INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW

Volume 4 | Issue 1 Art. 11

2025

National Security vs. Individual Rights: A Balanced Approach in India

Mohan Kumar N and Jyotirmoy Banerjee

Recommended Citation
Mohan Kumar N and Jyotirmoy Banerjee, *National Security vs. Individual Rights: A Balanced Approach in India*, 4 IJHRLR 142-156 (2025).
Available at www.humanrightlawreview.in/archives/.

National Security vs. Individual Rights: A Balanced Approach in India

Mohan Kumar N and Jyotirmoy Banerjee

LLM Student, Amity Law School, Amity University, Bengaluru
Assistant Professor, Amity Law School, Amity University, Bengaluru

Manuscript Received	Manuscript Accepted	Manuscript Published
04 Jan. 2025	06 Jan. 2025	08 Jan. 2025

ABSTRACT

A comprehensive study over the concept of security and liberty must begin with the legal and political framework of India. India inherited an intricate surveillance system, shaped by colonial influences, notably through the Indian Telegraph Act of 1885 and the Information Technology Act of 2000, which were modeled after the evolving legal frameworks in Great Britain. With the advent of the digital revolution, India has implemented a range of surveillance systems, including the National Intelligence Grid (NATGRID), Centralized Monitoring Systems (CMS), air traffic surveillance (NETRA), and Aadhaar (the unique biometric identification system). These systems, mirroring global trends, have prompted concerns regarding the delicate balance between privacy and security. The Supreme Court of India, in its landmark ruling in Justice K.S. Puttaswamy (Retd) v. Union of India, recognized privacy as a fundamental right, underscoring the importance of proportionality, legality, and necessity when state actions infringe upon an individual's privacy. This ruling has significantly influenced the ongoing discourse on surveillance, which revolves around the tension between monitoring for safeguarding liberty and maintaining security. The balance between these competing objectives evolves in response to shifts in legal frameworks over time. The recent passage of the Personal Data Protection Bill exemplifies this dynamic, acknowledging the complex tension between upholding privacy rights within the democratic legal framework and ensuring the need for security and surveillance in an increasingly digitized society. This ongoing legislative development reflects India's commitment to evolving its laws in line with the challenges of privacy protection and data security.

KEYWORDS

Surveillance, Privacy, National Security, India, IT Act Aadhaar, NETRA, NATGRID.

INTRODUCTION

India's complicated legal systems, pluralistic democracy, and technology improvements all influence the country's debate over privacy and monitoring. The Telegraph Act of 1885, which permits monitoring activities, and the IT Act of 2000 are part of India's regulatory structure. Despite facilitating data collection for security and administration, tools like Aadhaar, the Central Monitoring System (CMS), NETRA, and NATGRID create privacy concerns.

Privacy was acknowledged as a basic right under personal liberty by the Supreme Court in its historic ruling in *Justice K.S. Puttaswamy v. Union of India*[1], which mandated that surveillance adhere to the legality, reasonableness, and proportionality standards. For democracy and the rule of law to be upheld, privacy and national security must be balanced. If left uncontrolled, surveillance runs the risk of turning into a surveillance state, despite being essential for safeguarding society and counterterrorism. The civil freedoms may be undermined by a surveillance state brought on by unchecked secret police surveillance. In order to minimise misuse, surveillance must be required, minimally invasive, and subject to court review, as well as judicial monitoring, proportionality, and legality. Achieving a balance between privacy and security is essential to preventing a authoritarian system or institutional mistrust.[2]

It is difficult for governments to manage private areas openly without running the danger of human rights abuses or security breaches. To resolve these conflicts, cooperation and democratic principles are essential. To stop the misuse of surveillance authority, there must be strong monitoring and oversight by the judiciary. The proposed Personal Data Protection Bill seeks to safeguard individual rights, create a regulatory body, and improve data protection. Laws and frameworks must be updated frequently to reflect changing democratic values and technological advancements.[3]

