Journal of Contemporary Politics

ORIGINAL ARTICLE

Securing Borders, Enabling Progress - Leveraging Technology for India's Border Surveillance and Developmental Vision 2047

Rahul G Gangaraj[1], Malka Biddappa[2,*]

[1] *III Year, School of Law, M. S. Ramaiah University of Applied Sciences, Bengaluru, Karnataka, India*
[2] *I Year, School of Law, M. S. Ramaiah University of Applied Sciences, Bengaluru, Karnataka, India*

ARTICLE INFO

Article history:
Received 31-03-2025
Accepted 21-05-2025
Published 24-07-2025

* *Corresponding author.*
Malka Biddappa
24slll418024@msruas.ac.in

https://doi.org/10.53989/jcp.v4i2.25.29

ABSTRACT

India is bordered by 15,106 kilometres of land which runs through different kinds of terrain, including mountains, hills, plains, valleys, forest, desert and swamp, and is sometimes difficult to monitor, especially at a time when territorial disputes and security troubles still plague parts of the Indian borderline.[1] India's pursuit of a developed nation by 2047 (Viksit Bharat) necessitates robust border security, a critical pillar for national sovereignty and economic advancement. This paper analyses India's strategic use of technology to bolster border surveillance. This study adopts a qualitative and doctrinal approach to examine the deployment of surveillance technologies along India's land borders. It analyses government reports, policy documents, and legal provisions, including Articles 19 and 21 of the Indian Constitution. The paper also incorporates secondary data from think tank publications, parliamentary debates, and media sources to assess the socio-legal and economic impact on border communities. A socio-legal analytical framework is used to evaluate the alignment of security measures with constitutional protections and national development goals. The paper examines the real-world impact of technological border security advancements on border communities. It assesses how improved security fosters a safer environment, boosting well-being and potentially increasing economic activity like trade, agriculture, and tourism, often hindered by cross-border threats. The study also explores how better border security improves access to essential services such as education, healthcare, and infrastructure in vulnerable regions. It also addresses challenges like funding, data privacy, cybersecurity, and the need for skilled personnel. By evaluating the effectiveness, societal impact, and legal considerations, this paper aims to provide a nuanced understanding of India's border security strategy and its contribution to the 2047 vision.

Keywords: Border Security; Border Surveillance; Data Privacy; Cybersecurity; Right to Privacy

INTRODUCTION

National security and border surveillance have always been paramount for India, a country with a vast and diverse terrain covering over 15,106 km of land borders shared with seven neighbouring nations. Given the persistent challenges of cross-border terrorism, illegal migration, and smuggling, ensuring robust and technologically advanced border security mechanisms is imperative. Traditional surveillance methods, such as physical patrolling and static fencing, have often proven inadequate in addressing these evolving threats. In response, India has begun integrating cutting-edge surveillance technologies, including radar systems, drones, and satellite-based monitoring, to enhance its border security framework.

One of the key innovations in India's border surveillance infrastructure is the Border Surveillance System (BOSS) developed by Bharat Electronics Limited (BEL). This system integrates radar and electro-optic sensors to provide real-time monitoring and early warning capabilities along sensitive border areas. By utilizing advanced imaging and motion detection technologies, BOSS significantly reduces human dependency while improving efficiency in threat detection and response. The deployment of such systems is particularly crucial in remote and high-altitude border regions where manual patrolling is challenging.[2]

Furthermore, India has increasingly adopted Unmanned Aerial Vehicles (UAVs) and drones to complement ground-based surveillance.[3] According to studies on technological innovations in border security, the Indian Armed Forces and

paramilitary units have deployed UAVs such as the Heron, Searcher Mk II, and DRDO's Netra for aerial reconnaissance, intelligence gathering, and real-time threat assessment. These drones provide high-resolution imaging and thermal detection, enabling security personnel to monitor large and inaccessible areas efficiently. Additionally, integrating satellite imagery from India's RISAT and Cartosat programs further enhances situational awareness by offering geospatial intelligence in border zones.[4]

India has also implemented laser fencing, floodlighting, and automated surveillance towers to fortify its border security, particularly along high-risk areas such as the Indo-Pak and Indo-Bangladesh borders. As outlined in a report by SPS Land Forces, laser fencing technologies have been deployed in sensitive regions to detect and prevent unauthorized crossings, while floodlighting along the western borders has improved night-time monitoring.[5] These technological interventions, coupled with an Integrated Border Management System (IBMS), reflect India's strategic shift towards smart border security solutions.

