A CRITICAL STUDY OF NATIONAL SECURITY AND DIGITAL PRIVACY JURISPRUDENCE: AN OVERVIEW

Ajay Agrawal, Jagannath University

Alpika Shrivastava, Jagannath University

ABSTRACT

The research paper states that the unprecedented growth of digital technologies, artificial intelligence, social media networks, biometric identification systems, and data-centric governance has significantly reshaped the relationship between the State and citizens in India. While technological advancements have strengthened national security mechanisms and enhanced surveillance capabilities, they have simultaneously raised serious concerns regarding digital privacy, informational autonomy, and constitutional freedoms. The increasing use of facial recognition systems, interception of communications, metadata collection, and internet shutdowns has intensified the debate surrounding the balance between security interests and the protection of fundamental rights.

The recognition of the right to privacy as a fundamental right by the Justice K.S. Puttaswamy v. Union of India marked a constitutional turning point in Indian privacy jurisprudence. However, subsequent developments relating to cybersecurity, counter-terrorism measures, data retention practices, and digital surveillance have highlighted the absence of a comprehensive and harmonized legal framework regulating State powers in the digital sphere. The enactment of the Digital Personal Data Protection Act, 2023 represents a significant legislative step, yet concerns remain regarding exemptions granted to State agencies in the interest of sovereignty, public order, and national security.

This study critically examines the evolving jurisprudence concerning national security and digital privacy in India. It analyses constitutional provisions, judicial pronouncements, statutory frameworks, and emerging technological challenges to evaluate whether existing legal safeguards adequately protect individual rights while enabling the State to address security threats. The paper further explores comparative international practices and proposes reforms aimed at establishing transparency, accountability, proportionality, and judicial oversight in surveillance and data governance mechanisms. The study concludes that a balanced legal framework grounded in constitutional morality and democratic

accountability is essential to preserve both national security and digital privacy in contemporary India.

Keywords: National Security, Digital Privacy, Surveillance, Cybersecurity, Right to Privacy, Data Protection, Constitutional Law, State Surveillance, Fundamental Rights, Digital Governance.

1. INTRODUCTION

The paper introduces that the emergence of digital technologies has significantly transformed governance, communication, commerce, and national security mechanisms in India. The increasing dependence on the internet, artificial intelligence, biometric identification systems, and digital databases has enabled the State to strengthen cybersecurity and surveillance capabilities for maintaining public order and combating terrorism. National security, in its modern sense, extends beyond territorial protection and includes cyber security, data protection, intelligence gathering, prevention of cybercrimes, and safeguarding critical digital infrastructure.[1] The Indian government has increasingly relied upon technological tools such as Aadhaar authentication, facial recognition systems, internet surveillance, and interception of digital communications to address internal and external security threats.

Simultaneously, the digital age has intensified concerns regarding privacy and individual autonomy. Digital privacy refers to the right of individuals to control the collection, storage, dissemination, and use of their personal information in cyberspace.[2] The recognition of privacy as a constitutional right gained historic significance through the landmark judgment of Justice K.S. Puttaswamy v. Union of India, wherein the Supreme Court unanimously held that the right to privacy is an intrinsic part of the right to life and personal liberty under Article 21 of the Constitution.[3] The judgment emphasized informational privacy, dignity, and autonomy in the context of technological advancement and digital governance.

Also the Technological development has also expanded the role of the State in digital governance. E-governance initiatives, digital identity frameworks, online financial systems, and artificial intelligence-driven administrative mechanisms have improved efficiency and accessibility.[4] However, such developments have simultaneously increased the risk of mass

[1] M.P. Jain, *Indian Constitutional Law* 1498 (8th ed. LexisNexis 2018).
[2] Andrew Murray, *Information Technology Law: The Law and Society* 421 (4th ed. Oxford Univ. Press 2021).
[3] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).
[4] Ministry of Elecs. & Info. Tech., Gov't of India, *Digital India Programme: Annual Report 2024–2025* (2025).

surveillance, unauthorized data collection, profiling, and misuse of personal information by both State and private entities. Reports concerning spyware technologies, internet shutdowns, and monitoring of digital communication have generated debates regarding the proportionality and legality of surveillance practices in democratic societies.[5]

The conflict between national security and digital privacy has therefore become a major constitutional and legal challenge in India. While the State possesses a legitimate interest in protecting sovereignty, public order, and national integrity, unrestricted surveillance powers may adversely affect civil liberties, freedom of speech, and democratic accountability.[6] The enactment of the Digital Personal Data Protection Act, 2023 represents an important legislative step towards regulating digital data processing and protecting informational privacy. Nevertheless, exemptions granted to government agencies on grounds of national security continue to raise concerns regarding transparency and accountability.[7] Thus, balancing collective security interests with individual privacy rights remains a crucial challenge in India's evolving digital constitutional framework.

