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

VOLUME 4 AND ISSUE 4 OF 2024

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

Published by

Institute of Legal Education

https://iledu.in

THE DOUBLE-EDGED SWORD: PRIVACY AND NATIONAL SECURITY IN A CONNECTED WORLD

AUTHOR - MATHEW S.N & SANTOSH ROSHAN, STUDENTS AT SASTRA DEEMED UNIVERSITY, THANJAVUR

BEST CITATION - MATHEW S.N & SANTOSH ROSHAN, THE DOUBLE-EDGED SWORD: PRIVACY AND NATIONAL SECURITY IN A CONNECTED WORLD, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 4 (4) OF 2024, PG. 677-684, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

The digital age has transformed, both in terms of national scope and individual impact, the reach of boundaries previously made between national security and personal privacy. This impact can be seen particularly in the development of India's legislation and policies accompanied by judicial interpretations. Given the threat of cyber espionage and cyberterrorism having multiplied manifold, national security operations have increasingly turned to widespread surveillance and data gathering at the cost of private rights. The rapid diffusion of modern technologies such as AI, blockchain, and IoT further intensifies the tensions and throws up new challenges towards safeguarding personal data. These improve national security capabilities but also unlock vulnerabilities that can expose private information to misuse demanding greater levels of legal protection. This paper critically reviews the nexus between national security and privacy in an Indian context, discussing key legislative frameworks. Deficiencies in the current legal and judicial system as it relates to the balance required for security and privacy are juxtaposed with the fast-emerging challenges of rapidly advancing digital technologies. The other aspect involves the moral and ethical considerations of state surveillance within governance. It argues for a more accountable, open, and proportionate way of governance. The study ended by making some proposals for change; it suggested that there should be strong laws for data protection, judicial check on surveillance, and rights for the individuals as well as risks of cyber space in this highly connected world.

Keywords: Artificial Intelligence, Blockchain technology, Cybersecurity, Internet of things, Personal Data Privacy

RESEARCH METHODOLOGY:

Statement of Research Problem:

Imbalance between Individual Privacy and National Security in certain legislations in India.

Research Objective:

The objective of this study is to analyze the statutes covering both Individual Privacy and National Security and examine the extent at which both are balanced. The Authors also aim to suggest measures to strike balance between those factors in the said statutes.

Research Gap:

The lack of balance between privacy and security in the concerned statutes involved in this study.

Research Questions:

1. What are the statutes in India concerning National Security and Individual Privacy, and which side of the fulcrum do they weigh more?
2. What measures are to be taken to strike balance between them?

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 4 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

1. Introduction:

With the increasing trend of digitalization sweeping into every corner of life, the line between national security and personal privacy grows thin. The challenge for governments both in India and around the world is that the cyber threats are growing rapidly, they include cyber terrorism and espionage as well as hacking, but all have impacts that affect not only national security but also erode the privacy of citizens. Technical advancement has provided the state access to such vast amounts of information that their handling has become a serious source of concern over the misuse of personal information. As governments amass voluminous personal data in the pursuit of counter-terrorism and public safety, pro-privacy advocates and civil liberties groups sound alarms over the potential for abuse, loss of autonomy, and erosion of constitutional rights. In this context, for India, there would be a need for a delicate interplay among legal, technical, and ethical factors to strike a balance between national security and personal privacy. This paper explores and reviews legal frameworks, key judicial decisions, public opinion, challenges, and the requirement for a more defined and balanced approach in protecting both national security and individual privacy without compromising each other.

2. Definition of National Security and Personal Data Privacy

2.1. National Security:

Coming from the traditional conceptualization, national security includes a nation's capacity to safeguard its territorial integrity, sovereignty, and citizen's wellbeing against both external and internal threats. National security, under the digital concept, includes cybersecurity. Cyberspace is one of the nation's critical infrastructures and is therefore exposed to cyberattacks that can manipulate communication networks, banking systems, and even the very defense mechanisms of the state. This has led the Indian government to place great emphasis on protecting the country's digital infrastructure from cyber-attacks by placing cybersecurity at the heart of the national security strategy.

National Cyber Security Policy-2013: In India, the protection of information, mainly in finance, defense, and public services, is emphasized as the most important concern against cyber-attacks. Preemption of terrorist activities and espionage and spreading false information and other misdeeds are considered to threaten the stability of the nation.[1030]

2.2. Personal Data Privacy

Personal data privacy is that right, individuals may claim over their personal information. Their concern is the way it collects, uses, and propagates their personal data. The kind of variety it covers-and what makes personal data and personal data privacy different in this digital generation-is from one's financial record, communication logs, health data, biometric information, and location details. This information is highly protected not only in terms of rights and autonomy but also to restrain its misuse in identity theft, fraud, or unauthorized surveillance.