As India moves towards its Vision 2047, a long-term strategic roadmap for national development, leveraging advanced surveillance technologies will be a key pillar of its border security framework. By integrating AI-driven threat detection, automated sensor networks, and geospatial intelligence, India aims to build a more resilient and technologically empowered security apparatus. This research paper explores the role of technology in transforming India's border surveillance mechanisms and examines how these advancements align with the nation's broader developmental and security objectives.

EXISTING BORDER SECURITY INFRASTRUCTURE IN INDIA

India has significantly modernized its border security infrastructure by integrating advanced technologies to monitor and secure its extensive and varied frontiers. The Comprehensive Integrated Border Management System (CIBMS) is central to this modernization, incorporating a suite of surveillance tools and systems to enhance real-time threat detection and response.

The CIBMS employs a multi-layered security grid that includes motion sensors, laser barriers, and intrusion detection systems. These are integrated into centralized control centres, enabling real-time monitoring and swift responses to breaches. For instance, in Assam's Dhubri district, where the Brahmaputra River creates challenging terrain, the BOLD-QIT (Border Electronically Dominated QRT Interception Technique) project has been implemented. This project utilizes microwave communication, optical fiber cables, digital mobile radio communication, day and night surveillance cameras, and intrusion detection systems to monitor the border effectively.[6]

AI algorithms analyse data from various surveillance devices, filtering out false positives and highlighting genuine threats. This capability allows for predictive analysis of infiltration patterns, aiding in strategic deployment of security forces.

Traditional Surveillance Mechanisms

India's border security relies on multiple conventional methods such as border fencing, floodlighting, ground patrols, check posts, and human intelligence networks. The Border Security Force (BSF), Indo-Tibetan Border Police (ITBP), Assam Rifles, and Sashastra Seema Bal (SSB) play a critical role in patrolling the nation's international borders. These methods serve as primary deterrents against unauthorized crossings and illegal activities. However, they have inherent limitations, particularly in rugged terrains and densely forested regions.

The deployment of physical barriers like fencing and floodlighting has been instrumental in restricting unauthorized movement. According to Boukhalfa et al., security along international borders requires 24/7 monitoring to ensure effectiveness.[7] Despite these efforts, gaps remain, leaving the borders vulnerable to infiltration and smuggling activities.

Limitations of Conventional Methods

Borders often pass through mountainous and forested regions, making constant surveillance challenging. The difficult terrain limits visibility and accessibility, increasing the risk to security personnel while also reducing coverage. Traditional border security measures, such as manual patrolling, observation towers, security posts, and organized patrols, have long been used to monitor these areas. However, these static and manpower-intensive methods fail to provide seamless surveillance, particularly in regions with extreme climatic conditions.[7] The reliance on physical presence alone creates vulnerabilities, as harsh weather and rugged landscapes often impede effective monitoring and response.

Another significant challenge in border security is the heavy dependence on manpower, which proves to be both costly and inefficient. With evolving security threats, such as cross-border terrorism, smuggling, and illegal migration, a shift toward technology-driven solutions has become increasingly necessary. The International Journal of Information Retrieval Research highlights that manual monitoring of extensive and harsh terrains not only places an excessive burden on personnel but also slows down response times in critical situations.[7] Over-reliance on human surveillance reduces efficiency, particularly when faced with fast-moving threats that require real-time intelligence and swift action. This underscores the need for automated and AI-driven surveillance mechanisms to enhance border

security operations.

In addition to the challenges posed by terrain and manpower dependency, border fencing alone is not a fool-proof security measure. Unauthorized breaches are common, as fencing can be cut, climbed, or circumvented, making it an insufficient standalone defence. Moreover, certain border regions remain unfenced due to environmental constraints, difficult landscapes, or diplomatic sensitivities. While border fencing plays a crucial role in preventing unauthorized crossings and smuggling activities, it remains susceptible to breaches unless reinforced with advanced technological solutions. To address these gaps, integrating smart fencing, real-time surveillance, and AI-powered monitoring is essential for strengthening border security and ensuring a more effective and proactive defence mechanism.

