AI AND MILITARY SURVEILLANCE: BALANCING NATIONAL SECURITY WITH CIVIL LIBERTY

Sri Subiksha D., B.A.LL.B. (Hons.), Sastra Deemed To Be University

Arunothaya Arasi M.P., B.B.A.LL.B. (Hons.), Sastra Deemed To Be University

ABSTRACT

Artificial Intelligence (AI) is one of the major parts of military surveillance across the world in this Twenty-first century. It helps the armies to use drones, facial recognition and spyware to track enemies, monitor borders, detect threats and make quick operational decisions. AI is also used to analyze satellite imagery and even predict patterns of insurgent, terrorist activity or hostile activities. Some systems can even coordinate multiple surveillance devices simultaneously, providing commanders with detailed situational awareness. This system operates 24/7 and processes massive amounts of data quickly and assists in decision making faster than human analysts. Though it gives speed and accuracy, it may cause mistakes sometimes. AI systems are also vulnerable to hacking, which results in stolen Intelligence, manipulated operations or unintended escalation of conflicts. For example in Libya "The Turkey's Kargu-2" drone attacked a person without human control and in India Pegasus spyware[1], a scandal revealed illegal surveillance of Journalists and activists. AI misuse in countries like Israel and the United States also led to civilian harm which breaches of privacy and serious civil liberties.

Keywords: Artificial Intelligence, Military Surveillance, Civil liberties, AI misuse, Peacekeeping

[1]https://www.delhipolicygroup.org/publication/policy-briefs/pegasus-privacy-and-national-security.html

Research problem:

The growing use of Artificial Intelligence in military surveillance raises legal concerns over violations of the right to privacy under Article 21 of the Indian Constitution. Despite protections under the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023, India still lacks an expanded legal framework to regulate AI-driven surveillance activities. The EU Artificial Intelligence Act (2024) adopts a risk-based approach to ensure transparency and accountability in AI deployment, yet under Article 2(3), it excludes military and national security applications. There is an urgent need for India to expand the scope of its existing laws to balance national security with civil liberties."

Background of the Study

Artificial Intelligence has become central to modern military surveillance systems worldwide, revolutionizing how governments gather intelligence and respond to threats. AI enables continuous monitoring through advanced sensors, facial recognition, and data analysis, making defense operations faster and more efficient. However, the same tools can be used for mass surveillance, profiling, and manipulation, leading to violations of privacy and human rights.

Globally, nations have taken different approaches to regulate military use of AI. The European Union has proposed ethical standards under the AI Act (2024), the United States relies on independent oversight by the Privacy and Civil Liberties Oversight Board (PCLOB), and Israel uses AI for precision targeting but faces criticism for civilian harm. In contrast, India's current legal system is governed by the Indian Telegraph Act (1885), Information Technology Act (2000), and Digital Personal Data Protection Act (2023) which lacks specific safeguards for AI surveillance.

This study arises from the growing need to assess whether India's legal and constitutional protections under Articles 14, 19, and 21 are sufficient to address these new challenges. It explores how India can strengthen its framework to ensure that military AI surveillance serves national security without infringing civil liberties.

Literature Review

1. Kartik Bommakanti (2021) in "AI in the Indian Armed Services:[2] An Assessment"

[2]https://share.google/zJAAJIQDj3MVvyjIn

observes that India's defence doctrine acknowledges the potential of Artificial Intelligence in surveillance and warfare but lacks detailed implementation and oversight strategies for ethical use.

2. Merin Bency (2025) in "AI Regulation in India: Through the Lens of Constitutional Ethics"[3] discusses how the absence of AI-specific laws creates uncertainty in regulating AI-driven surveillance and emphasizes the need for constitutional safeguards rooted in privacy and proportionality.

3. Preksha Singh (2025) in "Mass Surveillance in the Age of AI[4] – The Indian Dilemma of Security versus Privacy" explores how mass surveillance powered by AI challenges India's legal balance between national security and civil liberties, stressing that current laws like the IT Act are inadequate for modern AI tools.