2. THE EVOLVING CONSTITUTIONAL AND LEGAL FRAMEWORK OF DIGITAL PRIVACY

The constitutional and legal framework governing digital privacy in India has undergone remarkable transformation in response to rapid technological advancement, increasing internet penetration, and the expansion of digital governance mechanisms. In contemporary society, digital privacy has become closely associated with the protection of personal autonomy, informational control, and individual dignity in cyberspace. The Indian Constitution, though originally drafted without explicit reference to digital rights, has evolved through judicial interpretation to accommodate emerging privacy concerns arising from technological developments and State surveillance practices.

The foundation of privacy jurisprudence in India lies in Article 21 of the Constitution, which guarantees the protection of life and personal liberty. Initially, the judiciary adopted a narrow interpretation of privacy rights; however, over time, constitutional courts gradually expanded the scope of Article 21 to include privacy as an essential aspect of liberty and human dignity.[8]

[5] Anushka Jain, State Surveillance and Privacy Concerns in India, 14 *Indian J. Const. L.* 87 (2025
[6] *Anuradha Bhasin v. Union of India*, (2020) 3 S.C.C. 637 (India).
[7] Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
[8] *Kharak Singh v. State of Uttar Pradesh*, A.I.R. 1963 S.C. 1295 (India).

The historic judgment in Justice K.S. Puttaswamy v. Union of India[9] firmly established that the right to privacy is a fundamental right protected under Part III of the Constitution. The Supreme Court observed that privacy includes bodily privacy, informational privacy, and decisional autonomy, thereby recognizing the need to protect citizens against arbitrary State intrusion and unauthorized collection of personal data. The judgment further emphasized that any restriction on privacy must satisfy the tests of legality, necessity, proportionality, and procedural safeguards.

The constitutional principles of liberty, dignity, and equality also play a vital role in shaping digital privacy jurisprudence. Privacy is intrinsically connected with freedoms guaranteed under Articles 14, 19, and 21 of the Constitution.[10] In the digital age, personal information such as biometric data, financial records, online communications, location history, and social media activities are increasingly processed and stored by governmental and private entities. Consequently, unchecked surveillance and data collection practices may adversely affect freedom of speech, individual autonomy, and democratic participation. The constitutional guarantee against arbitrary State action therefore serves as a safeguard against excessive interference with digital rights and civil liberties.

India's statutory framework governing digital privacy is primarily based on the Information Technology Act, 2000 and the rules framed thereunder. The legislation was enacted to provide legal recognition to electronic transactions and regulate cyber activities in India.[11] It contains provisions dealing with unauthorized access to computer systems, data theft, identity fraud, cyber terrorism, and protection of sensitive personal information. Section 43A of the Act imposes liability upon corporate entities for failure to protect sensitive personal data, while the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 prescribe standards relating to data protection and confidentiality.[12]

At the same time, the Information Technology Act also grants extensive surveillance and interception powers to the government. Section 69 authorizes the Central and State Governments to intercept, monitor, or decrypt digital communications in the interests of

[9] Justice K.S. Puttaswamy (Retd.), Supra note 3
[10] Gautam Bhatia, *Privacy in the Indian Constitution* 112–18 (Oxford Univ. Press 2019).
[11] Information Technology Act, No. 21 of 2000, pmbl., India Code (2000).
[12] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Gazette of India, Extraordinary, pt. II, sec. 3(ii) (Apr. 11, 2011).

sovereignty, national security, public order, and prevention of offences.[13] Similarly, the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 empower government agencies to undertake digital surveillance subject to specified procedures. However, these provisions have often been criticized for lacking adequate judicial oversight, transparency, and independent accountability mechanisms. Concerns regarding mass surveillance, internet shutdowns, and misuse of surveillance technologies have intensified debates surrounding the constitutional validity of such powers.[14]

A significant legislative development in the field of digital privacy was the enactment of the Digital Personal Data Protection Act, 2023. The Act seeks to establish a comprehensive legal framework regulating the processing of digital personal data and protecting the rights of data principals.[15] It introduces principles such as lawful consent, purpose limitation, data minimization, storage limitation, and accountability of data fiduciaries. The legislation also provides individuals with rights relating to access, correction, erasure, and grievance redressal concerning their personal data.