Integration of Advanced Technologies

The deployment of biometric technologies at border crossings has been a significant step toward strengthening border security. Modern biometric methods include facial recognition, fingerprint identification, and iris scanning. However, biometric technologies pose challenges related to privacy, accuracy, and potential bias. According to the recommendations of ARTICLE 19, the implementation of biometric surveillance must balance security needs with human rights protection.[8]

One key issue is the reliability of biometric data. Studies warn that facial expressions and external behaviours are not always reliable indicators of identity or intent.[8] The concerns surrounding biometric mass surveillance highlight the need for a robust legislative framework to govern its use.[9] These challenges highlight the necessity of integrating complementary technologies, such as IoT-based surveillance, to enhance border security while mitigating the limitations associated with biometric systems.

The Internet of Things (IoT) has enabled border security forces to integrate smart sensors, drones, and automated surveillance systems. Drones equipped with cameras and motion sensors have been instrumental in enhancing border security. Studies state that their proposed system classifies human gestures from drone video footage in real time.[7] This approach enables round-the-clock surveillance without the need for constant human intervention. Building on these advancements, the integration of artificial intelligence and machine learning further enhances border security by enabling predictive threat detection and automated decision-making.

AI-driven border security solutions leverage machine learning algorithms to detect anomalies and predict threats. One such system employs the Grouping Cockroaches Classifier (GCC), which uses bio-inspired techniques to detect unwanted individuals based on gestures rather than facial recognition.[7] The AI-driven classification method enhances accuracy while mitigating concerns about privacy and racial bias.

AI-powered surveillance systems can also automate decision-making, allowing border security forces to respond swiftly to potential threats. Research on AI-based video surveillance suggests that a threat level classifier and alert warning system categorize threats in real-time, ranking them from safe to high-danger levels. These advancements significantly improve border security without increasing manpower requirements.

Ethical and Legal Considerations

While advanced surveillance methods enhance security, they raise ethical concerns related to privacy and data protection. Biometric databases, if not properly managed, can lead to "mission creep," where data collected for security purposes is repurposed for unrelated activities.[8] The absence of a clear legislative framework governing biometric surveillance could result in human rights violations.

Additionally, AI-driven surveillance systems must be transparent and accountable. Research on automated decision-making highlights the "black box" problem, where machine learning algorithms make decisions without clear explanations.[8] Ensuring accountability in AI-based surveillance systems is crucial for maintaining public trust and preventing misuse.

Though extensive, India's border security infrastructure faces significant challenges in terms of terrain adaptability, manpower efficiency, and evolving threats. While conventional methods provide a foundational layer of security, integrating technology-driven solutions such as biometrics, IoT, and AI can enhance efficiency and response capabilities. However, the implementation of these technologies must be accompanied by stringent regulatory frameworks to ensure ethical use and compliance with human rights principles. The future of border security lies in balancing technological advancements with accountability and privacy protection.

LEGAL FRAMEWORKS GOVERNING BORDER SURVEILLANCE AND SECURITY

India's border security is governed by a range of laws and policies aimed at protecting its territorial integrity while addressing modern security challenges. With evolving threats such as illegal migration, smuggling, and cross-border terrorism, the country has increasingly turned to technology-driven surveillance to enhance its border management. The legal framework for border security is primarily shaped by constitutional provisions, parliamentary laws, and policy guidelines, which grant the central government the authority to deploy advanced monitoring systems, including drones, biometric identification, and artificial intelligence-based surveillance.

However, the growing use of digital technologies in border security also raises concerns about privacy, data protection, and individual rights. Courts have emphasized the need to balance national security with fundamental freedoms, particularly in light of India's commitment to constitutional principles such as the right to privacy. As technology continues to shape border surveillance, India's legal framework must adapt to ensure effective governance, accountability, and ethical use of digital tools in securing its frontiers.

Legislative Competence and Union's Authority

The Indian Constitution provides the Union Government with extensive legislative and administrative authority over border security through Article 245 and Article 246, read with Schedule VII, List I. These provisions empower Parliament to legislate on matters related to "defense," "foreign affairs," and "border security."[10] This exclusive jurisdiction enables the central government to frame laws and deploy technological measures to ensure robust border surveillance.

Additionally, Article 355 places a duty on the Union to protect states from external aggression and internal disturbances, reinforcing the need for centralized border security management. The expansion of Border Security Force (BSF) jurisdiction into states like Punjab and Assam has sparked debates regarding federalism. While some state governments argue that such extensions infringe upon List II (State List) powers, the Supreme Court in Naga People's Movement of Human Rights v. Union of India (1998) has affirmed the necessity of central intervention in security matters.[11] The judiciary has also established the principle that national security considerations may necessitate temporary shifts in jurisdiction, as evidenced in S.R. Bommai v. Union of India (1994).[12]

Understanding Evolution of Surveillance Laws through Juridical Analysis

The nascent stages of surveillance law in India can be traced to cases like M.P. Sharma v. Satish Chandra (1954) and Kharak Singh v. State of U.P. (1962).[13,14] While M.P. Sharma declined to recognize a constitutional right to privacy akin to the American Fourth Amendment, Kharak Singh signalled a crucial shift, laying the groundwork for the eventual recognition of privacy as an integral facet of personal liberty under Article 21 of the Indian Constitution.