4. Apoorva Thakur and Manish Kumar (2024) in "Right to Privacy vis-à-vis Artificial Intelligence:[5] Indian Scenario" highlight that AI's capacity to process massive personal data threatens privacy and data protection, especially under Article 21 of the Indian Constitution.

5. Niharika Puri (2025) in "Watching the Watchers: AI Surveillance, Privacy, and India's Constitutional Vacuum in the Shadow of the EU AI Act"[6] links India's lack of AI regulation to global frameworks such as the EU AI Act, noting that while international models advance AI accountability, India's national security applications remain outside formal oversight.

However, these contributions tend to discuss AI surveillance in general or civilian contexts; few studies focus specifically on the intersection of military surveillance, algorithmic decision-making and constitutional rights in India.

Therefore, this study seeks to fill that gap by examining how India can balance national security imperatives with fundamental rights under Articles 14, 19, and 21 in the deployment of military

[3] https://share.google/G1b0dkBDLJjaO3fMW
[4] https://share.google/TVgJWKWYZlvd88FgL
[5] https://share.google/KGhfakxychizp7EUg
[6] https://share.google/8M1al4R8SXzTzCJYh

AI surveillance.

Research Objectives

1. To analyze the scope and challenges of AI use in military surveillance in India.

2. To examine the legal implications of AI misuse in national security operations.

3. To analyse how military surveillance affects the fundamental rights under Articles 14, 19, and 21 in India.

Research Questions

1. How is Artificial Intelligence currently being used in India's military surveillance and national security operations?

2. Identify and explain the primary risks, errors, and ethical challenges associated with the use of Artificial Intelligence in the military surveillance sector.

3. How can India balance national security imperatives with constitutional rights and international peacekeeping obligations?

Research Methodology

This study follows a doctrinal research method. It focuses on constitutional provisions, particularly Article 21, and statutory frameworks such as the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023. The research highlights the existing gaps within these laws in regulating AI-based surveillance and protecting fundamental rights in India.

1. INTRODUCTION

In this Twenty-first century, AI is rapidly becoming the most important component in military surveillance and security worldwide. Militaries mostly rely on AI powered drones, satellite imagery analysis, predictive analytics, autonomous robots, and cyber intelligence platforms to improve operational efficiency. The adoption of AI in the military is not limited to offensive operations. It is also used for defensive measures, border surveillance, disaster response and

support to peacekeeping missions. AI can track troop movements, analyze satellite imagery, and even predict potential conflicts before they occur. By combining multiple data sources, the military can make better informed decisions in high pressure situations quickly which helps reduce time consumption and improve operational efficiency.[7]

However the rapid use of AI brings several challenges. AI systems can make mistakes due to algorithmic errors, biased data, or technical malfunctions. AI systems may misidentify civilians, misrepresent intelligence or malfunctions during critical operations which lead to unintended consequences. Hacking further complicates the situation, as adversaries can manipulate AI systems, access sensitive information illegally. These risk questions about civil liability and accountability, as it is always unclear whether government, military authorities, or technology developers should bear responsibility for AI related harm. Establishing clear legal frameworks and ethical guidelines is crucial to address these challenges and maintain public trust.[8]

The international humanitarian norms and peacekeeping are also influenced by AI. Mistakes or abuse may escalate the conflicts, threaten the safety of the civilians, or interfere with humanitarian operations. Peace keeping missions are based on impartiality, credibility and truthfulness. The creation of any errors by a system that uses AI may be against these principles. The countries tackle these issues in various ways like the European Union focuses on rigorous ethical standards, the United States focuses on review boards and transparent actions, Israel focuses on clarity in targeting and China is practicing mass surveillance with minimal responsibility. In the meantime, there is the Constitution and Data protection laws that cover India. It has few restrictions on military AI that poses a possible loophole in control and accountability. With a careful balance between technological innovations and accountability, global collaboration, and humanitarian values, Ai can increase the level of national security, better the peacekeeping operations, and save the lives of civilians. This paper discusses the AI uses in army surveillance, errors and hazards taken and their attempts on peacekeeping and civil liability. It also looks at the legal and policy framework of India as compared to the global practice.[9]

