International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Digital Privacy vs. National Security: A Constitutional Dilemma

Divyanshu Raj[1], Dr Mudra Singh[2]

[1,2]Amity Law School, Amity University Lucknow Campus, Lucknow, UP

Abstract

Nowadays, in the 21st century, the skyrocketing development of digital technologies has greatly changed the ways in which information is generated, stored, and shared. Such a digital metamorphosis, with its inconvenience and connectivity never seen before, has also heightened the privacy and data security issues regarding personal information. The use of digital surveillance and data collection by governments worldwide and in India is escalating in an effort to justify national security. But such increased surveillance is at many times against the right of citizens to privacy thus bringing about an intricate constitutional conundrum.

This paper is a critical research on the conflict between national security and digital privacy in India and how the constitutional values, especially the Right of Privacy enshrined in Article 21 are synthesized with the legislations and state surveillance work. It discusses important legal treatments, including the Puttaswamy decision (2017), and state monitoring programs including CMS, NATGRID, and Aadhaar and the resulting tensions they create on a legal and ethical level.

In continuation of the same, the paper explores the possibility of maintaining national security without infringing on individual freedoms relying on the Indian and global case-laws, and the data protection principles. It ends on balanced prescriptions of produce the harmonious relationship among the privacy rights and security necessities involving the need of clear laws, court oversight and effective data protection system.

Finally, to conclude that the research at hand contends that the quest to achieve security should not serve as an excuse to allow the state to exercise its unquestioned will, and that protecting privacy should be seen as preserving the face of democracy featured Indian Constitution.

Introduction

The digital age has changed how people interact, communicate and do business in a new way. As we continually become more dependent on the internet, smart phones, and information based technologies, the amount of personal data being created and exchanged over the internet has become overwhelming. It is this digital footprint which has become a new capital resource not only to the business sector with the technology companies but also to governments wishing to protect national interests.

In this respect, digital privacy is the right of people to regulate the process of collecting, using, distributing their personal data in the digital environment. National security on the other hand is the role of the state in safeguarding its citizens against the menace of terrorism, cyber-attacks, gang violence and alien espionage. Whereas they are both needed, their existence is tense. The technologies that make people so powerful give the states the possibility to surveil and control in ways that have never been possible before.

The question of balance is a critical issue that India, as the largest democratic country in the world has to consider. Indian Constitution promises some basic rights along with Article 21, which the Supreme Court of India has come to mean the Right to Privacy in its landmark ruling of 2017 on the case Justice K.S. Puttaswamy (Retd.) v. Union of India. Yet, the national security argument is applied by the same state, to legitimize surveillance and data gathering activities a lot of the time obfuscatingly, or in ways not fully clear to legal definitions.

The goal of this paper is to examine the constitutional dilemma that is so complicated to solve, when the responsibility of the state to provide the national security seems to conflict with the right of privacy of the individual. The main argument is that though some balance is necessary, this balance can be achieved with the help of transparent arrangements, legal schemes, judiciary checks, and respect of democratic principles. In the globalized world we are living in today, the necessity to solve the arising issues of the digital world without infringing on the basic rights is more urgent than ever before.

Historical Background

The paradigm of surveillance by the state versus privacy of the person has taken many twists and turns in India. Then the country was under control of colonialist laws, such as the Indian Telegraph Act of 1885, whose mechanisms were not transparent and accountable. Privacy was not a fundamental human right that was acknowledged early in the judicial pronouncement

A landmark case is Kharak Singh v The case of State of Uttar Pradesh (1963) where the petitioner questioned the acts of police surveillance. Most of the acts were validated by the Supreme Court, though Justice Subba Rao in his dissenting opinion identified the existence of a right to privacy even in Article 21. It formed the basis of arguments in the future.

In PUCL v In Union of India (1997) based on accusations of illegal surveillance of telephone calls, the Court acknowledged the telephone conversations are confidential and they cannot be tapped at will. The judgment made it clear that procedural protection had to be ensured and ensured the presence of an oversight mechanism under Section 5(2) of the Telegraph Act to introduce a restricted facet of lawful interception.