A watershed moment arrived in 1975 with Gobind v. State of M.P. (1975).[15] This landmark ruling explicitly recognized the right to privacy as an essential component of personal liberty under Article 21. Crucially, the judgment introduced the "compelling state interest" test, mandating that any infringement on privacy must be justified by a substantial and pressing government interest. This standard became a cornerstone of subsequent legal discourse on privacy and surveillance.

The principles established in Gobind v. State of M.P. (1975) were further refined in subsequent cases.[15] Malak Singh v. State of Punjab & Haryana (1980) emphasized the necessity of targeted surveillance, grounded in reasonable grounds and proportionate to the objective pursued.[16] This ruling underscored the importance of narrowly tailored surveillance measures to minimize intrusions on individual rights, particularly privacy and dignity.

The contentious issue of telephone tapping came under judicial scrutiny in People's Union for Civil Liberties (PUCL) v. Union of India (1997).[17] This pivotal case established strict procedural safeguards for such surveillance activities, reflecting the court's concern about the potential for abuse of state power. While acknowledging national security as a legitimate concern, the judgment stressed the critical need for oversight and transparency in surveillance measures, especially those involving intrusive techniques like phone tapping.

More recent cases, such as Distt. Registrar & Collector v. Canara Bank (2004) and Selvi v. State of Karnataka (2010), have continued to shape the discourse on surveillance and privacy.[18,19] These rulings have reinforced the principles of privacy and individual dignity in the face of evolving surveillance technologies, demonstrating the judiciary's ongoing commitment to balancing national security needs with individual rights.

While the provided precedents do not explicitly address border security, the principles of privacy and proportionality articulated in these cases are clearly applicable to all forms of state surveillance, including those related to border control and national security. The courts have consistently maintained that any infringement on privacy must be justified by a compelling state interest and must be narrowly tailored to achieve specific security objectives.

Although the state's need to safeguard national security is undeniable, the courts have consistently emphasized that this cannot serve as a blanket justification for unregulated or excessive surveillance. The PUCL case, for instance, demonstrates the court's insistence on robust procedural safeguards and judicial oversight even in matters of national security, particularly before intrusive measures like telephone tapping are authorized.[17]

The Border Security Force Act, 1968 and Its Implications

The Border Security Force Act, 1968 serves as the cornerstone of India's border security framework. It establishes the BSF and empowers it to combat illegal immigration, cross-border crimes, and infiltration. Section 139(1)(i) grants the Central Government discretionary powers to expand BSF's jurisdiction, reinforcing cooperation with state police to enhance trans-border crime prevention.

Critics argue that the extension of BSF's operational jurisdiction into states with volatile border regions may infringe upon state autonomy. However, jurisprudence such as in re: The Berubari Union & Exchange of Enclaves (1960) supports the argument that national security concerns trump state authority when territorial sovereignty is at stake.[20]

Moreover, in light of increasing cross-border infiltration and arms smuggling, legal scholars argue that enhanced BSF jurisdiction must be balanced with civil liberties to prevent undue state overreach. The courts have emphasized that policing powers must align with constitutional safeguards under Articles 19 and 21, ensuring proportionality and necessity in border security interventions.

Legal Framework for Technology-Driven Border Surveillance

The Information Technology (IT) Act, 2000, alongside recent cybersecurity policies, provides a statutory basis for digital surveillance and cybersecurity enforcement. The Act outlines key provisions that allow for state intervention in cyber espionage, digital forensics, and cross-border intelligence sharing. Section 68 grants the power to issue directions for interception, monitoring, or decryption of any information through any computer resource, facilitating border intelligence gathering. Section 69A empowers the government to block public access to online content deemed a threat to national security, while Section 69B authorizes government agencies to monitor and collect traffic data from digital networks to enhance cybersecurity in border regions. Although these provisions establish a legal basis for AI-powered surveillance, UAV reconnaissance, and biometric border controls, concerns persist regarding accountability and potential misuse. Given the global backlash against mass surveillance programs, India must incorporate judicial oversight mechanisms to ensure compliance with constitutional protections of privacy and free movement.