[7] https://www.brookings.edu/articles/the-risks-of-artificial-intelligence-in-military-applications/
[8] https://lawfullegal.in/the-role-of-ai-surveillance-does-it-threaten-the-right-to-privacy/
[9]https://ohrh.law.ox.ac.uk/ai-surveillance-and-privacy-in-india-human-rights-in-the-age-of-technology/

2. AI Use in military surveillance

Modern military surveillance is built on three promises such as to see more, to process faster and to decide sooner. Artificial intelligence has become the key technology that allows armed forces to reach these promises by combining sensors together such as satellites, drones, radars, and CCTV systems with larger volumes of data and communication. AI systems can detect patterns, highlight abnormality and reduce the overwhelming flow of information. This means the commanders do not have to look through endless streams of raw footage or reports. Instead they receive a small set of alerts and they can act upon it. Though this has made surveillance more powerful, it has also created new dangers and ethical problems. [10]

2.1 Main application of AI in surveillance

One of the most common and visible uses of AI is drones and other unmanned systems. AI is developed either in ground control or onboard systems to help drones to navigate, recognise people or vehicles and track moving targets. In most of the cases AI is mainly used as eye on sky, with AI helps to filter and tag hours of video footage. In other cases autonomy goes further with loitering munitions that can stay in air, identify the target type and even attach with little human involvement. This loitering munitions are also referred as a suicide drone. The Turkish Kargu-2 drone used in Libya is one of the examples that raised serious concerns about whether humans are still in charge of life or death decisions.

AI is also used in facial recognition and other biometric systems. These tools compare faces, body shapes, or walking styles to large databases in order to find specific people. Militaries and police use this kind of surveillance at checkpoints to protect bases and also in crowded cities. The way China uses large scale surveillance and face recognition in Xinjiang, shows tools developed for security can be used to watch and control the entire population. These technologies are more powerful but still they have more flaws.

Another important use is the analysis of satellite and aerial images. Modern conflicts are tracked from above, AI is now used in spotting new bunkers,troop gatherings or military vehicles. Once this took many days for analysts but nothing can be done within a few minutes. NATO and other alliances are investing more in this technology to give them early warning of

[10] https://unidir.org/publication/artificial-intelligence-military-decision-making

threats. By combining images from different sources, such as radars, heat sensors and normal cameras, AI can provide a clear picture.

AI is also applied in signals and cyber surveillance. Modern wars create mountains of digital information from phone calls, texts and internet traffic. AI systems are used to pick out suspicious activities or hidden networks within this data. Spyware such as Pegasus created by the NSO Groups is one of the high profile cases. Pegasus could secretly enter into smartphones, could collect messages and even turn on microphones and cameras. Investigations showed that it was used against journalists and activists in many countries including India. This case shows how tools meant for national security can be turned inwards and threaten democracy and civil rights.

Militaries are using AI for prediction and decision support. These systems try to forecast where conflicts might start, how enemies might move and where to send resources. If this information is correct, they can save lives and prevent attacks. But if the prediction were wrong it can mislead commanders or give false confidence leading to mistakes on the battlefield.

2.2 Advantages of AI in military surveillance

The main attraction of AI is that it can do things faster and at a larger scale than humans. Unlike soldiers or analysts AI does not get tired and it can work 24/7. It has the ability to notice small changes across different kinds of data that humans might miss or take longer time to connect. It allows smaller military teams to cover more grounds and act with the kind of awareness the once required much bigger forces.

2.3 Problems and dangers

- **Misidentification**

AI vision systems do not always recognize objects correctly, especially in difficult conditions. Civilians can be mistaken for combatants or everyday vehicles for weapons.

Example - US drone strike in Kabul, Afghanistan, in August 2021. At that time American forces were on high alert after an ISIS-K attack at the airport. The surveillance systems flagged a car as suspicious, interpreting the driver's activity as preparing for another bomb blast. Based on this assessment, a strike was launched. Later it was revealed that the man was an aid worker

not a terrorist and the 10 civilians we killed including 7 children. Though the final strike was approved by humans, their decision was heavily based on automated intelligence assessments.