In the landmark case **K.S. Puttaswamy v. Union of India (2017)**, the Supreme Court of India recognized privacy as a fundamental right based upon **Article 21** of the Indian Constitution that deals with the Right to Life and Personal Liberty. In this judgment, it was held that an individual's privacy shall be protected from unreasonable state action except when proportionate and reasonably necessary to serve a legitimate public interest.[1031]

3. Legal Frameworks in India:

India's legal framework related to national security and personal privacy is really mixed up because of numerous laws, though each of them looks to cover different facets of

[1030] https://www.meity.gov.in/writereaddata/files/National_cyber_security_policy-2013_0.pdf
[1031] (2017) 10 SCC 1

both the rights. Whereas national security issues may necessitate surveillance as well as data collection, privacy rights need protection from abuse and overreach.

3.1. National Security-Based Frameworks

3.1.1. The Information Technology (IT) Act, 2000: The IT Act is the main enactment that governs all cyber activities in India. Under **Section 69** of the IT Act, the government shall be empowered to intercept, monitor, and decrypt any information generated, transmitted, or stored in any computer resource if that is necessary for national security or sovereignty or preventing offenses like terrorism. This section is a broad surveillance provision that vests in the state very wide powers for national security, but which again has raised the specter of potential violation of privacy due to the vagaries of its definitions as well as procedural safeguards.[1032]

3.1.2. National Cyber Security Policy, 2013: This policy intends to provide security against cyber attacks on critical digital assets of India and unauthorized access. The policy focuses on the development of capability generation to produce actionable intelligence and response towards cyber threats in real time. Though it strengthens cybersecurity, it always has associated activities like surveillance and collection of data that impact personal privacy.[1033]

3.2 Privacy-Centric Frameworks:

1. **Right to Privacy**: The Supreme Court held that privacy is a right in **K.S. Puttaswamy v. Union of India in 2017**. The judgment further established that any interference with privacy is subject to the tests of **proportionality, legality, and necessity**. This, in this sense, established a robust precedent for protection of privacy in India in light of the ever-growing digitization of personal data.[1034]

2. **The Digital Personal Data Protection Act, 2023**: It is the Act that introduces legislation for the collection, processing, and storage of personal data in India. Originating from the **EU's General Data Protection Regulation (GDPR)**, it prevents the breach of personal data by private as well as public bodies. It will provide measures for the collection of data based on consent, data minimization, and limitations on processing. But it has criticized the exceptions of the Act as the government agencies include national security, which would mean weakening privacy protections.[1035]

3. **Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016**: Aadhaar is an identification system by biometrics in India, and it collects a huge amount of personal data. Thus, the Aadhaar Act could be said to indeed allow for the easy and efficient delivery of government services, but state agencies also could misuse this data. Further, in the **Aadhaar case** (2018) by the Supreme Court, Aadhaar became a limited service under welfare schemes and could not compulsorily be used for banking or telecom-type services. However, again, it strengthened protection toward privacy in respect of the possibility of surveillance.[1036]

4. **The Digital India Act, 2023**, supersedes the IT Act, 2000, as the primary regulatory framework for cyber activities in India. It introduces comprehensive provisions on user rights, trust, and safety, and addresses emerging risks from new technologies like AI, blockchain, and IoT.

The challenge in the balance between national security and personal privacy is rooted in the fact that each is critical to the health of a democratic society. National security ensures

[1032] https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf
[1033] https://www.meity.gov.in/writereaddata/files/National_cyber_security_policy-2013_0.pdf
[1034] (2017) 10 SCC 1
[1035] https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf
[1036] https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf

the safety and stability of the state, whereas the means used to secure it surveillance, data collection, and monitoring are all too frequently violations of citizen rights regarding privacy. Individual privacy is a determinant of preserving individual freedom and dignity, but extreme privacy safeguards may leave the government without access to necessary information to counter perceived threats to national security.

This tension has particularly been visible in the context of terrorism, where government surveillance is often ramped up to catch emerging threats. For instance, after the 2008 Mumbai attacks, India amplified the already advanced surveillance infrastructure it had in place to prevent such future events from happening, but once again brought up a wave of highly publicized controversies about unregulated collection and use of personal data.