Digital Personal Data Protection (DPDP) Act, 2023 and the Right to Privacy

The enactment of the Digital Personal Data Protection (DPDP) Act, 2023, represents a significant step towards safeguarding digital privacy in India. However, its provisions also carry substantial implications for border security and state surveillance. Notably, section 17 of the Act grants the government the authority to exempt itself from certain provisions in the interest of national security. This exemption enables the collection, processing, and retention of biometric and personal data, particularly in sensitive border regions, where security concerns are paramount.

While such measures may be justified on the grounds of national security and counterterrorism efforts, they also raise critical questions regarding the potential for excessive state surveillance and the absence of robust legislative and judicial oversight. The constitutional framework governing privacy, as established in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), underscores that any data collection practice must adhere to the principles of legality, necessity, and proportionality.[21] The Supreme Court, in this landmark ruling, recognized the Right to Privacy as an intrinsic aspect of Article 21 of the Indian Constitution and emphasized that state surveillance must be subject to legal safeguards to prevent arbitrary intrusions. Given this legal precedent, any exemption granted under the DPDP Act must be scrutinized to ensure it meets constitutional thresholds of reasonableness and proportionality.

Without adequate oversight mechanisms, the broad powers conferred by Section 17 could lead to disproportionate surveillance in border regions, affecting not only security concerns but also fundamental rights. Therefore, India's data protection framework must evolve to strike a careful balance between national security imperatives and the protection of individual privacy rights, particularly in areas where security-related surveillance is intensified.

ARTIFICIAL INTELLIGENCE (AI) AND BORDER SECURITY: ETHICAL AND LEGAL CHALLENGES

The deployment of AI-powered surveillance in border security, while enhancing monitoring capabilities, raises significant concerns regarding algorithmic bias, false positives, and the potential for racial profiling. Empirical studies have demonstrated that AI-driven facial recognition technologies disproportionately misidentify ethnic minorities, increasing the likelihood of wrongful detentions and undue hardships for vulnerable populations at border checkpoints. Such issues bring into question the constitutional validity of automated surveillance mechanisms that operate without adequate human oversight.[22]

The Supreme Court, in Maneka Gandhi v. Union of India (1978), established that any restriction on fundamental rights must be just, fair, and reasonable, reinforcing the principle that state actions impacting individual liberties must adhere to due process.[23] Furthermore, automated decision-making in border security, when conducted without human intervention, may violate Article 14 and Article 21 of the Indian Constitution, as it deprives individuals of the right to contest or challenge erroneous AI-generated outcomes. Given these constitutional and ethical concerns, it is imperative that AI-driven surveillance technologies incorporate robust oversight mechanisms, transparency in algorithmic decision-making, and safeguards against discriminatory outcomes to ensure compliance with fundamental rights.

India's legal approach must balance security concerns with constitutional liberties, ensuring border surveillance does not encroach upon civil rights. Given the complexities and ethical concerns surrounding AI-driven surveillance in border security, India must establish a comprehensive legal

framework to regulate its deployment effectively. Such a framework should prioritize transparency in AI decision-making processes, ensuring the rationale behind AI-generated surveillance outcomes is accessible and accountable.

Additionally, there must be legislative clarity on liability for wrongful identification, addressing potential legal ramifications for misidentifications that may lead to undue detentions or violations of individual rights. Furthermore, implementing strict guidelines for AI-based threat classification is essential to prevent arbitrary or discriminatory targeting, ensuring that AI systems operate within clearly defined legal and ethical boundaries. Lastly, India's regulatory approach must align with United Nations principles on the ethical use of AI in law enforcement, incorporating global best practices to safeguard fundamental rights while maintaining national security imperatives.

NAVIGATING THE COMPLEX CHALLENGES OF INDIA'S BORDER SECURITY

As India seeks to enhance its border security through advanced technologies such as AI-driven surveillance, biometric identification, satellite monitoring, and automated response systems, it faces numerous challenges. These challenges can be broadly classified into internal (policy, legal, infrastructural, and operational issues) and external (geopolitical, cybersecurity, and cross-border threats). While technology offers enhanced security and efficiency, its integration must be carefully managed to avoid legal overreach, surveillance concerns, and national security vulnerabilities.

By analysing India's constitutional stance on surveillance and privacy, as discussed in the document, we can draw parallels to border security measures and the possible implications of an over-reliance on technology without adequate safeguards.