[1] Justice K.S. Puttaswamy & Anr. vs. Union of India (2017) 10 SCC 1.
[2] Digital Surveillance and the Threat to Civil Liberties in India, https://www.giga-hamburg.de/en/publications/giga-focus/digital-surveillance-and-the-threat-to-civil-liberties-in-india (last visited Jan 2, 2025).
[3] Understanding India's New Data Protection Law, Carnegie Endowment for

THE EVOLUTION OF DIGITAL SURVEILLANCE IN THE 21ST CENTURY

Since the IT Act of 2000 was introduced, surveillance in India has undergone tremendous change due to the digital age. This act opened the door for sophisticated monitoring powers driven by the internet and digital technology revolution by granting legal legitimacy for digital signatures, electronic records, and cybercrime. The massive operations digital surveillance initiatives including the NETRA program, CMS, NATGRID, and the biometric database Aadhaar have been put into place in India. These programs use technology to gather and analyse enormous volumes of data in an effort to expedite service delivery, strengthen national security, and foster better governance. But these actions, particularly with regard to privacy, have drawn a lot of criticism and legal attention. Critics contend that these programs frequently lack sufficient protections and transparency, which fuels concerns about abuse and overbearing government control[4].

But a significant change was brought about by the ruling *in Justice K S Puttaswamy (Retd) v. Union of India*[5]. It stated that the Indian constitution's guarantee of privacy is a basic right. Since the Supreme Court's 2017 ruling, there has been a heated discussion concerning the purposes, legitimacy, and acceptability of digital surveillance. In this case it has reaffirmed the necessity to strike a balance between governmental monitoring and the fundamental right to privacy, as highlighted by domestic and legal remarks.

India's surveillance history shows how colonial regulatory frameworks gave way to contemporary digital monitoring, which changed through law to meet emerging issues. Current discussions about striking a balance between personal privacy and national security are contextualised by this continuity. It is essential to have a complex framework that is influenced by India's history, democracy, and rule of law. The state must protect individual freedoms while maintaining security if India is to prosper as a democracy. India has to carefully establish the limits of surveillance in the digital era, focussing on concerns about misuse and striking a balance with the rights to privacy and the

International Peace, https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en (last visited Jan 2, 2025).

[4] Vrinda Bhandari & Karan Lahiri, *The Surveillance State: Privacy and Criminal Investigation in India: Possible Futures in a Post-Puttaswamy World*, (2020), https://papers.ssrn.com/abstract=3580630 (last visited Jan 2, 2025).

[5] Supra Note.1

grievances of its inhabitants.[6]

LEGAL FRAMEWORK GOVERNING SURVEILLANCE IN INDIA

In India, the legal framework that permits surveillance is a patchwork of colonial-era laws, modern legislation, and seminal court rulings that require the state's security needs to be weighed against the fundamental rights of its citizens. With the advancement of technology and societal shifts, these conflicts are occurring more frequently.

- ***Constitution of India Fundamental Rights and Privacy***

Numerous essential rights that safeguard the private rights of Indian citizens are found in the Constitution, which is the country's highest law. Although the right to privacy is not explicitly stated in the Constitution, the Supreme Court of the nation has made it clear time and again via case law that privacy is a necessary component of the right to life and liberty as guaranteed by Article 21 of the Constitution. The right to privacy was ultimately recognised as a fundamental right in the recent decision in the Justice K S Puttaswamy case, which subtly upheld the constitutional standing of individual liberty, bodily integrity, and personal judgement. The ruling also established a precedent that all monitoring methods, both present and future, must adhere to the privacy rights threshold[7].

- ***Article 21. Protection of Life & Personal Liberty***

No person shall be deprived of his life or personal liberty except according to procedure established by law. Article 21 of the Indian Constitution guarantees the fundamental right to protection of life and personal liberty. It ensures certain safeguards against arbitrary deprivation of life and liberty[8].

