Using Technology for India's Border Surveillance and Developing Vision 2047: Protecting Borders, Facilitating Progress

Dr Khyati Jagatkumar Patel
Assistant Professor
SEMCOM
The Charutar Vidya Mandal University
Vallabh Vidyanagar

Introduction:

With more than 15,106 km of land boundaries shared with 7 bordering countries, India has always placed a high priority on border monitoring and national security. Strong and cutting-edge border security measures are essential given the on-going problems of smuggling, illegal immigration, and cross-border terrorism. Conventional surveillance techniques, such static fencing and physical patrolling, have frequently shown themselves to be insufficient in dealing with these changing dangers. In response, India has started incorporating state-of-the-art surveillance technologies to improve its border security framework, including as radar systems, drones, and satellite-based monitoring.

The Border Surveillance System (BOSS), created by Bharat Electronics Limited (BEL), is one of the major advancements in India's border investigation scheme. Along sensitive border areas, this system combines radar and electro-optic sensors to give real-time surveillance and timely threatening abilities. BOSS greatly decreases human reliance while increasing threat detection and response efficiency through the use of cutting-edge imaging and motion detection technology. In distant and high-altitude edge areas where physical guarding is difficult, the use of such technologies is especially important.

Additionally, India has been using drones and unmanned aerial vehicles (UAVs) more frequently to supplement ground-based monitoring. The Indian Armed Forces, Searcher Mk II, and DRDO's Netra for floating investigation, intellect meeting, and real-time risk valuation are examples of technology advancements in border security, according to research. Security officers can effectively monitor broad and inaccessible areas thanks to these drones' high-resolution image and thermal detection capabilities. Furthermore, by providing geospatial intelligence in border regions, including satellite descriptions from India's RISAT and Cartosat platforms improves situational consciousness even more.

In order to strengthen border security, especially in high-risk locations like the borders with Bangladesh and Pakistan, India has also installed automated surveillance towers, laser fence, and floodlighting. According to a study by SPS Land Forces, floodlighting alongside the western boundaries has enhanced night time observing, and laser barrier skills have been installed in vulnerable areas to identify and stop

unauthorised crossings. India's strategy shift towards intelligent border security solutions is seen in these technology interventions and an Integrated Border Management System (IBMS). Utilising cutting-edge scrutiny skills will be a crucial component of India's border security architecture as it advances towards its Vision 2047, a long-term planned map for nationwide growth. India wants to create a more robust and technologically advanced security system by combining AI-driven risk discovery, automatic device systems, and geospatial intellect. This study looks at how technology is changing India's limit scrutiny systems and how these developments fit with the country's larger security and development goals.

India's Existing Border Safety Structure:

By incorporating cutting-edge skills to monitor and protected its vast and diverse borders, India has greatly updated its border safety scheme. A key component of this modernisation is the Comprehensive Integrated Border Management System (CIBMS), which integrates a number of surveillance technologies and systems to improve threat identification and reaction in real time. Motion sensors, laser barriers, and imposition discovery schemes are all part of the multi-layered security grid used by the CIBMS. Real-time monitoring and prompt responses to breaches are made possible by their integration into centralised control centres.

For example, the BOLD-QIT (Border Electronically Dominated QRT Interception Technique) scheme has been undertaken in the Dhubri area of Assam, where the Brahmaputra River presents difficult terrain. To efficiently monitor the border, this project makes use of optical fibre chains, digital movable radio communication, microwave communication, day and night security cameras, and interruption discovery systems.

Data from a range of surveillance equipment is analysed by AI algorithms, which highlight real risks and eliminate false positives. This feature facilitates the strategic deployment of security forces by enabling predictive analysis of infiltration patterns.

Conventional Monitoring Techniques:

Many traditional techniques, including boundary fence, floodlighting, ground guards, checkpoints, and social intellect systems, are used in India's border security. The Assam Rifles, Sashastra Seema Bal (SSB), Indo-Tibetan Border Police (ITBP), and Border Security Force (BSF) are vital to the country's international border patrol. These techniques operate as the main barriers to criminal activity and unauthorised crossings. They do, however, have certain inherent limits, especially in areas with deep forests and rough terrain. Restricting unauthorised movement has been made possible by the installation of physical barriers like floodlighting and fence. Boukhalfa et al. claim that in order to guarantee efficacy, security at international borders needs to be monitored continuously. Gaps still exist despite these efforts, making the frontiers susceptible to smuggling and infiltration.