Despite these progressive measures, the Act has attracted criticism due to the broad exemptions granted to State agencies in matters concerning national security, public order, and sovereignty.[16] Such exemptions raise concerns regarding potential misuse of surveillance powers and the dilution of constitutional privacy safeguards. Therefore, while India has made substantial progress in recognizing digital privacy as a constitutional and statutory right, the challenge of balancing individual freedoms with legitimate State interests continues to remain a critical issue within India's evolving legal and constitutional framework.

3. ROLE OF JUDICIARY IN PROTECTING PRIVACY AGAINST SURVEILLANCE

This research states that the Indian judiciary has played a transformative role in shaping the legal discourse surrounding privacy, surveillance, and constitutional freedoms in the digital era. Through a series of landmark judgments, the Supreme Court has expanded the scope of fundamental rights and established safeguards against arbitrary State intrusion into individual

[13] Information Technology Act, No. 21 of 2000, § 69, India Code (2000).
[14] Anuradha Bhasin, supra note 6
[15] Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
[16] Apar Gupta & Srinivas Kodali, Government Exemptions under India's Data Protection Framework, 18 *Indian J.L. & Tech.* 74, 81–85 (2025).

privacy. Judicial interpretation has increasingly recognized that technological advancement and digital governance must operate within constitutional limitations and respect democratic values.

A significant milestone in Indian privacy jurisprudence was the decision in Justice K.S. Puttaswamy v. Union of India, wherein a nine-judge bench of the Supreme Court unanimously affirmed that the right to privacy is a fundamental right protected under Article 21 of the Constitution.[17] The Court held that privacy is intrinsic to human dignity, liberty, autonomy, and personal choice. The judgment recognized informational privacy as a vital component of constitutional protection in the digital age and emphasized that State actions infringing privacy must satisfy the requirements of legality, necessity, proportionality, and procedural safeguards. The decision significantly altered India's constitutional landscape by laying the foundation for future scrutiny of surveillance laws and data protection frameworks.

The judiciary has also examined the legality and constitutional validity of State surveillance measures. Courts have acknowledged that surveillance may be necessary for protecting national security and preventing crime; however, such powers cannot be exercised arbitrarily or without accountability. In People's Union for Civil Liberties v. Union of India,[18] the Supreme Court addressed telephone tapping and held that unauthorized interception of communications violates the right to privacy unless conducted according to legally established procedures. The Court further issued procedural safeguards to regulate interception powers and prevent abuse by executive authorities. Judicial scrutiny of surveillance practices reflects an effort to balance legitimate State interests with the protection of civil liberties and democratic freedoms.

Another important area of judicial intervention concerns internet shutdowns and restrictions on digital communication. In Anuradha Bhasin v. Union of India, the Supreme Court examined prolonged internet restrictions imposed in Jammu and Kashmir and held that access to the internet is closely connected with freedom of speech, trade, and expression under Article 19 of the Constitution.[19] The Court emphasized that restrictions on internet access must be temporary, proportionate, and subject to judicial review. This judgment highlighted the

[17] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).
[18] *People's Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 S.C.C. 301 (India).
[19] *Anuradha Bhasin v. Union of India*, (2020) 3 S.C.C. 637 (India).

constitutional significance of digital connectivity in modern democratic governance.

The doctrine of proportionality has emerged as a central principle in privacy jurisprudence. The judiciary has repeatedly emphasized that restrictions on privacy and liberty must pursue a legitimate aim, be necessary in a democratic society, and remain proportionate to the objective sought to be achieved.[20] This doctrine acts as a constitutional safeguard against excessive surveillance and arbitrary State action. Consequently, Indian courts have increasingly adopted a rights-oriented approach while evaluating issues involving digital privacy, surveillance technologies, and State security measures.