The right to life and personal liberty, including the right to privacy as construed by the judiciary in various cases, are guaranteed by Article 21 of the Indian Constitution. The Supreme Court adopted a three-pronged approach for determining the legitimacy of privacy invasions in the historic 2017 Justice Puttaswamy case ruling

1. A legitimate law must support the invasion.

[6] Divyanshu Dembi, *Privacy & National Security: A Balancing Act?*, (2021), https://papers.ssrn.com/abstract=3953357 (last visited Jan 2, 2025).
[7] Gautam Bhatia, *State Surveillance and the Right to Privacy in India: A Constitutional Biography*, 26 National Law School of India Review (2014).
[8] Constitution of India 1950, art. 21.

2. The law must have a "legitimate" and "necessary" purpose.
3. In order to prevent undue interference, the measures of the legislation must be proportionate to the purpose[9].
4. The constitutional criterion for determining whether surveillance operations in India are lawful is currently this framework.

- ***IT Act, 2000: Provisions for Digital Surveillance and Data Protection***

One important component of Indian law that regulates data security, cyber activity, and digital monitoring is the IT Act, 2000. It gives the union government or its designated representatives the power to monitor, intercept, or decrypt information sent or stored by computer systems. The use of this authority is permitted for the purposes of public order, defence, national security, or the prevention of specific criminal activity; nevertheless, prior authorisation is necessary to guarantee that monitoring is justified and not capricious.

a) **Section 69** Power to issue directions for interception or monitoring or decryption of any information through any computer resource[10].
b) **Section 69A** Power to issue directions for blocking for public access of any information through any computer resource[11].
c) Section 69B Power to authorise to monitor and collect traffic data or information through any computer resource for cyber security[12].

Some of the important sections in the IT Act, such Section 69, give the government the authority to require third parties, such as social networking sites and telecom providers, to access, track, or decrypt data for purposes of public order or national security. While Section 69B permits real-time traffic data monitoring to strengthen cybersecurity, Section 69A permits the government to restrict accessibility to online content judged detrimental to national sovereignty. These clauses create questions regarding the scope of monitoring power while also attempting to safeguard the interests of the state and react quickly to security risks.

The IT Act has drawn criticism for its ambiguous clauses and shortage of procedural safeguards, despite its significance

[9] Supra Note.1
[10] Information Technology Act, 2000, Sec. 69.
[11] Information Technology Act, 2000, Sec. 69A.
[12] Information Technology Act, 2000, Sec. 69B.

in maintaining national security. Because Sections 69, 69A, and 69B do not explicitly outline the parameters or extent of surveillance, there is potential for abuse. Furthermore, as shown in the Puttaswamy case, the lack of an independent supervision body calls into question accountability and transparency, particularly with regard to privacy rights. The Act needs to be updated to include greater protections, more precise definitions, and a balance between the safeguarding of individual private rights and monitoring activities[13].

- ***The Telegraph Act, 1885 and The Indian Post Office Act, 1898: Surveillance of Communications***

Early legislation pertaining to communication monitoring in India include the Indian Telegraph Act of 1885, the Indian Post Office Act of 1898, and the Indian Wireless Telegraphy Act of 1933. According to these Acts, the government may intercept wireless communications, postal goods, and telegraph messages for public order, defence, foreign policy, and national sovereignty purposes. They were developed before the advent of digital technology, but judicial interpretations still use them in contemporary communication technologies. But in the digital age, many rules have grown antiquated, which raises questions about how well they regulate digital communication. Demand for their modernisation is rising in order to better safeguard citizens' right to privacy while juggling the demands of national security. To guarantee that the legal system keeps up with technical advancements and safeguards privacy for individuals in the digital age, these Acts must be updated.

- ***The Aadhaar Act, 2016: Biometric Data and Privacy Concerns***

In order to facilitate digital governance, the Aadhaar Act of 2016 seeks to give citizens a unique identity system via which they can access subsidies and services. However, the gathering and use of biometric data raises privacy issues, leading to requests for more robust safeguards to protect people' privacy while weighing the advantages of Aadhaar's targeted delivery system.[14]

With continuous discussions over the effects of technology on privacy, India's legislative framework for surveillance

[13] Chandak, L. (2017). Privacy and Data Security – a National Need. Retrieved from https://trai.gov.in/sites/default/files/Span_Technology_07_11_2017.pdf.