The interpretation of legal rights to privacy has been overturned by Paradigm shift brought about when the Supreme Court ruled in Puttaswamy v. The constitutional bench judgment in Union of India (2017). A nine judge bench unanimously held Right to Privacy as a fundamental right under Article 21. The Court concluded that privacy is inherent in liberty and dignity as well as autonomy and instituted the proportionality test, of any restriction and that it should be legal, necessary and, it should be proportionate to the legitimate aim.

This case ruling did not just safeguard the citizens against unfettered data gathering but also demanded restrictions on state monitoring. It tried to institute the measures of assessing the emerging technologies and national security practices and governance of data on the constitutional front.

Even after all that progression in the jurisprudence, however, India does not have prominent legislation, which governs surveillance and regulates it and provides judicial oversight. The dilemma between constitutional principles and practical practices of the executive remains a concern to realising a balance and rights-respecting national security approach.

National Security & Surveillance Mechanisms

National security has assimilated into the most critical issue vis-a-vis the increased threat of terrorism,

cyber crime, as well as external espionage, that is, the Indian state. The government has developed a number of surveillance systems and legal tools in order to respond to such threats, though in many cases at the expense of transparency and personal privacy.

The Information Technology Act, 2000 (especially the Section 69) is one of the key legal mechanisms, and it enables the government to intercept, monitor, or decrypt any information on the grounds of sovereignty, preservation of public order or aspects of national security. Equally, telephone interception under the Section 5(2) of the Indian Telegraph Act 1885 has been permitted in very nebulous and expanded requirements usually with little checks

India has also come up with massive surveillance schemes. Central Monitoring System (CMS) allows the government to track all the telecommunications without prior consent of the telecom services providers. NETRA, designed by Defence Research and Development Organisation (DRDO) monitors traffic on the internet and gets suspicious leads when certain key words are detected. NATGRID is a surveillance framework by which data collected by several government agencies is amalgamated.

Moreover, biometric and demographic data collection programs such as Aadhaar have also presented some privacy related concerns because they concentrate sensitive information. Aadhaar in spite of its intention to provide efficient service delivery has danger of profiling and misuse since it is being integrated with other databases

According to the government, these systems are justified on the ground of national security (to safeguard the country and crime aversion). Nevertheless, the absence of judicial checks and balances, transparency, and legal protection render these tools to be vulnerable to abuse and random monitoring.

As much as the role the state plays in carrying out security is valid, the free development of its surveillance powers is dangerous to constitutional freedoms. Such mechanisms have the potential of becoming counterproductive to the democracies that they are supposed to serve without legal clarity and legal oversight.

Privacy Concerns & Constitutional Conflict

High rates of gaps between the encryption and the use of digital surveillance in India created significant concerns about the privacy of citizens and protection under the constitution. With more and more data being introduced to the world, the question of whether or not the state is allowed to keep track of the traffic of the internet, the use of mobile devices, and the communication among each other becomes highly questionable in terms of its consent, transparency, and legality.

Since India did not have a unified data protection system until the enactment of the Digital Personal Data Protection (DPDP) Act, 2023, the country has not been able to implement a trademark registration system. There were no defined regulations on what to collect and how to use and store the data which exposed the citizen to unconstitutional invasion by the government and the non-state entities. Even though the DPDP Act is an improvement, it continues to fall short of several aspects such as non-state oversight and protection against surveillance by the state.

The Israeli company Pegasus spyware was used by Indian authorities to spy on journalists, activists and opposition members which is an example of how people can be endangered through unmonitored surveillance. The press intrusion issue is that although there was the invasion of privacy, freedom of expression was chilled by the activities of Pegasus -a situation that raises the issue of freedom of expression under Article 19 of the Constitution.

In a bigger picture, due process-less digital surveillance endangers a part of the Article 21 that encompasses the right to life and personal liberty. Puttaswamy decision (2017) of the Supreme Court reiterated that privacy is a fundamental right, whereas systems such as CMS and NATGRID exist in legal grey areas and are usually unexamined by courts or even the parliament.

Besides, the government-led initiatives tend to undermine consent, which is the cornerstone of any privacy framework. It can be linking Aadhaar with a service as a requirement or policies governing data sharing being unclear, citizens do not have much control over their information.

It is an ecosystem of unchecked surveillance that portrays two competing civil interests inherent in the constitution: the state has a reason to be secure that is, in many cases, obtained in an unconstitutional way. Unless there are effective procedural safeguards, data protection enforcement, judicial oversight, etc., the online surveillance will turn into an oppression facility rather than a security instrument.