One of the primary internal challenges India faces in integrating technology into border security is the legal and constitutional restrictions on mass surveillance and privacy. Various Supreme Court judgments highlight the need for stringent safeguards when implementing surveillance mechanisms. For instance, the PUCL v. Union of India (1997) ruling emphasized that mass surveillance must be subject to legal oversight and due process.[17] Similarly, large-scale data collection at border checkpoints—through biometric scanners, facial recognition cameras, and AI-based movement tracking systems—could lead to potential violations of Article 21 (Right to Life and Personal Liberty), as interpreted by the Supreme Court in Justice K.S. Puttaswamy v. Union of India (2017), which recognized the Right to Privacy as a fundamental right.[21] To address this, India must introduce specific legislation that regulates surveillance at borders, ensuring that any data collected is stored securely, used proportionally, and deleted after a specified period. Establishing a Border Security Technology Oversight Authority could help review and audit surveillance operations, ensuring compliance with legal frameworks and preventing misuse.

India's border regions—particularly along the Line of Actual Control (LAC) with China, Line of Control (LoC) with Pakistan, and the India-Myanmar border—often suffer from poor digital infrastructure, making it difficult to deploy and maintain advanced surveillance systems. Remote border areas lack a stable power supply, high-speed internet, and reliable sensor networks, affecting the efficiency of AI-based monitoring and satellite tracking. The government has made significant investments in the Comprehensive Integrated Border Management System (CIBMS) and Smart Fencing along the Indo-Pakistan and Indo-Bangladesh borders. However, technical failures, a shortage of skilled personnel, and outdated infrastructure remain major obstacles. A phased approach to technology integration is necessary, starting with high-risk zones where infiltration risks are greatest. Investments in solar-powered surveillance towers, satellite-based communication, and automated drone monitoring can help overcome infrastructure deficits.

Technological integration in border security is also hampered by inter-agency coordination issues. Multiple agencies, including the Border Security Force (BSF), Indo-Tibetan Border Police (ITBP), Assam Rifles, and local law enforcement, operate under different mandates, which results in a lack of unified command and data-sharing protocols.[24] This fragmentation leads to inefficiencies in intelligence gathering and response mechanisms. Moreover, manual intervention in automated surveillance systems often results in delays, misinterpretation of data, and bureaucratic bottlenecks. Border personnel may also lack the technical skills required to operate and maintain AI-driven security infrastructure effectively. To address these challenges, a unified digital command and control system should be implemented, integrating all border security agencies into a centralized AI-driven intelligence network. This system should use machine learning algorithms to process real-time data and automatically alert security forces to potential threats. Additionally, regular training programs must be conducted for border personnel to familiarize them with AI-based decision-making tools and cybersecurity protocols, ensuring efficient and coordinated responses to emerging security threats.

The risk of government overreach and mass surveillance also remains a critical concern. The Central Monitoring System (CMS) and National Intelligence Grid (NATGRID), designed for national security, have already raised concerns about excessive surveillance. If border security technologies such as biometric tracking, AI-powered movement analysis, and automated drone surveillance are implemented without proper oversight, they could lead to widespread privacy violations. Supreme Court rulings in cases such as Kharak

Singh v. State of Uttar Pradesh (1963) and Gobind v. State of Madhya Pradesh (1975) have set legal precedents for privacy protections, warning against unchecked surveillance. These concerns become even more significant when border security measures extend to monitoring civilians in border regions, potentially criminalizing innocent movement and activity.[14,15] To prevent such overreach, a Privacy and Surveillance Regulatory Framework must be introduced to establish clear guidelines on data collection, storage, and access permissions. Judicial oversight should be mandated for any prolonged surveillance or use of intrusive biometric identification measures in border areas to maintain transparency and accountability.

Beyond domestic challenges, India faces external threats that complicate its efforts to enhance technological border security. As AI-based surveillance, drone patrolling, and satellite communication become integral to border security, India becomes increasingly vulnerable to cyberattacks from hostile nations and non-state actors. GPS spoofing, signal jamming, and AI-based disinformation campaigns can be used to manipulate border intelligence, mislead security forces, and create operational confusion. To counter such cyber threats, end-to-end encryption protocols, AI-driven anomaly detection systems, and blockchain-based data verification mechanisms must be integrated into India's border security infrastructure. Establishing a Cybersecurity Task Force for Border Protection, in collaboration with the Indian Computer Emergency Response Team (CERT-In) and the Defence Cyber Agency (DCA), will help mitigate risks and safeguard critical infrastructure.