To balance this, India has to work on providing laws and policies that are proportionate, clear, and strictly overseen. The measures of national security must be so constituted that they deliver without putting people's privacy abuses. Conversely, privacy laws must have well-defined exceptions for national security in such a way that these exceptions cannot be used as an opportunity to indulge in over-surveillance.

4. Gaps and Inconsistencies:

Despite all this, many loopholes and disparities still exist in current law, making it hard to strike the right balance between national security and privacy.

4.1. **Unclear Certain Definitions and General Surveillance Powers**: The IT Act has provided government agencies with such vast surveillance powers that are barely even half-defined and left not fully overseen. Generally, the phrases used are too broad and vague with wide discretionary power lying in the authority's hands, leaving an easy way out for the misuse of the surveillance power. The DIA, 2023, mitigates several gaps of the IT Act by introducing robust regulations for high-risk technologies, online safety, and accountability of intermediaries. The DPDP Act strengthens data protection with a focus on consent, individual rights, and penalties.

4.2. **Absence of Holistic Data Protection Legislation**: India does not have comprehensive legislation on data protection. The DPDP Act provides clarity where many of its concerns are attended to, but leaves much scope for exceptions on grounds of national security, unclear in definition, and therefore potentially counter to the interest of protecting individual privacy.

4.3. **No Independent Review by the Third Party**: Surveillance powers granted to the state are often administered with hardly any judicial review. Also, surveillance orders are often issued within the state organization without requiring independent authorization from a judicial entity. This means that unelected or biased bureaucrats decide whether the surveillance order is proper and what information must be collected, without sufficient third-party review of such decisions being an effective check on unmerited intrusions by the state.

5. Public Opinion and Concerns About Privacy:

Public opinion about mass surveillance and privacy varies very dramatically; it often depends on how much one is worried about national security and the perceived threat, as well as one's trust in institutions of government.[1037]

Public opinion on Aadhaar in India has been divided, While many welcome the benefits accruing to the system in creating ease of access to government services, others fear the loss of privacy and the likelihood of data breaches. Activists have documented cases of exclusion related to Aadhaar, where a person was refused welfare benefits due to authentication failure or an out-of-date record. Several such incidents led to starvation deaths.

[1037] Reddick, C. G., Chatfield, A. T., & Jaramillo, P. A. (2015). Public opinion on National Security Agency surveillance programs: A multi-method approach. *Government Information Quarterly*, *32*(2), 129-141.

And it is in this context that debate, with all its attendant scholarly hue and cry, has intensified on whether security, efficiency, or privacy should be prioritized.

6. Balancing National Security and Privacy:

Balancing the looming national security issues with those on privacy, there will be enough challenges in this rapidly changing digital landscape. These include:

1. **Technological Complexity**: Modern surveillance techniques, such as those involving artificial intelligence, data analytics, and facial recognition, allow the gathering and real-time processing of large amounts of data by governments. Even though these techniques are crucial for national security, they often

This may lead to mass surveillance, whereby the privacy of others who are not involved in any unlawful activities is violated.

2. **Unclear Legal Provisions**: The legal requirements about surveillance and data gathering under the banner of national security are unduly vague, leaving it almost impossible to determine whether or not the activities of the state are proportionate and necessary. Most legal frameworks do not offer clear criteria for when one should justify surveillance or how long data collected should be kept.

3. **Public Trust**: This means that too much government surveillance undermines public trust in such institutions. Erosion of trust takes place in the governing framework because citizens expect their rights to be protected, which includes the right to privacy. Overall, there would be a depressed form of state functioning in the event that surveillance is perceived as invasive or excessive when there is a lack of trust in government.

7. Impact of Cyber Security on Individual Privacy:

Therefore, while indispensable for protecting national infrastructure, cybersecurity measures involve scope for important data collection and surveillance activities. For example, India's **Central Monitoring System** (CMS) and **Netra** systems have allowed the government to tap the metadata of telecommunication activities as well as online activities for security purposes. Netra is an advanced surveillance system that analyzes internet traffic to identify certain keywords to signal criminal or terrorist designs. Systems such as these may seem necessary in this new digital world but bring with them grave threats to often blindly target individuals without due process and flagrantly infringe upon the right to privacy.[1038] More broadly, it is also observed that the content of malware detection and network monitoring cybersecurity systems developed for the prevention of cyberattacks scans massive volumes of data which may include personal communications.