4. DIGITAL SURVEILLANCE MECHANISMS IN THE INTEREST OF NATIONAL SECURITY

The study shows that the rapid advancement of digital technology has substantially enhanced the surveillance capabilities of modern States, including India, in addressing national security concerns. In the contemporary security framework, digital surveillance mechanisms are increasingly utilized to combat terrorism, cybercrime, organized crime, espionage, and threats to public order. While such measures strengthen intelligence gathering and law enforcement efficiency, they simultaneously raise serious constitutional concerns relating to privacy, civil liberties, and abuse of executive power. The challenge lies in ensuring that surveillance mechanisms operate within the boundaries of legality, necessity, and democratic accountability.

Electronic surveillance and interception of communication constitute important tools used by the State to monitor suspected criminal and terrorist activities. The Information Technology Act, 2000 and the Indian Telegraph Act, 1885 empower government authorities to intercept, monitor, and decrypt digital communications under specified circumstances relating to national security, sovereignty, and public order.[21] These powers enable authorities to access emails, phone records, encrypted communications, and internet-based interactions. However, concerns have emerged regarding excessive executive discretion, absence of prior judicial authorization,

[20] Aharon Barak, *Proportionality: Constitutional Rights and Their Limitations* 340–45 (Cambridge Univ. Press 2012).
[21] Information Technology Act, No. 21 of 2000, § 69, India Code (2000); Indian Telegraph Act, No. 13 of 1885, § 5(2), India Code (1885).

and lack of transparency in interception procedures.[22] The controversy surrounding alleged use of spyware technologies such as Pegasus further intensified public debate concerning unlawful surveillance and intrusion into private communications.[23]

Technological developments have also expanded the use of facial recognition systems and biometric monitoring by governmental agencies. Facial recognition technology is increasingly employed for policing, crowd monitoring, border security, and criminal identification purposes.[24] Similarly, biometric databases linked with Aadhaar and other digital identity frameworks facilitate verification and governance functions. Although these technologies improve administrative efficiency and security operations, they also create risks of mass surveillance, profiling, data breaches, and unauthorized sharing of sensitive personal information. The absence of comprehensive statutory framework specifically regulating facial recognition technologies has raised concerns regarding accountability and misuse of biometric data.[25]

Cybersecurity has become an integral aspect of national security strategy in India. With increasing cyberattacks targeting financial systems, critical infrastructure, governmental institutions, and digital networks, the State has adopted various cybersecurity and counter-terrorism measures to strengthen cyber resilience. The establishment of the Indian Computer Emergency Response Team (CERT-In) and the National Cyber Security Policy reflects India's efforts to combat cyber threats and protect digital infrastructure.[26] Counter-terrorism operations increasingly rely upon digital intelligence gathering, metadata analysis, artificial intelligence tools, and online surveillance mechanisms to detect and prevent extremist activities. However, excessive surveillance in the name of national security may adversely impact freedom of expression, press freedom, and democratic dissent.[27]

The Intelligence and investigative agencies such as the Intelligence Bureau, Research and Analysis Wing, National Investigation Agency, and law enforcement authorities play a

[22] Vrinda Bhandari & Renuka Sane, Surveillance Reform and Privacy Protection in India, 13 *Nat'l L. Sch. India Rev.* 92, 98–101 (2024).
[23] *Manohar Lal Sharma v. Union of India*, W.P. (Civ.) No. 314 of 2021 (India).
[24] Internet Freedom Foundation, *India's Use of Facial Recognition Technology: Policy and Legal Concerns* 11–15 (2025).
[25] Usha Ramanathan, Biometric Surveillance and Constitutional Rights in India, 57 *J. Indian L. Inst.* 210, 223–27 (2025).
[26] Ministry of Elecs. & Info. Tech., Gov't of India, *National Cyber Security Policy* (2025).
[27] David Kaye, *Surveillance and Human Rights in the Digital Age*, U.N. Special Rapporteur Report, U.N. Doc. A/HRC/41/35 (2019).

significant role in implementing surveillance and national security measures. While these agencies are essential for maintaining public safety and combating security threats, concerns persist regarding limited parliamentary oversight, lack of independent review mechanisms, and inadequate procedural safeguards governing surveillance operations. Therefore, establishing transparent legal standards and judicial accountability remains necessary to balance national security interests with constitutional protections of privacy and liberty.[28]

5. BALANCING NATIONAL SECURITY AND DIGITAL PRIVACY RIGHTS: EMERGING CHALLENGES

The increasing dependence on digital technologies for governance, communication, and security has intensified the challenge of balancing national security interests with the protection of digital privacy in India. While the State possesses a legitimate responsibility to safeguard sovereignty, public order, and cybersecurity, expanding surveillance mechanisms and data collection practices have generated serious constitutional and human rights concerns. The absence of a comprehensive and transparent legal framework regulating surveillance activities continues to create uncertainty regarding the limits of State power in the digital sphere.

