountability on government surveillance programs.

- **Rules under the IT Act:** The Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009, and the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, grant authorities the power to demand user data from digital platforms, further raising concerns over state surveillance.

Major Shortcomings:

1. **Lack of Judicial Oversight:** Surveillance orders under Section 69 do not require prior judicial approval, unlike in democratic countries where independent judicial review is mandatory.

---

resource. (4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine.

[11] *69A.Power to issue directions for blocking for public access of any information through any computer resource. (1) Where the Central Government or any of its officers specially authorised by it in this behalf is satisfied that it is necessary or expedient so to do, in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource.*
(2) The procedure and safeguards subject to which such blocking for access by the public may be carried out, shall be such as may be prescribed.
(3) The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.

[12] *66E.Punishment for violation of privacy. Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.*

2. **Opaque Implementation:** The government does not disclose how often or for what purpose digital surveillance is conducted, making it difficult to challenge potential abuses.

3. **Overbroad and Vague Language:** The law uses broad terms such as "public order" and "sovereignty," allowing authorities to interpret them in a manner that suppresses dissent.

4. **Absence of Safeguards:** Unlike data protection laws in developed countries, the IT Act does not mandate transparency, accountability, or redressal mechanisms for individuals subjected to surveillance.

Due to these shortcomings, the IT Act fails to adequately protect digital privacy and serves as a tool for mass surveillance without sufficient legal constraints.

2. The Personal Data Protection Bill and Its Challenges

Recognizing the growing concerns over digital privacy, the government introduced the Personal Data Protection Bill, 2019 (later replaced by the Digital Personal Data Protection Act, 2023). The bill aimed to regulate data collection, processing, and protection, inspired by global privacy standards like the General Data Protection Regulation (GDPR) of the EU.

Key Features of the Personal Data Protection Bill:

- **Definition of Personal Data:** Classified data into categories such as sensitive personal data and critical personal data, imposing restrictions on data handling.

- **Consent-Based Model:** Required companies and government bodies to seek explicit consent before collecting personal data.

- **Data Protection Authority (DPA):** Proposed the establishment of an independent Data Protection **Authority (DPA)** to oversee compliance and address privacy violations.

- **Data Localization:** Mandated that certain categories of sensitive data be stored within India to enhance data security.

Challenges and Criticism:

1. **Exemptions for Government Surveillance:**
    - Section 35 of the Bill allowed the government to exempt itself from its provisions, citing reasons such as national security and public order.
    - This effectively granted the state unchecked powers to conduct surveillance without judicial oversight, contradicting the privacy principles laid down in *K.S. Puttaswamy v. Union of India* (2017).
2. **Weak Oversight Mechanisms:**
    - The proposed Data Protection Authority (DPA) was to be appointed by the executive branch, raising concerns about its independence.
    - Unlike the EU GDPR, which has strict penalties for privacy violations, the bill lacked effective enforcement mechanisms.
3. **Data Localization Issues:**
    - While data localization aimed to prevent foreign interference in India's digital economy, it also expanded the government's control over citizens' data, increasing the risk of domestic surveillance.
4. **Lack of Transparency and Public Participation:**
    - The bill was criticized for being drafted without public consultation and for failing to incorporate the recommendations of privacy advocates and legal experts.

Due to these issues, the Personal Data Protection Bill was withdrawn in 2022 and replaced by the Digital Personal Data Protection Act, 2023, which critics argue further dilutes privacy safeguards by granting greater surveillance powers to the state.

3. International Perspectives on Surveillance and Privacy

India’s approach to digital surveillance and privacy contrasts sharply with international

frameworks, particularly those in democratic nations that emphasize individual rights and accountability.

European Union – General Data Protection Regulation (GDPR)

- The GDPR (2018) is considered the world's strongest privacy law, imposing strict requirements on how personal data is collected, stored, and shared.
- **Key Features of GDPR:**
    - **Right to be informed:** Individuals must be notified about how their data is used.
    - **Right to consent:** Data cannot be collected without explicit user consent.
    - **Right to be forgotten:** Individuals can demand the deletion of their data.
    - **Independent oversight:** Regulatory bodies enforce privacy protections, and violators face heavy penalties.
- **How India Can Learn from GDPR:**
    - Stronger independent regulatory authorities instead of government-controlled bodies.
    - Strict accountability mechanisms to prevent misuse of personal data.
    - Transparent reporting requirements to inform citizens about surveillance practices.

United States – Privacy and Surveillance Laws

- The U.S. has a mixed approach, balancing national security concerns with constitutional protections such as the Fourth Amendment (protection against unreasonable searches).
- Key surveillance laws include:

- **Foreign Intelligence Surveillance Act (FISA), 1978**: Requires judicial authorization for surveillance.
- **USA PATRIOT Act, 2001**: Expanded government surveillance but faced criticism for mass data collection programs like PRISM.
- **California Consumer Privacy Act (CCPA), 2020**: One of the strongest privacy laws in the U.S., similar to GDPR.