[14] Privacy Concerns with Aadhaar – Communications of the ACM, (Nov. 1, 2019), https://cacm.acm.org/research/privacy-concerns-with-aadhaar/ (last visited Jan 2, 2025).

strikes a difficult balance between the rights of individuals and the interests of the state. In a democratic setting, the legislature and courts continue to balance these conflicting objectives in their efforts to safeguard individual liberties and national security[15].

- ***Digital Personal Data Protection Act, 2023 (DPDP Act): Implications for surveillance and privacy***

The Digital Personal Data Protection Act, 2023 (DPDP Act), which was introduced to control data processing and safeguard individuals' privacy in the digital era, is a noteworthy breakthrough in this area. The structure for the rights and responsibilities of people (Data Principals) and organisations (Data Fiduciaries) with regard to personal data is established by the DPDP Act. By regulating the handling of personal data, it aims to avoid unwarranted surveillance and guarantee privacy, which is a step forward in protecting digital privacy while still meeting the demands of national security and governance.[16]

GOVERNMENT EXEMPTIONS AND SURVEILLANCE CONCERNS

The absence of clear guidelines for establishing such exemptions is an issue raised by the Digital Personal Data Protection Act, 2023's provisions that exempt the government from some surveillance protections. Although the Act attempts to protect privacy, it leaves out sections pertaining to foreign data processed in India and makes exclusions for supervisory and governing organisations without explicit guidance. This could have an impact on international collaboration and confidence, especially with organisations like the European Union.[17]

In order to supervise data protection measures, the Act also requires the establishment of the Data Protection Board of India (DPBI). It can't, however, create dynamic privacy regulations in reaction to technology advancements because its authority is restricted to an adjudicatory role.[18] The Act has drawn criticism

[15] The Real Struggle for Privacy and National Security in terms of Liberty and Surveillance, The Amikus Qriae (Jun. 30, 2023), https://theamikusqriae.com/the-real-struggle-for-privacy-and-national-security-in-terms-of-liberty-and-surveillance/ (last visited Jan 2, 2025).
[16] Pam Dixon, *A Failure to "Do No Harm" -- India's Aadhaar Biometric ID Program and Its Inability to Protect Privacy in Relation to Measures in Europe and the U.S.*, 7 Health Technol (Berl) 539 (2017).
[17] The Digital Personal Data Protection Act of India, Explained - Future of Privacy Forum, https://fpf.org/, https://fpf.org/blog/the-digital-personal-data-protection-act-of-india-explained/ (last visited Jan 2, 2025).
[18] Understanding India's New Data Protection Law, Carnegie Endowment for

for its lack of adequate supervision procedures and for giving the government exclusions that could jeopardise privacy rights. Additionally, it has drawn criticism for providing "half-baked protections." The Act sets monetary sanctions for non-compliance and mandates data handling agreements for outsourcing. It gives people greater authority over their personal data and encourages appropriate data handling.[19]

LANDMARK JUDGMENTS AND THEIR IMPACT ON SURVEILLANCE AND PRIVACY

India's stance on privacy and surveillance saw a dramatic shift with the *K.S. Puttaswamy v. Union of India* case. A nine-judge Supreme Court panel unanimously decided that, in accordance with Article 21 of the Indian Constitution, which protects the rights to life and personal liberty, the right to privacy is a basic right. By overturning earlier rulings that had dismissed privacy as a fundamental right, this ruling established that privacy is essential to personal freedom and dignity. Important guidelines that influence India's legal system on privacy and surveillance were established by the Puttaswamy ruling-

1. Since privacy is a fundamental right, it is given the strongest legal defence against capricious government actions.
2. The Court established three requirements for any government action that can violate privacy it must be proportionate (use the least restrictive measures to accomplish its goal), necessary (serve a legitimate state interest), and legal (have legal support).
3. The ruling underlined the significance of protecting personal information and suggested the development of strong regulations to stop the unauthorised use of people's data[20].

India's surveillance laws and practices have been influenced by this historic decision, which raised the threshold for state intervention and had an impact on later privacy and data protection legislation.

The Apex Court examined the legitimacy of the Aadhaar

International Peace, https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en (last visited Jan 2, 2025).