One of the main fears is that the cybersecurity measures would collect more information than needed to satisfy the national security services. This is worsened by the fact that most cybersecurity measures are enforced without the individuals' clear consent, and information collected can be used for unproportional purposes aside from security. For instance, while the Aadhaar biometric database was designed to make welfare delivery efficient, it has been criticized for being used predominantly for surveillance over its original mandate.

The second is that data collected under what appears to be the auspices of cybersecurity quite often lacks protection against wrongful use. Because cybersecurity measures are supposed to protect the state against the external threat, they also have created an enhanced risk of internal exploitation when the rules for protecting data come into conflict.

[1038] Bignami, F., & Resta, G. (2018). Human rights extraterritoriality: the right to privacy and national security surveillance. *Francesca Bignami & Giorgio Resta, Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance in Community Interests Across International Law (Eyal Benvenisti & Georg Nolte, eds., Oxford University Press, Forthcoming), GWU Law School Public Law Research Paper, (2017-67), 2017-67.*

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

VOLUME 4 AND ISSUE 4 OF 2024

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

Published by

Institute of Legal Education

https://iledu.in

Balance of power between the state and its citizens: State surveillance, an ethically contested issue on privacy The balance of power between the state and its citizens quite often lies heavily in favor of the former. Powers of state surveillance are largely classified, and little transparency accompanies their operations. Ethical questions arise over how far a government may push in the collection and exploitation of personal data and whether individual privacy may be sacrificed in the name of national security.

The last of the troubling issues is "mission creep" and the concern thereof. Systems of surveillance established for purposes of national security may in fact end up being used for unrelated purposes of political control or censorship. Use of surveillance for such contrary purposes thwarts democratic values and violates the trust relationship between citizens and state institutions.

In this regard, balancing these ethical issues involves developing and setting a proper legal framework that provides for transparency, accountability, and proportionality in the actions of the state. The state must prove the relevance of surveillance using concrete realities of danger to national security, and there must be adequate oversight mechanisms to prevent situations of an abuse of power.

8. Emerging concerns as a result of high digitization:

Cybercrime has faced a rate of increase that has never been experienced. In an increasingly technical world, individuals and businesses are being hacked, phished, their identities stolen, doxxed, and there is overall digital payment frauds. India does not have any law that tackles the issue related to all concerns for this digital sphere so far. Thereby, victims will have to depend on Indian Penal Code, 1860 sundry crimes such as theft, forgery, voyeurism, stalking, and criminal intimidation, apart from the provisions of the Information Technology Act, 2000 (act), and its ancillary rules. They so far have been completely inept in countering the issues arising from the rising complexity in technology and interference with such criminal acts. The advent of the Bhartiya Nyaya Sanhita, 2023 (BNS), has not seen drastic changes in the dealing with cyber crimes, except the updating on selling obscene books to incorporate contents in electronic form and the introduction of cybercrimes in the organized crime offense. It has popularly taken the crimes in the IPC as amended by the act.

The DIA envisions an 'open, safe, and accountable internet' by categorizing intermediaries, regulating high-risk AI systems, and enhancing user safety. The DPDP Act complements this with stricter data protection measures.

It focused mainly on specific cybercrimes such as identity theft, impersonation fraud, hacking, and data breaches, making it a bit more computer-centric. It does not adequately address the many new risks, especially advanced persistent threats and complex phishing scams. The slow approach to cybercrime, starting as early as June 2000, only dealt with three offenses: tampering with computers and systems, hacking, and distributing obscene content. It was only in 2008 that it was amended to include sending offensive messages via communication servers, fraudulently receiving a stolen computer resource or communication device, identity theft, privacy violation, and cyber terrorism with the introduction of sections 66A to 66F and sections 67A to 67C.

As such, the provisions of this act apply only to the uniqueness of the first generation and not the savviness of the present regarding technology because the well-coordinated, advanced, and organized cyber crimes committed by organizations of other countries go unheard and unpunished. Proper systems, including the assessments, administration, and monitoring of progress in the launching of new technologies like blockchain, generative artificial intelligence, datafication, and the

internet of behavior, are lacking, which may have a huge impact and risk.

These problems called for the government to bring forth the Digital India Act, 2023; otherwise referred to as the DIA for short back in March 2023. This was aimed at supersede the law while establishing flexible legislation responsive to the ever-changing landscape of technology and adjusting to the country's digital systems. Administrative acknowledgment is done for not being able to keep pace with the fast-changing cyberspace, and the DIA seeks to address that problem. The general aim of the law is to make the net safer, categorize intermediaries, ensure an equitable and transparent internet, and advocate for more accountability. However, it does not provide any instruction to achieve those purposes.