The deployment of AI-driven surveillance, drone monitoring, and automated security systems at India's borders could also lead to diplomatic tensions with neighbouring countries. China, Pakistan, Nepal, and Bangladesh may perceive India's increased use of high-tech border security measures as a provocative military build-up, potentially leading to escalations in border disputes. The Indo-China border dispute in Ladakh has already seen increased technological deployments, with both sides relying on satellite imaging, AI-driven military surveillance, and cyber-warfare tactics.[25] Similarly, deploying automated surveillance drones along the Indo-Pakistan border might be seen as aggressive military posturing, affecting diplomatic negotiations. To prevent such conflicts, India must engage in strategic diplomacy and confidence-building measures, including establishing bilateral agreements on technological deployments at sensitive borders. Regular military and intelligence exchanges with neighbouring countries can help de-escalate tensions and promote mutual surveillance transparency protocols, ensuring that border security technologies are used for defensive rather than offensive purposes.

Furthermore, India must anticipate the adaptive strategies of non-state actors, such as smugglers and terrorist groups, who will seek to bypass AI-driven security measures. While automated border surveillance is highly effective against traditional infiltration tactics, adversaries may exploit AI-generated deepfake identities to fool biometric scanners, employ cyber tools to disable smart fences, or construct underground tunnels to evade electronic detection. To combat these evolving threats, India must adopt a multi-layered security approach that combines technology with human intelligence. Deploying counter-AI measures, such as deep fake detection algorithms and predictive analytics, can help security forces anticipate and neutralize sophisticated infiltration tactics. Additionally, a border intelligence network, integrating local informants and AI-driven risk analysis models, will be essential in providing real-time updates on emerging threats and ensuring swift countermeasures.

In conclusion, while the integration of AI, biometrics, and automated surveillance into India's border security offers immense potential, it also presents significant legal, infrastructural, cybersecurity, and geopolitical challenges. Balancing security imperatives with constitutional protections, investing in cyber resilience, strengthening inter-agency coordination, and engaging in diplomatic negotiations will be key to ensuring that technological advancements in border security are both effective and ethically sound. By addressing these challenges through a holistic and adaptive approach, India can successfully leverage modern surveillance technologies to enhance national security while upholding democratic values and human rights.

CONCLUSION

The evolution of surveillance law in India reveals a gradual but consistent recognition of privacy as a fundamental right. The courts have diligently sought to balance legitimate state interests with individual rights, particularly in the context of surveillance. While national security concerns are accorded due weight in legal deliberations, they cannot entirely eclipse the fundamental right to privacy.

However, recent judicial pronouncements have, at times, appeared inconsistent in upholding these established principles. As surveillance technologies advance and the state's capacity for surveillance expands, there is a risk that national security concerns may be invoked to justify unchecked surveillance practices. This underscores the crucial importance of vigilant judicial oversight to ensure that all surveillance measures, particularly those related to border security, adhere to the principles of proportionality, necessity, and respect for individual dignity.

The rapid pace of technological development and the expanding scope of surveillance systems necessitate continued and robust deliberation on the issue of privacy in the context of surveillance. The courts must remain adaptable to these evolving challenges while steadfastly safeguarding fundamental privacy rights. The principles of

proportionality, necessity, and respect for individual dignity must remain central to any judicial analysis of surveillance measures, ensuring the delicate balance between national security and personal liberty.

In conclusion, the evolution of surveillance law in India reflects a progressive recognition of privacy as a fundamental right. The courts have consistently strived to navigate the complex balance between protecting national security and safeguarding individual rights. As new challenges emerge in an increasingly monitored world, the judiciary must continue to engage with these critical issues, ensuring that the principles of privacy and liberty are upheld in the face of evolving technologies and national security concerns.