Conventional Methods' Drawbacks:

Borders frequently cross through forested and mountainous areas, making on-going observation difficult. Because of the challenging terrain, visibility and accessibility are restricted, which increases the risk to security officers and decreases coverage. These regions have long been monitored using conventional border security techniques like organised patrols, security checkpoints, observation towers, and manual patrolling. However, these labour-intensive and immobile approaches fall short of offering seamless surveillance, especially in areas with harsh weather. Because severe weather and difficult terrain can make it difficult to monitor and respond effectively, relying solely on physical presence poses weaknesses. The extensive reliance on labour, which is both expensive and ineffective, is another major issue in border security. Technology-driven solutions are becoming more and more significant as security challenges like unlawful movement, trafficking, and cross-border violence change. According to the International Journal of Information Retrieval Research, staffs are overworked and response times in urgent situations are slowed down when large and difficult terrains are manually monitored. Efficiency is decreased by an over-reliance on human surveillance, especially when dealing with rapidly evolving dangers that call for prompt knowledge and action. This emphasises the necessity of AI-driven and automated surveillance systems to improve boundary safety actions. In addition to the difficulties caused by the ground and reliance on labour, boundary barrier by itself is not an infallible security solution. Fencing is an inadequate stand-alone defence since it can be cut, climbed, or circumvented, resulting in frequent unauthorised breaches. Furthermore, because of environmental limitations, challenging terrain, or diplomatic sensitivities, certain border areas are still unfenced. Even though border fencing is essential for stopping illegal crossings and smuggling, it is still vulnerable to breaches unless it is strengthened with cutting-edge technology solutions. Smart fence, real-time scrutiny, and AI-powered checking must be integrated to close these loopholes in order to improve border security and guarantee a more efficient and proactive defensive system.

Using Cutting-Edge Technologies:

One important step in bolstering border security has been the implementation of biometric technologies at border crossings. Iris scanning, fingerprint identification, and facial recognition are examples of contemporary biometric techniques. However, there are issues with privacy, accuracy, and possible bias with biometric technologies. The deployment of biometric monitoring must strike stability between safety requirements and the defence of human rights, as per the guidelines of Article 19. The accuracy of biometric data is one important concern. Research cautions that outward behaviours and facial expressions are not necessarily trustworthy markers of identity or purpose. The need for a strong legal framework to regulate the use of biometric mass monitoring is highlighted by the issues surrounding it. These difficulties emphasise the need to use complementary technologies, including Internet of Things-based investigation, to improve limit safety while reducing the drawbacks of biometric systems. Drones, automated surveillance systems, and smart sensors can now be integrated by border security authorities

thanks to the Internet of Things (IoT). Improved border security has been made possible by drones with motion sensors and cameras. According to studies, their suggested method can identify human motions in real time from drone video data.

This method allows for 24-hour surveillance without requiring continuous human interaction. Building on these developments, the incorporation of machine learning and artificial intelligence improves border security even further by facilitating automated decision-making and predictive danger detection. Machine learning algorithms are used by AI-driven border security systems to identify irregularities and anticipate risks. The Grouping Cockroaches Classifier (GCC), one such system, usages bio-inspired methods to identify undesirable people based on motions rather than facial gratitude. While reducing privacy and racial prejudice problems, the AI-driven classification system improves accuracy. Additionally, decision-making can be automated by AI-powered surveillance systems, enabling border security personnel to react quickly to possible threats. A risk level classifier and alert caution scheme classify dangers in real-time, grading them from harmless to high-danger points, according to research on AI-based video surveillance. These developments greatly enhance border security without requiring more personnel.

Legal and Ethical Issues:

Advanced surveillance techniques improve security, but they also bring up moral questions about data protection and privacy. Inadequate management of biometric databases might result in "mission creep," which is the repurposing of security-related data for unrelated objectives. Human rights may be violated if biometric surveillance is not subject to a defined legal framework.