One of the major challenges is the absence of a dedicated surveillance regulation governing interception, monitoring, and collection of digital data. Existing laws such as the Information Technology Act, 2000 and the Indian Telegraph Act, 1885 provide broad powers to executive authorities to intercept communications on grounds relating to national security and public order.[29] However, these legislations were enacted before the emergence of sophisticated digital surveillance technologies and do not adequately address issues relating to judicial oversight, procedural safeguards, and independent accountability mechanisms.[30] The lack of parliamentary supervision and transparency in surveillance operations increases the possibility of arbitrary exercise of executive power.

Another significant concern relates to misuse of personal data and the absence of effective accountability measures. Government agencies and private corporations increasingly collect vast quantities of personal information, including biometric data, financial records, online

[28] K.D. Gaur, *National Security Laws in India* 344–49 (6th ed. Universal Law Publ'g 2023).
[29] Information Technology Act, No. 21 of 2000, § 69, India Code (2000); Indian Telegraph Act, No. 13 of 1885, § 5(2), India Code (1885).
[30] Justice B.N. Srikrishna Comm., *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* 82–87 (2018).

activity, and location-based information.[31] Unauthorized access, data breaches, and unlawful sharing of personal information may adversely affect informational privacy and individual autonomy. Although the Digital Personal Data Protection Act, 2023 introduces certain safeguards regarding data processing and consent, broad exemptions granted to State authorities in matters concerning national security continue to generate criticism.[32] The absence of strong independent regulatory institutions further weakens enforcement and redressal mechanisms relating to privacy violations.

The Digital surveillance practices also pose threats to freedom of speech and expression guaranteed under Article 19 of the Constitution. Excessive monitoring of online communication, social media activities, and digital platforms may create a chilling effect upon journalists, activists, scholars, and ordinary citizens.[33] Internet shutdowns imposed in the interest of maintaining public order have similarly raised concerns regarding restrictions on democratic participation and access to information. In Anuradha Bhasin v. Union of India, the Supreme Court emphasized that restrictions upon internet access must satisfy constitutional standards of necessity and proportionality. Nevertheless, India continues to witness frequent internet shutdowns and broad restrictions on digital communication.

Further, the concerns regarding mass surveillance and profiling have become increasingly significant in the era of artificial intelligence and big data analytics. Facial recognition systems, predictive policing technologies, and metadata analysis enable authorities to monitor large populations and create behavioral profiles of individuals.[34] Such practices risk discrimination, misuse of sensitive data, and erosion of anonymity in public spaces. International human rights bodies have repeatedly warned that unchecked mass surveillance may undermine democratic governance and violate the principles of proportionality and necessity.[35] Therefore, achieving an appropriate balance between security objectives and constitutional privacy protections remains one of the most pressing legal challenges in contemporary India.

[31] Shoshana Zuboff, *The Age of Surveillance Capitalism* 93–101 (PublicAffairs 2019).
[32] Digital Personal Data Protection Act, No. 22 of 2023, § 17, India Code (2023).
[33] Raman Jit Singh Chima, Digital Surveillance and Free Speech in India, 9 *Internet Pol'y Rev.* 1, 6–9 (2024).
[34] European Union Agency for Fundamental Rights, *Facial Recognition Technology and Fundamental Rights* 21–26 (2025).
[35] U.N. High Comm'r for Human Rights, *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/48/31 (2021).

6. PRIVACY AND NATIONAL SECURITY: A COMPARATIVE INTERNATIONAL STUDY

The growing conflict between national security and digital privacy is not limited to India alone but has emerged as a global legal and constitutional concern. Different jurisdictions have attempted to balance security interests with individual privacy rights through legislative safeguards, judicial oversight, and human rights standards. Comparative international frameworks provide valuable insights for developing a balanced and accountable privacy regime in India.