REFERENCES

1. Saddiki S. Border Fencing in India. In: World of Walls. Open Book Publishers. 2017;p. 37–56. Available from: https://www.openbookpublishers.com/books/10.11647/obp.0121/chapters/10.11647/obp.0121.03.
2. Border Surveillance System (BOSS) - BEL. Indian Defense Surveillance Technology, India. 2024. Available from: https://bel-india.in/product/border-surveillance-systemboss/#:~:text=Border%20Surveillance%20System%20(BOSS)%20provides,for%2014%20days%20continuous%20operation.
3. DefenceXP. Military Drones in India and Pakistan: A Detailed Analysis. Indian defense analysis, India. 2024. Available from: https://www.defencexp.com/military-drones-in-india-and-pakistan-a-detailed-analysis/.2024.
4. Chansoria M. A Perspective on India. Proliferated Drones. *Center for a New American Security*. 2023;p. 1–24. Available from: http://drones.cnas.org/reports/aperspective-on-india/.
5. SPS Land Forces. Technologies used in Border and Perimeter Security — The Indian Context. Indian border technology developments, India. . Available from: https://www.spslandforces.com/story/?id=426.
6. Hindustan Times. Rajnath inaugurates smart fence in Assam to curb illegal border crossings, India. Mar 06, 2019. Available from: https://www.hindustantimes.com/india-news/rajnath-inaugurates-smart-fence-in-assam-to-curb-illegal-border-crossings/story-tllLuQy3NBStimKGdm8T6J.html,%202018.
7. Boukhalfa S, Amine A, Hamou RM. Border Security and Surveillance System Using IoT. *International Journal of Information Retrieval Research*. 2021;12(1):1–21. Available from: https://dx.doi.org/10.4018/ijirr.289953.
8. When bodies become data: Biometric technologies and freedom of expression. ARTICLE 19. UK. 2021. Available from: https://www.article19.org/biometric-technologies-privacy-data-free-expression/.
9. Kak A. Regulating biometrics: Global approaches and open questions. *Global Policy*. 2021;12(S2):28–38. Available from: https://just-tech.ssrc.org/citation/regulating-biometrics-global-approaches-and-open-questions/.
10. 17.Supreme Court Observer. Extension of Border Security Forces Jurisdiction in Punjab | Day1: Court frames issues. India. 2024. Available from: https://www.scobserver.in/reports/extension-of-border-security-forces-jurisdiction-in-punjab-day-1-court-frames-issues.
11. Naga People's Movement of Human Rights v. Union of India. (1998) 2 SCC 109 (India). 1998. Available from: https://indiankanoon.org/doc/1072165/.
12. S.R. Bommai v. Union of India, (1994) 3 SCC 1 (India). . Available from: https://indiankanoon.org/doc/60799/.
13. M.P. Sharma & Ors. vs. Satish Chandra, (1954) SC 300 (India). . Available from: https://privacylibrary.ccgnlud.org/case/saroj-rani-vs-sudarshan-kumar-chadha.
14. Kharak Singh v. State of U.P., AIR 1963 SC 1295 (India). . Available from: https://indiankanoon.org/doc/619152/.
15. Gobind v. State of Madhya Pradesh. (1975) 2 SCC 148 (India). . Available from: https://indiankanoon.org/doc/845196/.
16. Malak Singh v. State of Punjab and Haryana, (1981) 1 SCC 420 (India). . Available from: https://indiankanoon.org/doc/971635/.
17. People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301 (India). . Available from: https://indiankanoon.org/doc/31276692/.
18. Distt. Registrar & Collector v. Canara Bank, (2005) 1 SCC 496 (India). . Available from: https://indiankanoon.org/doc/1068532/.
19. Selvi v. State of Karnataka, (2010) 7 SCC 263 (India). . Available from: https://indiankanoon.org/doc/338008/.
20. In re: The Berubari Union & Exchange of Enclaves, (1960) 3 SCR 250 (India). . Available from: https://indiankanoon.org/doc/1120103/.
21. Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India). . Available from: https://indiankanoon.org/doc/91938676/.
22. Sahana System. Pioneering Electronic Warfare (EW), Information Warfare (IW), and Next-Gen Defense Strategies: AI-Powered Border Security. 2024. Available from: https://www.sahanasystem.com/pioneering-electronic-warfare-ew-information-warfare-iw-and-next-gen-defense-strategies-ai-powered-border-security/.
23. Maneka Gandhi v. Union of India, (1978) 1 SCC 248 (India). . Available from: https://indiankanoon.org/doc/1766147/.
24. Chandrasekaran GCA. Invisible Sword Arm: Unmanned Vehicles in Border Management. *Electronic Journal of Social and Strategic Studies*. 2021;02(01):111–133. Available from: https://www.ejsss.net.in/article_html.php?did=9316&issueno=0.
25. Langeh A, Sudhakar R. Understanding the role of military intelligence in the India-China border conflict. *International Journal of Multidisciplinary Research*. 2024;2(9):729–740. Available from: https://theacademic.in/wp-content/uploads/2024/10/69.pdf.