The kabul incident is not isolated. Similar misrepresentation risks appear whenever AI is implemented in fast moving environments. For countries like India, which may use AI to monitor borders or conflict zones. The danger is clear: if the AI cannot reliably distinguish between a farmer carrying a tool and a militant with a weapon, innocent lives could be lost, with massive political and ethical consequences.[11]

- **Lethal autonomy - When Machines act alone**

If a weapon can select and strike a target without human approval. These are often called Lethal Autonomous Weapons Systems (LAWS), which are also known as killer robots. These Military systems that use artificial intelligence and robotics to independently search for, select, and engage targets without direct human intervention in the critical decision-making process. They raise questions about accountability. If the mission kills the wrong person who is responsible? The programmer of the commander or the machine itself.[12]

Example Kargu-2 drones in Libya . In 2020,a United Nations report described how these drones, supplied by Turkey, attacked without human command. This was the first incident where the machine acted independently, choosing to kill a human. This raises the question of whether the drone correctly distinguishes between a soldier and the common people? Did it have the capacity to follow international law which requires distinguishing combatants from civilians?

Machines cannot make such moral judgments, yet they were given the powers to act.

International experts including those who are at the United National have repeatedly warned that lethal autonomy crosses a dangerous line. Many argue for a global treaty for banning fully autonomous weapons,insisting that human control must be required. As for India, adopting autonomy without clear policies could drag the country into a legal grey zone where accountability vanishes.

[11] https://www.nytimes.com/2021/09/10/us/kabul-drone-strike.html
[12] https://undocs.org/S/2021/229

- **Bias in AI**

If the data used to train AI is biased, the system will inherit those flaws. AI does not think like humans, it learns by identifying patterns in a large set of past information. But if that information is biased, then the system simply reproduces those flows. For example facial recognition systems are less accurate with certain ethnic or racial groups. This can lead to unfair targeting, wrongful arrests, or discrimination.

In the United States the studies showed that commercial face recognition systems were far less accurate while identifying African-American females.[13] In a military operations police context such bias can lead to wrongful arrests, unfair targeting, or even lethal mistakes.

In Xinjiang[14]facial recognition AI has been used to monitor Uighur Muslims. These systems used to track where people go, who they met, and even how often they visit the mosque. The technology was built in such a way that automatically treats Uighurs as suspicious. Facial recognition often makes more mistakes with minority faces so that people can be easily flagged or arrested. This is not simple misidentification but systematic discrimination based on AI surveillance. Such practices show how bias in AI can be weaponised not just as a technical failure but as a tool of oppression.

The mistakes in Military Surveillance are both just bugs in code but they can lead to wrongful deaths, erosion of civil liberties and damages to peacekeeping efforts. A single wrong in algorithms can affect hundreds of decisions in minutes, far faster than human mistakes even could.

- **Privacy invasion and mass surveillance**

Pegasus spyware scandal[15]- Pegasus was developed by Israel cyber-arms company NSO Group. They marketed it as a counter terrorism tool but ended up being implemented against journalists, lawyers, and activists in dozens of countries. In India, forensic investigations showed that several civil society members had their phones infected, which allowed their private messages, location, and even microphone feeds to be taken. This danger here was not

[13] https://share.google/8crX1nHTesONJmrvV
[14] https://www.technologyreview.com/2019/04/09/136094/how-chinas-ai-surveillance-works/
[15] https://main.sci.gov.in/pegasus-report-2022/

a technology failure, but it was misused. A system was meant to fight external threats but it was turned inward against the citizens.

In India surveillance is regulated by the telegraph Act of 1885 and the Information Technology Act of 2000, both allow interception in the name of national security. However the approval came from the executive (government), not from the judiciary. This raises a constitutional question, especially in the light of Article 19, which guarantees freedom of speech and expression. In 2021, the Supreme Court appointed a committee to investigate the Pegasus allegations, which criticized the lack of transparency in the state's surveillance. This shows how weak oversight mechanisms allow misuse of advanced surveillance technology against citizens, which damages their civil liberties.