[19] Understanding the Digital Personal Data Protection (DPDP) Act: A Comprehensive Guide for Businesses, https://www.zscaler.com/blogs/product-insights/understanding-digital-personal-data-protection-dpdp-act-comprehensive-guide (last visited Jan 2, 2025).

[20] Supra Note.1.

project following the 2017 privacy ruling in *K.S. Puttaswamy* case. The Court ruled that the requirements for Aadhaar for bank accounts and mobile connections were excessive and infringed upon private rights, but it upheld the use of Aadhaar for government assistance programs and PAN linkage.[21] The ruling emphasised that the collecting of biometric data must adhere to the legality, need, and proportionality requirements to prevent arbitrary invasions of privacy[22].

Implementing rules prohibiting arbitrary phone taping under the Indian Telegraph Act, 1885, was made possible in large part by the *People's Union for Civil Liberties (PUCL) v. Union of India* case. According to the Supreme Court, tapping violates a person's right to privacy unless it is specifically approved by a legally mandated process. This case influenced subsequent decisions on privacy rights by establishing guidelines for differentiating between arbitrary and legal surveillance[23].

According to the case of, *Union of India v. Navtej Singh Johar,* The Navtej Singh Johar ruling, which invalidated Section 377, which forbade consenting sexual relations between people of the same sex, broadened the definition of the right to privacy, even though it had nothing to do with surveillance. According to the Court, all individuals have the right to preserve all facets of their personal lives free from outside interference, with a particular focus on sexual intimacy. This is known as "the right to be let alone." In other words, sexual autonomy was included in decisional privacy, which gave privacy a far wider definition under the Constitution[24].

In view of the judgements' comprehensive reach, both in terms of the issues they address and the wording of their rights and responsibilities, they will significantly affect privacy and surveillance practices throughout the nation. In addition to guaranteeing a constitutionally protected area for privacy, they have also set the legal foundation for upcoming laws and policies about these matters.

SURVEILLANCE FOR NATIONAL SECURITY SCOPE AND LIMITATIONS

[21] Constitutionality of Aadhaar Act: Judgment Summary, Supreme Court Observer, https://www.scobserver.in/reports/constitutionality-of-aadhaar-justice-k-s-puttaswamy-union-of-india-judgment-in-plain-english/ (last visited Jan 2, 2025).
[22] Supra Note.1.
[23] People's Union for Civil Liberties (PUCL) vs. Union of India AIR 1997 SC 568.
[24] Union of India v. Navtej Singh Johar (2017) 9 SCC 1).

Across the world, including in India, surveillance is essential to national security plans that seek to combat systemic violence and safeguard both state authority and individual liberties. It is crucial to strike a balance between security and data privacy, which calls for a close examination of both legal and illegal uses of surveillance technologies.

Legal Provisions Enabling Surveillance in India

- In order to protect sovereignty, integrity, national security, public order, or to stop crimes that are punishable by law, the government is authorised by Sections 69, 69A, and 69B of the IT Act of 2000 to acquire, track, or decrypt data from any computer resource.
- When it is judged necessary for public order, state security, or good relations with other nations, Section 5(2) of the Indian Telegraph Act, 1885, permits intercepting of messages or the surveillance of individuals. The 2007 amendment greatly and occasionally controversially increased these authorities.
- The Unlawful Activities (Prevention) Act of 1967 gives the government the authority to stop illegal acts that endanger India's integrity, sovereignty, or public order, such as attempts to topple the government by illegal means[25].