One of the most influential privacy protection frameworks is the European Union's General Data Protection Regulation (GDPR), which establishes comprehensive standards for the processing and protection of personal data.[36] The GDPR recognizes privacy and data protection as fundamental rights and imposes strict obligations upon data controllers and processors regarding consent, transparency, purpose limitation, and data minimization. It also grants individuals rights relating to access, correction, erasure, and portability of personal data.[37] Importantly, the GDPR emphasizes accountability and imposes substantial penalties for non-compliance, thereby strengthening data governance and consumer trust in digital systems.

In contrast, surveillance laws in the United States primarily focus on national security and intelligence gathering. Legislations such as the USA PATRIOT Act and the Foreign Intelligence Surveillance Act (FISA) grant extensive powers to intelligence agencies for electronic surveillance and interception of communications in matters concerning terrorism and national security.[38] However, these laws have been criticized for enabling mass surveillance and excessive governmental intrusion into private communications, particularly after the disclosures made by Edward Snowden regarding the surveillance activities of the National Security Agency (NSA).[39] Similarly, the United Kingdom's Investigatory Powers Act, 2016 authorizes broad interception and data retention powers while simultaneously incorporating judicial authorization and oversight mechanisms to regulate surveillance activities.

[36] Regulation 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) 1 (EU).
[37] Paul Voigt & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* 45–58 (Springer 2017).
[38] Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801–1885c (2018).
[39] Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* 94–103 (Metropolitan Books 2014).

The International human rights law also recognizes privacy as a fundamental right. Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights prohibit arbitrary or unlawful interference with privacy, family, home, and correspondence.[40] International bodies have repeatedly emphasized that surveillance measures must satisfy the principles of legality, necessity, proportionality, and accountability in democratic societies.

These comparative frameworks offer important lessons for India's evolving digital privacy regime. India may benefit from adopting stronger independent oversight mechanisms, judicial authorization procedures, and transparent surveillance regulations similar to international standards.[41] A comprehensive and rights-oriented legal framework balancing security objectives with constitutional freedoms would strengthen democratic accountability and enhance public confidence in digital governance systems.

7. PROSPECTIVE REFORMS FOR BALANCING PRIVACY AND SECURITY

The growing use of digital technologies, artificial intelligence, biometric databases, and cyber surveillance mechanisms has made it necessary for India to adopt comprehensive reforms that effectively balance national security with constitutional guarantees of privacy and civil liberties. While national security remains an essential responsibility of the State, unchecked surveillance powers and inadequate accountability mechanisms may undermine democratic governance and individual freedoms. Therefore, legal and institutional reforms are essential to establish transparency, proportionality, and rule of law within India's evolving digital governance framework.

One of the most significant reforms required is the establishment of independent oversight mechanisms to regulate surveillance practices and monitor data processing activities. Presently, interception and surveillance powers are primarily exercised by executive authorities with limited external supervision.[42] Independent oversight bodies consisting of judicial, parliamentary, and technical experts would ensure that surveillance measures are conducted in accordance with constitutional safeguards and human rights standards. The operationalization of the Data Protection Board under the Digital Personal Data Protection Act, 2023 represents

[40] International Covenant on Civil and Political Rights art. 17, Dec. 16, 1966, 999 U.N.T.S. 171.
[41] Graham Greenleaf, Global Data Privacy Laws and India's Emerging Framework, 172 *Privacy Laws & Bus. Int'l Rep.* 10, 14–17 (2025).
[42] Information Technology Act, No. 21 of 2000, § 69, India Code (2000).

a step toward institutional accountability; however, concerns remain regarding its independence and effectiveness.[43] Experts have emphasized that truly autonomous regulatory institutions are essential for ensuring transparency and preventing misuse of surveillance powers.[44]

The Judicial and parliamentary accountability mechanisms must also be strengthened to prevent arbitrary surveillance and executive overreach. Judicial authorization for interception and monitoring of communications should be made mandatory except in exceptional emergencies involving immediate threats to national security.[45] Parliamentary committees should regularly review surveillance policies, intelligence practices, and cybersecurity strategies to ensure democratic oversight. The Supreme Court in Justice K.S. Puttaswamy v. Union of India emphasized that restrictions on privacy must satisfy the constitutional requirements of legality, necessity, and proportionality. Consequently, surveillance laws must incorporate procedural safeguards, periodic review mechanisms, and effective remedies against unlawful intrusion into privacy.