AI-powered surveillance technologies also need to be accountable and open. The "black box" issue—where machine knowledge processes make conclusions without providing explicit clarifications—is highlighted by research on automated decision-making. For AI-based surveillance systems to remain trustworthy and avoid abuse, accountability is essential. India's border security system is vast, yet it faces many obstacles in terms of workforce efficiency, terrain adaptation, and changing threats. While traditional approaches offer a basic security layer, incorporating technology-driven keys like biometrics, IoT, and AI can improve response times and efficiency.

To guarantee ethical use and adherence to human rights standards, these technologies must be used in combination with strict regulatory frameworks. The future of border security depends on striking a balance between responsibility, privacy protection, and technical developments.

The Legal Frameworks that Oversee Border Security and Surveillance:

India's boundary safety is regulated by a number of bylaws and regulations designed to safeguard the country's territorial integrity while tackling contemporary security issues. The nation has increasingly relied on technology-driven surveillance to improve border management in response to changing threats like illegal migration, smuggling, and cross-border terrorism. Legitimate requirements, governmental

rules, and plan strategies, which give the principal administration the power to implement cutting-edge observing schemes like drones, biometric documentation, and artificial intelligence-based observation, largely shape the legal framework for border security. However, issues with privacy, data security, and individual rights are also brought up by the expanding use of digital technologies in border security. In view of India's dedication to legitimate values including the right to confidentiality, courts have stressed the necessity of striking a balance between national security and fundamental liberties. India's legislative system needs change to guarantee efficient authority, responsibility, and moral usage of numerical tools in border security as technology continues to influence border monitoring.

Union Authority and Legislative Competence:

Through Articles 245 and 246, read with Schedule VII, List I, the Indian Composition grants the Union Government broad governmental and managerial jurisdiction over border safety. These clauses give Parliament the authority to enact laws pertaining to "defence," "foreign affairs," and "border security." The central government can pass legislature and implement technological means to guarantee effective border surveillance thanks to this exclusive jurisdiction.

The necessity of centralised border security management is further reinforced by Article 355, which requires the Union to defend states against both internal unrest and external assault. Federalism-related discussions have been triggered by the Border Security Force's (BSF) jurisdictional extension into statuses like Punjab and Assam. The Supreme Court upheld the essential for federal intervention in security problems in Naga People's Movement of Human Rights v. Union of India (1998), despite certain state managements' claims that such extensions violate List II (State List) powers. As demonstrated in S.R. Bommai v. Union of India (1994), the judiciary has also established the idea that temporary changes in jurisdiction may be required due to national security issues.

Comprehending the Development of Surveillance Laws via Legal Analysis:

Cases such as M.P. Sharma v. Satish Chandra (1954) and Kharak Singh v. State of U.P. (1962) mark the beginning of surveillance law in India. Kharak Singh marked a significant change, placing the foundation for the ultimate appreciation of confidentiality as a critical module of individual freedom under Article 21 of the Indian Composition, while M.P. Sharma refused to acknowledge a legitimate right to discretion akin to the American Fourth Amendment. Gobind v. State of M.P. (1975) marked a turning point. In accord with Article 21, this historic decision clearly acknowledged the right to discretion as an important aspect of private authority. Importantly, the ruling established the "compelling state interest" test, which requires that any invasion of confidentiality be supported by a significant and urgent public purpose. This norm converted a pillar of later lawful discussions about surveillance and privacy.

In later cases, the guidelines set forth in Gobind v. State of M.P. (1975) were improved. Malak Singh v. State of Punjab & Haryana (1980) highlighted the need for focused investigation that is appropriate for the

goal being sought and based on reasonable grounds. This decision emphasised how crucial it is to use surveillance methods that are specifically designed to minimise violations of people's rights, especially those related to privacy and dignity. In People's Union for Civil Liberties (PUCL) v. Union of India (1997), the controversial topic of phone recording was examined by the courts.

The law court concern about the possibility of misuse of state power was reflected in this landmark case, which set stringent procedural protections for such investigation actions. The ruling emphasised the vital necessity for control and openness in surveillance measures, particularly those using insensitive tactics like telephone tapping, even as it acknowledged national security as a legitimate concern.