The necessity of the national security and constitutional privacy purposes to find a reconciliation is no longer optional, but a vital step towards preventing threats to democracy.

Balancing Test: Can They Coexist?

The information presented above demonstrates that digital privacy and national security are not about one having to come first over the other, but rather about maintaining a state of coexistence between the two alongside the confines of a constitutional framework. The solution here is in the rule of proportionality, which was prescribed according to the Justice K.S. Puttaswamy (2017) case. This principle means that any restriction of the right to the privacy must have a legitimate purpose, which is essential in a democratic society and needs to be proportional to aimed purpose.

However, in India, a majority of the surveillance actions do not pass this test. Due to the lack of oversight through the judicial process and post-facto accountability mechanisms the surveillance programs can run relatively transparently with greater chances of overreach. There should also be independent oversight over surveillance activities and in particular bulk surveillance or the targeting of individuals, a process that cannot be operated fully democratically unless there is the independent review of surveillance decisions specifically.

Comparative examples can be drawn using the international practices. In the US, The USA PATRIOT Act granted more surveillance abilities after the 9/11 attacks, although it has been accused of violating civil liberties. In the long run, such legal reforms were aimed at providing checks and balances, such as USA FREEDOM Act. In the meantime, the European Union maintains high privacy standards by the General Data Protection Regulation (GDPR) that has accountability, consent, and rights of individuals in data processing, even state authorities.

It is important that India should come up with its own balance through fertilization of the listed models and adherence to constitutional principles. It is not to undermine national security operations, but to put them into a legal framework of respecting rights. Any policy should rely on transparency, necessity, little intrusion, and court control regarding surveillance.

Privacy and national security is a tricky but solvable issue. It demands a political will, citizen awareness, and a system of laws, which observe the individual right of freedom and the right to safety, collectively.

Current Legal Framework & Gaps

The evolution of India as a digital governance system has not been lost, thanks to the standing release of the Digital Personal Data Protection (DPDP) Act, which in effect overrides the Personal Data Protection

Bill (PDPB) drafts. Although this is a big milestone towards the protection of citizens data rights, there are still huge loopholes in regulating surveillance, judicial oversight, and responsibility.

The DPDP Act brings very fundamental ideas of data protection which include consent, limitation of purpose and minimization of data. But it includes wide exceptions of the State so that the government can override many of these protections on the bases of national security, sovereignty, or public order. This opens the door to a broad expanse of lawless surveillance and few means of redress.

In addition, the Act does not have an independent and strong Data Protection Authority that may be able to challenge government surveillance programs by questioning or auditing such programs. This power established under the DPDP Act is found to be greatly subjective to the executive, which begs the question whether its decisions are even taken in a neutral manner.

What further compounds these problems is the fact that there are major surveillance programs that have been run without actual parliamentary law such as CMS and NETRA and NATGRID. Such schemes are based on executive orders and pre-colonial legislation, such as the Telegraph Act, 1885, and IT Act, 2000, which in no way were made to be used as a mass monitoring scheme without a particular democratic society.

The guidelines of the Supreme Court in the cases such as the PUCL v. According to the Union of India and Puttaswamy, there must be transparent legal standards, necessity and proportionality. However, India does not have a surveillance reform legislation that includes such protections.

In brief, although India has since come a long way in establishing legal frameworks to protect data, it still has a long way to go with regard to the legal vacuum that exists around surveillance. The only way to bridge this gap would be structural changes, clear laws, checks of the executive power.

Recommendations

So as to balance national security with the constitutional right to privacy, India needs to establish extensive changes in both law and institutions. The implementation of a rights based approach grounded on the values enshrined in the constitution remains relevant in order to provide the assurance that individual freedoms are not being compromised as a result of security mechanisms.

1. Passing Aggressive Determination Law

India is in an extreme state of need of a Surveillance regulation Act that defines procedures, restrictions and responsibility of state surveillance. A law on lawful interception must specify what is lawful interception, that the interception must be approved by a court of law and interception must be done in compliance to the principle of proportionality.

2. Create Independent Checking Institutions

A strong and independent Data Protection Authority should be established that can conduct audit and regulation of the surveillance efforts or schemes of the state. Parliamentary or judicial oversight committees with the purpose of inspecting surveillance requests and whether they do not exceed the legal boundaries should be established.