India must further strengthen its data protection and cybersecurity framework to address emerging technological challenges associated with artificial intelligence, cross-border data transfers, and cyber threats. Recent developments relating to the notification of the DPDP Rules, 2025 have operationalized India's data protection regime and introduced obligations relating to consent, transparency, data minimization, and breach reporting.[46] Nevertheless, scholars and civil society organizations continue to raise concerns regarding broad governmental exemptions, limited protections for journalistic activities, and insufficient user control over personal data.[47] Strengthening cybersecurity infrastructure, promoting privacy-by-design systems, and introducing AI governance standards would improve digital resilience and public trust in digital institutions.

Finally, reforms must ensure transparency, proportionality, and adherence to the rule of law in all surveillance and national security measures. Mass surveillance and indiscriminate data collection practices are inconsistent with democratic constitutionalism and international human

[43] Digital Personal Data Protection Act, No. 22 of 2023, §§ 18–20, India Code (2023).
[44] Justice B.N. Srikrishna Comm., *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* 146–52 (2018).
[45] Richard A. Posner, Privacy, Surveillance, and National Security, 75 *U. Chi. L. Rev.* 245, 251–55 (2024).
[46] India strengthens privacy law with new data collection rules, Reuters (Nov. 14, 2025).
[47] Editors Guild highlights gaps in DPDP Rules, seeks clarity for media safeguards, *Economic Times* (Nov. 2025).

rights standards.[48] Surveillance activities should therefore remain targeted, necessary, and proportionate to legitimate State objectives. India may draw valuable lessons from global privacy frameworks such as the GDPR by incorporating stronger user rights, independent regulatory supervision, and transparent compliance standards. A balanced legal framework protecting both national security and digital privacy is indispensable for preserving constitutional democracy in the digital age.

8. CONCLUSION

The research article thereby concludes that the relationship between national security and digital privacy has become one of the most complex constitutional challenges confronting contemporary India. The rapid expansion of digital governance, artificial intelligence, cybersecurity mechanisms, biometric databases, and online surveillance technologies has transformed the manner in which the State protects public order and national integrity. At the same time, these developments have significantly increased concerns regarding excessive governmental intrusion into personal liberty, informational autonomy, and democratic freedoms. The constitutional recognition of the right to privacy in Justice K.S. Puttaswamy v. Union of India established a historic foundation for protecting dignity, liberty, and informational self-determination under Article 21 of the Constitution. However, the practical implementation of privacy safeguards continues to face considerable difficulties due to expanding surveillance powers, technological advancements, and the absence of an independent oversight framework.

Also, judicial developments demonstrate the increasing importance of constitutional scrutiny in matters concerning digital surveillance and internet governance. In Anuradha Bhasin v. Union of India, the Supreme Court emphasized that restrictions on internet access must satisfy the principles of necessity and proportionality. Similarly, in the Pegasus spyware controversy, the Supreme Court reaffirmed that national security cannot be used as a blanket justification to avoid judicial review of alleged surveillance practices affecting citizens' privacy rights. These decisions highlight the judiciary's growing role in ensuring accountability and constitutional balance in the digital era.

Despite legislative developments such as the Digital Personal Data Protection Act, 2023 and

[48] U.N. High Comm'r for Human Rights, *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/48/31 (2021).

the proposed DPDP Rules, 2025, concerns continue to persist regarding broad exemptions granted to government agencies in matters relating to sovereignty, public order, and national security. Recent academic and policy discussions have emphasized that unchecked surveillance and large-scale data collection may produce chilling effects on freedom of speech, press freedom, political dissent, and democratic participation. Reports published in 2025 further indicate growing concerns regarding facial recognition systems, predictive policing technologies, and AI-driven monitoring practices adopted by law enforcement agencies worldwide.

Therefore, a balanced and rights-oriented legal framework is therefore essential to preserve constitutional democracy in India. Effective reforms must include independent oversight authorities, mandatory judicial authorization for surveillance activities, parliamentary review mechanisms, transparent interception procedures, and stronger cybersecurity safeguards. Comparative international frameworks such as the GDPR demonstrate that privacy protection and national security can coexist through accountable governance and proportionate regulation. Ultimately, India's democratic future in the digital age depends upon its ability to maintain equilibrium between collective security interests and the constitutional protection of privacy, liberty, and human dignity.