The conversation around surveillance and privacy has continued to be shaped by more recent cases like Selvi v. State of Karnataka (2010) and Distt. Registrar & Collector v. Canara Bank (2004). In the face of developing surveillance technology, these decisions have upheld the values of privacy and individual dignity, indicating the judiciary's continued dedication to striking a balance between the demands of national security and individual rights.

Although border security is not specifically addressed in the examples given, the confidentiality and proportionality principles expressed in these judgements are obviously valid to all types of state scrutiny, with those pertaining to national security and border control. The courts have generally held that any invasion of confidentiality must be narrowly tailored to accomplish particular security goals and must be supported by a compelling governmental interest.

While it is indisputable that the state must protect national security, the courts have repeatedly stressed that this cannot be used as a general excuse for excessive or uncontrolled surveillance. For example, the PUCL case illustrates the court's stress on strong technical protections and legal monitoring even in circumstances of nationwide safety, especially prior to the authorisation of intrusive measures like telephone tapping.

The foundation of India's boundary safety system is the Border Security Force Act, 1968. It creates the BSF and gives it the authority to fight infiltration, illegal immigration, and cross-border crimes. In order to strengthen collaboration with state forces and recover trans-border crime prevention, Section 139(1)(i) gives the Central Government unrestricted authority to extend BSF's prerogative.

The expansion of BSF's working authority into states with unstable limit areas, according to critics, may violate state autonomy. Nonetheless, when territorial sovereignty is at risk, national security considerations take precedence over state power, according to jurisprudence such as in re: The Berubari Union & Exchange of Enclaves (1960).

Furthermore, legal experts contend that increased BSF authority must be together with public freedoms to avoid excessive national overreach given the rise in cross-border infiltration and arms smuggling. In order

to ensure proportionality and need in border security interventions, the law lords have stressed that regulating controls must be in line with legitimate protections under Articles 19 and 21.

Technology-Driven Border Surveillance: A Legal Framework:

Digital surveillance and cyber security enforcement have a legal foundation thanks to the Information Technology (IT) Act, 2000 and current cyber security regulations. Key parts of the Act permit national interference in digital forensics, cyber spying, and cross-border intellect exchange. In order to facilitate the collection of boundary intellect, Section 68 gives the authority to concern directives for the interruption, monitoring, or decryption of any info via any processor reserve. While Section 69B permits administration activities to display and gather movement statistics from numerical systems in order to improve cyber security in border regions, Section 69A offers the government the expert to confine community admission to online information that is thought to pose a threat to national security.

Despite the fact that these regulations provide a legal foundation for biometric border controls, AI-powered monitoring, and UAV reconnaissance, questions about accountability and possible abuse still exist. India must implement judicial monitoring procedures to assurance devotion to the constitutional guarantees of confidentiality and freedom of movement in light of the international pushback against mass surveillance initiatives.

The Right to Confidentiality and the Digital Personal Data Protection (DPDP) Act of 2023:

A significant step towards protecting digital privacy in India has been taken with the passage of the Digital Personal Data Protection (DPDP) Act, 2023. But its provisions also have significant effects on state surveillance and border security. Notably, the government may exempt itself from several restrictions in the sake of nationwide safety under section 17 of the Act. Biometric and personal data can be collected, processed, and stored thanks to this exemption, especially in critical border areas where security is a top priority.

Such actions raise serious concerns about the possibility of unnecessary state scrutiny and the lack of strong governmental and legal accountability, even though they may be defensible on the grounds of nationwide safety and counter-terrorism initiatives. According to Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), the statutory framework safeguarding confidentiality emphasises that any data gathering procedure must follow the principles of need, proportionality, and legality. In this historic decision, the Supreme Court emphasised that governmental monitoring must be subject to lawful protections to stop random interruptions and acknowledged the Right to Privacy as an essential component of Article 21 of the Indian Constitution. Any exception granted under the DPDP Act must be carefully examined to make sure it satisfies the legitimate requirements of reasonableness and proportionality in light of this legal precedence. The extensive powers granted by Section 17 could result in uneven scrutiny

in boundary areas without sufficient supervision measures, impacting both security issues and basic rights. Therefore, India's data protection system needs to change in order to carefully balance the defence of individual privacy rights with national security imperatives, especially in sectors where security-related observation is more prevalent.