3. Limit the Presidential Discretion

Exemptions to the DPDP Act by government agencies have to be small in scope. Wide and vague powers delegated to the executive ought to be changed with clear directives as envisaged in the statutes and observed in transparency and proper process

4. Bring in Transparency and Public Accountability:

Regular publishing of transparency reports with details of the number, character and response of surveilla-

nce requests would be useful in gaining confidence of the people. Citizens should be allowed to know when they are being accessed except in the debatable scenarios defined as national security cases that require the monitoring authority to seek permission of the courts before data can be accessed.

5. Enhance Public Awareness and Digital Literacy:

Government and the civil society should work together to facilitate a society that is knowledgeable of digital rights. The citizens are supposed to be educated on their right to privacy, redresses, and the means of protecting themselves against the pernicious nature of surveillance activities.

6. Be in tandem with international best practices:

India must learn the standards of frameworks, such as the EU GDPR and the UK Investigatory Powers Act, to find a balance between international norms of privacy and domestic policies.

Through institutionalizing such reforms, India will be in a position to balance the national security concerns with the privacy of individuals in the digital environment at a constitutional level.

Conclusion

Digital privacy versus national security is no longer an abstract way of thinking about relations between the individual and the state, it is a defining moment of disquiet among the most important constitutional politics that we currently face in this digital era. Due to advancing technology, the ability of the state to spy on its citizens has become huge. There needs to be some form of surveillance to tackle the 21 st century challenges like terror and cybercrime but at the same time they should not be allowed to compromise the democratic freedoms and their basic rights.

In it the constitutional scheme of India, particularly post the Puttaswamy judgment (2017) makes it clear that the Right to Privacy is indeed intrinsic to the Article 21. However, the current surveillance activities have taken place in a legal black hole with no transparent guidance, judicial oversight or parliamentary checks. The discretionary application of policies like the IT Act and the Telegraph Act alongside implementation of projects like CMS and NATGRID jeopardizes to cause mistrust among citizens and violate their constitutional rights.

The next dilemma is not to decide who should have stronger control, privacy or security, but to balance both of them in principled and disproportionate ways. A democratic state must also provide that its security infrastructure is effective as well as accountable, transparent and lawful. Although a step in the right direction, the Digital Personal Data Protection Act, 2023, does not do justice to the fundamental problems of government surveillance and a regulatory body that is independent of governments.

The trend in the increasing digitization of India suggests that defending personal information and the regulation of state activity should be a national objective. The reinforcement of legal structures, empowerment of supervisory bodies, and digital literacy are the key to supporting the Constitution.

In summary, privacy versus national security is not a game of chicken. It is, however, a challenge to lawfulness, human dignity, and democratic principles of a nation. India has to step up to this challenge by ensuring that the rights-respecting mechanisms find their way into the processes of governance so that there is a coexistence of security and liberty within a just constitutional framework.

References / Bibliography

Cases & Judgments:

1. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
2. *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.

3. *People's Union for Civil Liberties (PUCL) v. Union of India*, AIR 1997 SC 568.

Statutes & Government Documents:

1. Information Technology Act, 2000 (Section 69).
2. Indian Telegraph Act, 1885 (Section 5(2)).
3. Digital Personal Data Protection Act, 2023.
4. Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

Reports & White Papers:

1. Law Commission of India, Report No. 277: *Right to Privacy*.
2. Committee of Experts under Justice B.N. Srikrishna, *White Paper on Data Protection Framework for India*, 2018.

Articles & Journals:

1. Solove, Daniel J., "A Taxonomy of Privacy," *University of Pennsylvania Law Review*, Vol. 154, 2006.
2. Singh, Rohan. "Surveillance in India: A Legal and Constitutional Analysis." *Indian Journal of Constitutional Law*, 2021.

Think Tanks & Online Sources:

1. PRS Legislative Research – www.prsindia.org
2. Observer Research Foundation (ORF) – www.orfonline.org
3. Internet Freedom Foundation – www.internetfreedom.in
4. "The Pegasus Project", The Wire, 2021 – https://thewire.in/tag/pegasus
5. European Commission: General Data Protection Regulation (GDPR) – https://gdpr.eu/