Lessons for India:

1. Judicial oversight of surveillance orders, as practiced in the U.S. under FISA Courts.
2. Stronger privacy legislation modeled after GDPR, ensuring user consent and data minimization.
3. Public accountability and transparency regarding how surveillance data is collected and used.

IV. ETHICAL DIMENSIONS OF DIGITAL SURVEILLANCE

The ethical considerations surrounding digital surveillance are complex and multifaceted, particularly in a democracy like India, where fundamental rights such as privacy, freedom of expression, and due process are constitutionally protected. At the heart of this ethical debate is the challenge of balancing national security and law enforcement needs with the preservation of individual freedoms. While governments justify surveillance as a crucial tool to combat terrorism, cybercrime, and other threats, the absence of clear legal safeguards and oversight mechanisms raises concerns about the potential misuse of surveillance technologies. Without proper accountability, mass surveillance can lead to widespread human rights violations, chilling effects on free speech, and the erosion of democratic values.

One of the most pressing ethical issues in digital surveillance is the use of artificial intelligence (AI) and machine learning in law enforcement. AI-driven surveillance, including facial recognition technology, biometric tracking, and predictive policing, presents serious risks of bias and discrimination. Studies have shown that facial recognition algorithms often exhibit racial, gender, and socioeconomic biases, leading to higher error rates when identifying

individuals from minority groups. In India, where marginalized communities already face systemic discrimination, such biases can exacerbate existing inequalities, resulting in wrongful surveillance, profiling, and unjust state action. The opacity of AI-based surveillance further compounds the problem, as decisions made by algorithms lack transparency and often cannot be meaningfully challenged by those affected.

Another significant ethical dilemma arises from the massive data collection practices enabled by digital surveillance. Governments and private corporations amass vast amounts of personal information through internet activity tracking, mobile phone monitoring, and biometric databases. The Aadhaar system, for instance, has been at the center of controversy regarding privacy and data security. Unauthorized access, data leaks, and the commodification of personal data expose individuals to financial fraud, identity theft, and unwarranted state scrutiny. Moreover, the lack of informed consent mechanisms further exacerbates ethical concerns, as individuals are often unaware of how their data is being collected, stored, and used. The absence of stringent data protection laws in India, coupled with broad governmental exemptions in proposed legislations like the Personal Data Protection Bill, heightens these risks.

The potential for digital surveillance to suppress dissent and curtail political freedoms also poses a serious ethical challenge. Mass surveillance programs can create a climate of fear and self-censorship, discouraging journalists, activists, and ordinary citizens from expressing critical opinions against the state. The Pegasus spyware revelations, which exposed the surveillance of journalists, opposition leaders, and human rights defenders, underscore the dangers of unchecked surveillance in a democracy. Such practices violate the fundamental principles of transparency, accountability, and the right to dissent, turning surveillance into a tool of political control rather than public safety.

To ensure that digital surveillance aligns with ethical and democratic values, there must be clear legal safeguards, independent oversight bodies, and robust public discourse on the implications of surveillance technologies. Surveillance should be guided by the principles of necessity and proportionality, ensuring that any intrusion into privacy is justified by a legitimate state interest and is conducted in the least invasive manner possible. Additionally, transparency measures must be put in place to allow citizens to challenge unlawful surveillance and seek legal redress for violations of their rights.

Public awareness and digital literacy also play a crucial role in fostering ethical surveillance practices. Citizens must be educated about their rights in the digital space, the risks associated with mass surveillance, and the legal recourse available to them in cases of misuse. Advocacy groups, legal experts, and civil society organizations must work towards strengthening data protection laws and promoting privacy-centric policies.

Ultimately, the ethical governance of digital surveillance requires a fundamental shift in the way surveillance is conceptualized and implemented. Rather than functioning as a tool for unchecked state power, surveillance mechanisms must be embedded within a framework that prioritizes human dignity, civil liberties, and the rule of law. If left unregulated, digital surveillance has the potential to undermine democracy itself, transforming a free society into one of constant state oversight and control. Therefore, a rights-based approach—grounded in legal safeguards, ethical considerations, and democratic accountability—is essential to ensure that digital surveillance serves the public good rather than becoming an instrument of oppression.

V. CONCLUSION AND SUGGESTIONS

Conclusion

The increasing reliance on digital surveillance in India presents significant constitutional and ethical challenges, requiring a delicate balance between national security and the protection of fundamental rights. While surveillance is undoubtedly a crucial tool for law enforcement and counterterrorism, its unchecked expansion raises serious concerns regarding the erosion of civil liberties, particularly the right to privacy, freedom of speech, and protection against self-incrimination. The absence of a well-defined legal framework, coupled with broad governmental powers under existing laws, has led to concerns over mass surveillance, lack of accountability, and potential misuse for political or commercial purposes.