AI and Boundary Safety: Legal and Ethical Difficulties:

While improving monitoring capabilities, the use of AI-powered surveillance in border security raises serious concerns about algorithmic preference, fabricated positives, and the possibility of ethnic outlining. AI-driven facial recognition systems excessively misidentify racial factions, according to empirical research, which raises the possibility of erroneous detentions and unfair treatment of vulnerable groups at border checkpoints. The constitutionality of automated surveillance systems that function without sufficient human control is called into doubt by these problems.

In Maneka Gandhi v. Union of India (1978), the Supreme Court upheld the idea that state actions affecting individual liberties must follow due process by establishing that any constraint on vital human rights must be fair, just, and sensible. Additionally, when automatic decision-making in boundary safety is carried out without humanoid participation, it may interrupt Articles 14 and 21 of the Indian Constitution because it denies people the opportunity to question or encounter incorrect results produced by AI. In order to assure compliance with fundamental rights, AI-driven surveillance technology must have strong oversight systems, clearness in algorithmic decision-making, and protections in contradiction of biased consequences in light of these ethical and constitutional concerns. In order to safeguard that border surveillance does not violate civil rights, India's lawful strategy must strike stability between safety considerations and legitimate rights. India has to create a thorough legal framework to effectively control the use of AI-driven surveillance in border security due to its complexity and ethical issues. Transparency in AI decision-making processes should be given top priority in such a framework, guaranteeing that the reasoning behind AI-generated surveillance results is understandable and responsible. Legislative clarification on culpability for faulty identification is also necessary, addressing the possible legal repercussions for misidentifications that could result in unjustified detentions or rights abuses. Strict regulations for AI-based threat classification must also be put in place in order to stop discriminatory or arbitrary targeting and guarantee that AI systems function within well-defined ethical and legal bounds. Last but not least, India's regulatory strategy must incorporate international preeminent performs to protect essential privileges while upholding national safety constraints, in accordance with United Nations standards on the moral usage of AI in regulation implementation.

Managing India's Complex Border Security Difficulties:

India faces many obstacles as it looks to improve border security using cutting-edge technologies like biometric identification, AI-driven scrutiny, satellite observing, and automatic reply schemes. These difficulties can be largely divided into two categories: external (geopolitical, cyber security, and cross-

border threats) and internal (policy, legal, infrastructure, and operational obstacles). Even though technology improves efficiency and security, its integration needs to be carefully controlled to prevent surveillance issues, legal overreach, and national security weaknesses. We can make comparisons between boundary safety actions and the potential consequences of an excessive dependence on know-how deprived of sufficient protections by examining India's legitimate position on investigation and confidentiality, as covered in the text. The lawful and legitimate limitations on mass monitoring and discretion are one of the main internal obstacles India has when incorporating technology into border security.

Numerous rulings from the Supreme Court emphasise the necessity of strict precautions when putting monitoring systems in place. For example, the PUCL v. Union of India (1997) decision highlighted the need for due process and legal control of mass surveillance. According to the Supreme Court's interpretation in Justice K.S. Puttaswamy v. Union of India (2017), which acknowledged the Right to Privacy as a fundamental right, extensive facts gathering at border checkpoints—through biometric scanners, facial recognition cameras, and AI-based movement tracking systems—may result in violations of Article 21 (Right to Life and Personal Liberty). To address this, India wants to enact specific laws that govern border surveillance, guaranteeing that any information gathered is safely stored, used appropriately, and erased after an Oversight Authority assists in reviewing and auditing surveillance activities, guaranteeing adherence to lawful outlines and stopping exploitation.