While India stands second after China as regards the number of internet users, there is still quite a distance to go before comprehensive cyber security legislation such as the DIA comes into effect. The Ministry of Electronics and Information Technology seems to be holding discussions to introduce comprehensive legislation for the entire digital ecosystem or propose multiple targeted acts in order to take care of cyber-crime more effectively.

Being the third largest digitally transformed nation in the world, India is also on the hit list of phishing attacks on a third place basis. To be seen in a thoughtful and collaborative manner while being inclusive of the ideas brought about by jurisdictions with similar laws, such as the Digital Services Act of the European Union and Online Safety Act of the United Kingdom, would be utterly unrequired for the DIA or any other law proposed.

8.1. Jurisdictional issues:

Jurisdictional challenges are high, because cybercrime frequently transcends the borders of countries. With the easy-to-use geographical flexibility enjoyed by cybercriminals, it can be easy for him to penetrate any country, including India, from any other country to victimize people there. Besides, Indian law enforcement agencies find it difficult to investigate and prosecute such crimes. International cooperation and treaties are necessary but slow and cumbersome.[1039]

9. Key Recommendations to Balance National Security and Personal Privacy in India:

9.1. **Express Consent and User Rights:**

Companies and public authorities must obtain explicit consent before collecting personal data and provide users with rights to access, correct, and delete their data. Non-compliance should result in significant penalties to deter misuse of personal information.

9.2. **Surveillance Reform with Judicial Oversight:**

Government surveillance must have independent judicial oversight to prevent privacy violations. Surveillance should be conducted under clear legal provisions, following the K.S. Puttaswamy v. Union of India (2017) guidelines (Legality, Need, Proportionality), with citizens having access to legal remedies if their privacy is infringed.

9.3. **Global Best Practices and Data Minimization:**

India should draw from global frameworks like the EU's GDPR to strengthen privacy protections, implementing data minimization and anonymization practices to ensure only necessary data is collected, reducing the risk of misuse.

9.4. **Organizational Accountability and Risk Mitigation:**

Organizations must be held accountable for how they handle personal data through robust frameworks. Technical safeguards such as encryption and regular audits should be mandated to mitigate risks associated with data breaches.

[1039]https://lawbhoomi.com/challenges-to-indian-law-and-cyber-crime-scenario-in-india/#Challenges_to_Indian_Law

9.5. **Public-Private Collaboration and Privacy by Design:**

A collaborative approach between government, private sectors, and civil society should be promoted to create balanced policies. Incentivizing the integration of privacy-by-design principles into system development would ensure data protection from the outset.[1040]

9.6 **Updating legal frameworks:**

It is crucial in adapting to the rapid advancement of blockchain technology, big data, and quantum computing. These technologies, while highly efficient and robust, throw up new vulnerabilities that law might not fully be equipped to address, including the quest that a quantum computer will crack existing encryption, and the decentralized nature of blockchain technology. Cybercrime may take advantage of the regulatory gaps existing while the enormous volume of big data necessitates stronger privacy and data protection laws. There also needs to be an element of cooperation among countries and the realization that regulations must be harmonized to facilitate global cybersecurity strategies and cross-border enforcement mechanisms. Updating the laws and revising the same according to the incorporation of these emerging technologies ensures both national security along with personal privacy in this digital era.

Conclusion:

Thus, balancing national security with personal privacy is a complex, dynamic challenge in India. While there exist safeguards as well as exceptions in the legal frameworks for national security, there are many loopholes, uncertainties, and inconsistencies that still need to be worked upon. Vulnerability exists in the absence of fully enacted and effective data protection legislation, broad surveillance powers, and inadequate judicial oversight, all of which may lead to erosion of such privacy rights.

The effect of this balance can be maintained only if national security measures are seen as transparent, proportionate, and under strict oversight. It is also quite necessary that India enact comprehensive data protection laws that in a careful manner balance national security with privacy so that neither of these is given up. Ethical considerations, public trust, and accountability must guide further development of laws and policies in this area. By doing so, India could ensure both national security and fundamental rights for its citizens in the emerging digital world.

[1040] Jahan, K. T., & Reyad, Z. H. (2024). Safeguarding Privacy in the Digital Era: Finding the Balance in India.