INDIVIDUAL PRIVACY RIGHTS VS ENHANCED SURVEILLANCE FOR NATIONAL SECURITY AN BALANCING ACT

The critics caution that in the absence of strong protections, widespread monitoring could be misused for dissent suppression, political repression, and human rights violations. The fundamental goal of monitoring, which is to maintain security, is compromised by this abuse.
By restricting transparency, accountability, and citizen liberties, surveillance that lacks strong legal safeguards undermines democratic ideals.[26] It undercuts the free flow of ideas and discourages dissent and debate, both of which are essential to a healthy democracy.
People who are afraid of being observed may self-censor, abstaining from sharing ideas, taking part in protests, or voicing their thoughts. Such limitation undermines creativity,

[25] The Right to Privacy in the Digital Age: Legal Implications and Challenges, The Amikus Qriae (Jul. 18, 2024), https://theamikusqriae.com/title-the-right-to-privacy-in-the-digital-age-legal-implications-and-challenges/ (last visited Jan 2, 2025).
[26] India: Data Protection Bill Fosters State Surveillance | Human Rights Watch, (Dec. 22, 2022), https://www.hrw.org/news/2022/12/23/india-data-protection-bill-fosters-state-surveillance (last visited Jan 2, 2025).

inventiveness, and social progress in addition to attacking democratic life.[27]

India needs a strong surveillance system to combat terror threats, monitor movements, and destroy networks endangering national security and unity because of its distinct geopolitical environment and history of both internal and international terrorism. Regions such as Jammu and Kashmir are frequently subject to increased scrutiny because of their historical significance and strategic location. Furthermore, as a result of the digital revolution, surveillance has become crucial for identifying and combating dangers like financial theft, impersonation, and hacking, as well as for protecting the economy, digital infrastructure, and citizens.[28] To further maintain territorial integrity and make quick, well-informed judgements to preserve national sovereignty, enhanced surveillance is necessary in the face of external aggression, which includes cyber espionage, satellite photography, and signals intelligence[29].

The challenges do not provide itself to simplistic solutions, nor are there straightforward remedies Instead, striking a balance necessitates our ongoing attention to the interaction of evolving threats, technologies, and their uses—and, above all, the demands of a democratic society based on privacy and a conviction in the liberties that support it. The court has now established some preliminary guidelines to guide the balancing act, starting with *K.S. Puttaswamy v. Union of India*, which established the legislation defining privacy as a basic right with reasonable constraints that the state can impose in the sake of national security.

The argument between India's national security and rights to personal privacy is a component of the global discussion over how to strike a balance in a digital world saturated with data and surveillance technologies. Furthermore, it explains how national security can be maintained without compromising the constitutional liberty and privacy rights that are essential to a free society. The ongoing discussion will continue to shape India's

[27] Gayatri Malhotra, *India's New Data Protection Law: No Transparency, No Privacy | Context*, https://www.context.news/surveillance/opinion/indias-new-data-protection-law-no-transparency-no-privacy (last visited Jan 2, 2025).
[28] Issues of Government Surveillance and Spyware use in India, Tech4Humanity Lab (2023), https://tech4humanitylab.org/blog/2023/11/5/issues-of-government-surveillance-and-spyware-use-in-india (last visited Jan 2, 2025).
[29] Kazim Rizvi, *Personal Data Protection Bill 2019 And Surveillance: Balancing Security And Privacy*, Inc42 Media (Jul. 11, 2020), https://inc42.com/resources/personal-data-protection-bill-2019-and-surveillance-balancing-security-and-privacy/ (last visited Jan 2, 2025).

laws, policies, and values for years to come, if it is carefully watched, disagreements are resolved with strong legal frameworks, and the populace is knowledgeable enough to recognise the cliches[30].

To avoid these negative effects and guarantee that surveillance fulfils its intended function without violating democratic principles or individual liberties, robust legal frameworks and supervision procedures are necessary.

PROSPECTS FOR A BALANCED APPROACH IN INDIA

India's rapid adoption of artificial intelligence (AI) and facial recognition technologies has raised significant privacy concerns. The deployment of state-sponsored AI surveillance through widespread CCTV and facial recognition technology presents both opportunities and challenges. While these innovations can enhance public safety and national security, they also pose substantial risks to individual privacy and freedoms. India's rapid adoption of such technologies, exemplified by cities like Delhi, underscores the urgency of addressing these concerns.[31]

To address these challenges, India enacted the Digital Personal Data Protection Act 2023, a landmark law reshaping the country's data protection landscape. This legislation aims to balance the benefits of AI with the protection of personal data and privacy, ensuring a sustainable and responsible approach to technological advancements.[32]