India's boundary areas frequently have inadequate digital infrastructure, which makes it challenging to install and operate sophisticated surveillance systems, especially along the Line of Actual Control (LAC) with China, the Line of Control (LoC) with Pakistan, and the India-Myanmar border. The effectiveness of AI-based monitoring and satellite tracking is impacted by distant border parts' lack of a steady power supply, fast internet, and dependable device systems. Along the borders with Bangladesh and Pakistan, the government has invested heavily in smart fencing and the Comprehensive Integrated Border Management System (CIBMS). However, antiquated infrastructure, an absence of qualified workers, and technical issues continue to be significant barriers. Technology integration must be done gradually, beginning with high-risk areas where infiltration risks are highest. Infrastructure deficiencies can be addressed with savings in solar-powered scrutiny posts, satellite-based announcement, and autonomous drone observing. Interagency coordination problems are another obstacle to technological integration in border security. There is an absence of cohesive command and data-sharing procedures since various activities, including as the Border Security Force (BSF), Indo-Tibetan Border Police (ITBP), Assam Rifles, and local law implementation, function under disparate directives. Mechanisms for gathering intelligence and responding to it become ineffective as a result of this fragmentation. Furthermore, manual intervention in automated surveillance systems frequently leads to bureaucratic bottlenecks, delays, and incorrect data interpretation. Additionally, border workers might not have the technical know-how needed to successfully run and maintain AI-driven security infrastructure. All border safety activities should be

integrated into a centralised AI-driven intellect system through the implementation of a single digital command and control system in order to handle these issues. In order to procedure real-time data and mechanically notify security personnel of any dangers, this system should employ machine learning techniques. In order to ensure effective and coordinated responses to new security threats, border staff must also participate in frequent training programs that acquaint them with cyber security procedures and AI-based decision-making tools.

Another major worry is the possibility of government overreach and widespread spying. Concerns regarding excessive surveillance have previously been raised by the National Intelligence Grid (NATGRID) and Central Monitoring System (CMS), which were created for national security. Widespread privacy violations could result from the implementation of boundary safety skills like biometric monitoring, AI-powered drive study, and automatic drone scrutiny without adequate omission. Supreme Court decisions in instances like Gobind v. State of Madhya Pradesh (1975) and Kharak Singh v. State of Uttar Pradesh (1963) have established lawful instances for confidentiality defences and cautioned against unrestricted surveillance. When border security measures are expanded to monitor residents in border areas, possibly criminalising cleared travel and activities, these concerns become even more serious. A Privacy and Surveillance Regulatory Framework must be implemented to set detailed instructions for data collecting, storage, and access permissions in order to stop such overreach. To ensure accountability and transparency, any extended scrutiny or use of invasive biometric documentation methods in border regions should be subject to judicial oversight.

India's attempts to improve technology border security are complicated by external dangers in adding to domestic ones. India is more vulnerable to cyber-attacks from adversarial countries and non-state actors as AI-based investigation, drone patrolling, and satellite television message develop essential components of boundary safety. AI-based dis-information campaigns, GPS spoofing, and signals jamming can all be used to distort boundary intellect, deceive safety personnel, and cause working misperception. India's border security infrastructure has to incorporate block chain-based data verification processes, AI-driven anomaly detection systems, and end-to-end encryption protocols to combat such cyber threats. In order to reduce risks and protect vital infrastructure, a Cyber security Task Force for Border Protection would be established in cooperation with the Defence Cyber Agency (DCA) and the Indian Computer Emergency Response Team (CERT-In).

Diplomatic difficulties with neighbouring nations may potentially result from the installation of automated security systems, drone monitoring, and AI-driven surveillance at India's borders. India's amplified use of sophisticated boundary safety events may be interpreted by China, Pakistan, Nepal, and Bangladesh as a provocative military build-up that could escalate border tensions. Both sides of the Indo-Chinese border dispute in Ladakh have already escalated their use of technology, depending on cyber warfare strategies, satellite imagery, and AI-driven military monitoring. Similarly, the use of unmanned surveillance drones along the border between India and Pakistan could be interpreted as aggressive military posturing, which

could have an impact on diplomatic talks. India must involve in planned negotiation and confidence-building initiatives, such as creating bilateral agreements on technology deployments along sensitive borders, in order to avert such disputes. In order to guarantee that border safety skills are employed for cautious rather than aggressive objectives, fixed armed and intellect contacts with adjacent countries can assist reduce tensions and foster reciprocal investigation transparency norms.