The Supreme Court's landmark ruling in *K.S. Puttaswamy v. Union of India (2017)* established privacy as a fundamental right under Article 21 of the Indian Constitution, reaffirming the need for strict limitations on state interference in personal data and digital activities. However, the reality remains that surveillance mechanisms, whether through state-driven initiatives such as the Central Monitoring System (CMS) and NATGRID or through private entities collecting vast amounts of user data, continue to operate in a legal grey area. The proposed Personal Data

Protection Bill, though a step in the right direction, lacks strong safeguards against state surveillance and fails to establish an independent authority to regulate government access to personal data.

Moreover, the ethical implications of emerging technologies such as Artificial Intelligence (AI)-driven surveillance, facial recognition, and predictive policing further complicate the debate. The potential for bias, discrimination, and violation of due process principles necessitates urgent reforms to ensure that technological advancements do not come at the cost of democratic freedoms. Without a transparent and accountable regulatory system, digital surveillance risks being weaponized against dissenting voices, journalists, activists, and opposition figures, thereby undermining the very fabric of democracy.

To address these concerns, India must take proactive steps to establish a rights-based approach to digital surveillance. This requires legislative, judicial, and technological reforms that prioritize accountability, transparency, and proportionality in surveillance practices.

Suggestions

1. **Judicial Oversight and Independent Regulatory Mechanisms :** One of the most effective ways to prevent the misuse of digital surveillance is to establish independent judicial committees or oversight bodies that review and authorize surveillance activities. Currently, the government has broad discretion to monitor digital communications without prior judicial approval, leading to concerns over arbitrary surveillance. Implementing a system where any request for surveillance must pass through an independent judicial body would ensure that such actions are legally justified, necessary, and proportionate. Additionally, setting up an independent data protection authority with adequate enforcement powers would further strengthen oversight and accountability.

2. **Strengthening Data Protection Laws :** The enactment of a robust and comprehensive data protection law is crucial in limiting state and corporate surveillance. The current version of the Personal Data Protection Bill includes wide exemptions for government agencies, allowing them to bypass privacy protections in the interest of “national security” or “public order.” These vague terms can be misused to justify large-scale surveillance without proper safeguards. A stronger data protection law should impose

strict limitations on how government bodies collect, store, and process personal data, ensuring that surveillance practices do not infringe on individual rights. Furthermore, clear provisions should be included to provide citizens with legal recourse in case of data misuse.

3. **Transparency and Public Accountability Measures:** Transparency in surveillance policies is essential to prevent abuse and build public trust. Currently, most government surveillance programs operate in secrecy, with little public knowledge about their scope, effectiveness, or legal justification. To enhance accountability, periodic disclosures should be mandated regarding the number of surveillance requests made, the reasons for such requests, and the extent of data collection. A system similar to the transparency reports released by technology companies such as Google and Apple should be implemented at the governmental level. Additionally, affected individuals should be informed when they have been subjected to surveillance, allowing them the opportunity to challenge the action in court.

4. **Technological Safeguards to Protect Privacy:** The development and implementation of technological solutions such as encryption, anonymization, and decentralized data storage can significantly enhance privacy protections. End-to-end encryption should be encouraged for personal communications to prevent unauthorized access by both state and non-state actors. Moreover, strict regulations must be imposed on biometric data collection, particularly in large-scale government projects like Aadhaar and facial recognition initiatives. Adopting privacy-enhancing technologies can help mitigate the risks associated with digital surveillance while still allowing legitimate security measures to function effectively.

5. **Alignment with International Standards on Privacy and Surveillance:** India must look towards global best practices in privacy protection and surveillance regulation. The European Union's General Data Protection Regulation (GDPR) sets a strong precedent in ensuring transparency, accountability, and individual rights in data protection. Aligning India's data protection framework with such international standards would strengthen legal safeguards against excessive state and corporate surveillance. Additionally, India should engage in global discussions on surveillance ethics and cooperate with international bodies to formulate balanced digital rights

policies.

6. **Public Awareness and Digital Literacy Campaigns:** Educating citizens about their digital rights and privacy protections is crucial in building a more informed and resilient society. Many individuals are unaware of the extent to which their online activities are monitored or how their personal data is being used. Digital literacy campaigns should be promoted at the national level to inform people about encryption, secure online practices, and the legal avenues available to challenge unlawful surveillance. Civil society organizations, academic institutions, and legal experts must collaborate to create awareness programs that empower individuals to demand stronger privacy protections.

BIBLIOGRAPHY

- The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1.
- Vrinda Bhandari, *Right to Privacy in the Digital Age*, Oxford University Press (2021).
- Justice B.N. Srikrishna Comm., *Report of the Committee of Experts on Data Protection*, 2018 (India).