However, the implementation of facial recognition technology (FRT) without adequate legal safeguards poses serious threats to individual privacy and civil liberties. The widespread use of FRT in India has raised concerns about its impact on privacy and civil liberties. The Information Technology (Amendment) Act 2008 and the Personal Data Protection Bill 2019 are analyzed to understand their adequacy in addressing these concerns. The research emphasizes the need for robust regulatory frameworks to ensure that the deployment of FRT does not infringe on fundamental rights.[33]

---

[30] The Real Struggle for Privacy and National Security in terms of Liberty and Surveillance, The Amikus Qriae (Jun. 30, 2023), https://theamikusqriae.com/the-real-struggle-for-privacy-and-national-security-in-terms-of-liberty-and-surveillance/ (last visited Jan 2, 2025).
[31] Shantanu Sahay, *AI And Facial Recognition In India: Privacy Under Threat?*, (2024), https://www.legaleraonline.com/cybersecurity/ai-and-facial-recognition-in-india-privacy-under-threat-936572 (last visited Jan 2, 2025).
[32] IAPP, https://iapp.org/news/a/operationalizing-india-s-new-data-protection-law-the-challenges-opportunities-ahead (last visited Jan 2, 2025).
[33] Digital Surveillance and the Threat to Civil Liberties in India,

To mitigate these risks, it is essential to strengthen mechanisms for accountability on surveillance powers, whether by means of judicial, legislative, or executive oversight. The Indian government's expansion of surveillance through digitalization and artificial intelligence has increasingly threatened citizens' privacy. Pandemic surveillance also involves social media surveillance, with the government requesting platforms to take down posts critical of its handling of the pandemic.[34] Enhancing global security and privacy regulation can be achieved through taking part in international forums for information sharing, the development of common norms and standards, and the coordination of cross-border data protection and surveillance supervision[35].

RECOMMENDATIONS AND SUGGESTIONS

1. Amend existing legislation like the Indian Telegraph Act and the IT Act to provide clear definitions of acceptable monitoring and ensure judicial oversight to protect individual rights.
2. Implement comprehensive data protection laws, similar to the EU's GDPR, with strict sanctions for violations and controls on both public and private organizations' data usage.
3. Utilize advanced technologies such as end-to-end encryption, data anonymization, and blockchain to enhance security while ensuring privacy protection.
4. Promote public awareness and transparency regarding monitoring practices and individuals' privacy rights, with accessible grievance redressal mechanisms to build trust.
5. Ensure government exemptions under privacy and surveillance laws are strictly necessary, well-defined, and subject to independent oversight to prevent misuse.

CONCLUSION

One of the most important issues in the current digital era is striking a balance between personal privacy and national security. Although surveillance is a vital tool for preventing cybercrimes, fighting terrorism, and preserving sovereignty, it must be used

https://www.giga-hamburg.de/en/publications/giga-focus/digital-surveillance-and-the-threat-to-civil-liberties-in-india (last visited Jan 2, 2025).

[34] India's Advance on AI Regulation, Carnegie Endowment for International Peace, https://carnegieendowment.org/research/2024/11/indias-advance-on-ai-regulation?lang=en (last visited Jan 2, 2025).

[35] Debasish Nandy, *Human Rights in the Era of Surveillance: Balancing Security and Privacy Concerns*, 1 Journal of Current Social and Political Issues 13 (2023).

carefully to prevent violating fundamental rights. Significant changes are needed to India's legal system, notably the Indian Telegraph Act of 1885 and the IT Act of 2000, in order to satisfy contemporary privacy issues and stop power abuse. A significant turning point was reached when the Supreme Court recognised privacy as a basic right in the Puttaswamy ruling, highlighting the necessity, legality, and proportionality of state measures. Risks can be reduced by enacting strong data protection legislation, utilising technology protections, and setting up impartial oversight procedures. In the end, individual liberties and national security must coexist in a democratic system that guarantees openness, responsibility, and public confidence. Finding this balance is essential for maintaining the country's democratic culture as well as for safeguarding its citizens.