Additionally, India needs to prepare for the adaptive tactics used by non-state actors, like terrorist organisations and smugglers, to evade AI-driven security measures. Oppositions may use AI-generated deep fake distinctiveness to trick biometric scanners, use cyber techniques to damage keen fences, or build concealed channels to avoid electric discovery, even though automated border surveillance is quite effective against conventional infiltration techniques. India needs to implement a multi-layered safety strategy that blends knowledge and social intellect to counter these changing threats. Security forces can anticipate and thwart advanced infiltration tactics by implementing counter-AI tools like deep fake detection algorithms and predictive analytics. Furthermore, a border intelligence network that incorporates AI-driven risk analysis models and local informants would be crucial for delivering real-time reports on new risks and guaranteeing prompt countermeasures. In conclusion, there is a lot of promise for integrating AI, biometrics, and automatic investigation into India's boundary safety, but there are also a lot of legal, infrastructure, cyber security, and geopolitical obstacles to overcome. To ensure that technology developments in border security are both efficient and morally sound, it will be crucial to attack stability between safety necessities and legitimate rights, invest in cyber pliability, improve inter-agency cooperation, and engage in political discussions. India can effectively use contemporary surveillance technologies to improve nationwide safety while respecting self-governing principles and humanoid privileges by tackling these issues in a comprehensive and flexible manner.

Conclusion:

India's surveillance laws have gradually but consistently acknowledged confidentiality as a basic right. The magistrates have worked hard to strike equilibrium between individual rights and legitimate governmental interests, particularly when it derives to surveillance. The important right to secrecy cannot be completely overshadowed by national security considerations, even though they are given due weight in legal discussions. Recent court rulings, however, have occasionally been contradictory in preserving these well-established concepts. There is a chance that nationwide safety anxieties will be used as an excuse for unrestricted surveillance activities as scrutiny know-hows develop and the state's scrutiny capabilities grow. This emphasises how vital it is to have attentive judicial review to guarantee that all scrutiny measures, especially those pertaining to boundary safety, follow the standards of necessity, proportionality, and esteem for discrete formality. The matter of confidentiality in the situation of scrutiny requires on-going and thorough discussion due to the quick speed of technological advancement and the growing reach of monitoring systems. The courts must steadfastly protect core privacy rights while remaining flexible in the face of these changing difficulties. Any court review of surveillance methods

must uphold the fundamental values of proportionality, need, and respect for separate pride in order to maintain the gentle equilibrium between individual freedom and national security.

In conclusion, a liberal understanding of confidentiality as a important right is reflected in the growth of surveillance law in India. The courts have continuously worked to strike a difficult balance between defending separate rights and preserving national security. The judiciary must continue to address these crucial issues as new challenges arise in a world that is more closely watched, making sure that the values of liberty and privacy are maintained in the face of changing technical progressions and nationwide safety apprehensions.

References:

1) Saddiki S. Border Fencing in India. In: World of Walls. Open Book Publishers. 2017;p. 37–56.
2) Border Surveillance System (BOSS) - BEL. Indian Defense Surveillance Technology, India. 2024.
3) DefenceXP. Military Drones in India and Pakistan: A Detailed Analysis. Indian defense analysis, India. 2024.
4) https://www.defencexp.com/military-drones-in-india-andpakistan-
5) aChansoria M. A Perspective on India. Proliferated Drones. *Center for a New American Security*. 2023;p. 1–24. Available from: http://drones.
6) SPS Land Forces. Technologies used in Border and Perimeter Security — The Indian Context. Indian border technology developments, India.
7) Hindustan Times. Rajnath inaugurates smart fence in Assam to curb illegal border crossings, India. Mar 06, 2019. Available from:
8) 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/
9) 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/.
10) Kak A. Regulating biometrics: Global approaches and open questions. *Global Policy*. 2021;12(S2):28–38. Available from:
11) Naga People's Movement of Human Rights v. Union of India. (1998) 2 SCC 109 (India). 1998. Available from: https://indiankanoon.org/doc/
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-vssudarshan-

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/

18) Distt. Registrar & Collector v. Canara Bank, (2005) 1 SCC 496 (India). . Available from: https://indiankanoon.org/doc/1068532/.

19) Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India). .

20) 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/

21) Maneka Gandhi v. Union of India, (1978) 1 SCC 248 (India). . Available from: https://indiankanoon.org/doc/1766147/.

22) 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.

23) 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.

Copyright & License:

© Authors retain the copyright of this article. This work is published under the Creative Commons Attribution 4.0 International License (CC BY 4.0), permitting unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.