Project Maven- In the US, this program used AI to scan through endless hours of drone footage and highlight any possible threats. The idea was to reduce the human analysts' burden and to save them from staring at the screen all day. But when the news spread that Google was helping the Pentagon with Maven, thousands of its employees started protecting. They were worried that their technology would be used directly in warfare without proper oversight. Because of the public pressure, Google pulled out of this project.

Gaza conflict[16]**-** In 2023 - 2024, reports revealed that Israel used an AI system to speed up the process of selecting bombing targets. They used 2 systems called Gospel and Lavender. Gospel is used to scan huge amounts of surveillance data to find the targets such as buildings, vehicles or people linked to an enemy group. Once it finds something, it automatically sends it to a human analyst, who may then pass it on for attack. Lavender is used to generate a database of tens of thousands of Palestinian men and make them as suspected members of Hamas or Islamic Jihad.

Instead of spending weeks by human analysts for cross checking intelligence, the AI could produce a list of possible targets within hours. When the system treats such a large list there is a chance that innocent people can be easily included in that list because of their less or indirect connection.

[16] https://www.972mag.com/gospel-lavender-ai-israel-gaza/

3. AI and peacekeeping during wartime

Peacekeeping in this modern world has never been simple and the rise of AI has added both opportunities and dangers. The purpose of peacekeeping is to stop wars, protect civilians and maintain stability after conflicts. The United Nations peacekeeping operations started in 1948 work under three key principles:

1. Consent of the parties involved
2. Impartiality and
3. Non use of force except in self defense and defense of the mandate [17]

But as technology evolves these traditional principles are being tested by the growing use of AI in military and peace operations. Its dual use nature which is used to protect the lives can also be used to take them. When the AI begins to make autonomous decisions about life and death, it risks undetermining the humanitarian ideas that peacekeeping stands for.

In many UN missions, AI is now being used for surveillance and reconnaissance. Drone and satellite powered by AI monitor ceasefire lines, identify troops movements, and detect hidden explosives. For example, the Democratic Republic of Congo (MONUSCO MISSION) used AI powered drones which helped to observe remote areas where human peacekeeping might be in danger. These technologies can analyse satellite images and identify early signs of violence or population displacement. Similarly AI tools were also used in data analysis and conflict prediction, scanning social media and communication patterns to detect potential riots or insurgent activity. The United Nations Digital blue Helmets[18] programs uses this kind of technology to protect against cyberattacks and online hate campaigns that could trigger real world violence. These uses of AI can save lives by giving early warning and better information.

But with these benefits come serious risks. Machines do not understand human emotions or ethics. If the AI system makes a mistake it could cause harm that no one intended. In 2020, a kargu-2 drone in Libya reportedly attacked a group of soldiers without human command. A UN report later said the drone acted on its own. This incident raises a question that who will be

[17] https://peacekeeping.un.org/en/principles-of-peacekeeping
[18] https://unite.un.org/digitalbluehelmets

responsible when a machine kills

Such incidents go against International Humanitarian Law (IHL)[19], which is built on the Geneva Conventions (1949) and Additional Protocol I (1977). These laws require soldiers to always distinguish between civilians and fighters and to make sure that any attack is proportional. AI systems however cannot truly make moral judgments or understand the value of human life. They only follow data and algorithms. When AI makes the wrong decision, there is an accountability gap where no clear person or government is held responsible.

Using Artificial Intelligence in peacekeeping brings many ethical challenges. Peacekeeping is based on human values like empathy, compassion and moral judgments. These qualities AI does not have. If an AI system wrongly identifies an innocent person as a threat, it can cause serious harm. AI also learns from data and if the data is biased, the system may act unfairly, going against the UN's principle of treating all sides equally.

Another major issue is privacy. AI based surveillance tools often collect personal data, photos, and online messages without people's consent. This can violate the right to privacy protection under Article 17 of the International Covenant on Civil and Political Rights (1966).

Right now,there is no single international law that clearly controls Lethal Autonomous Weapons Systems (LAWS). The UN Convention on Certain Conventional Weapons (CWW) has discussed this issue for years, but countries still disagree. The International Committee of the Red Cross (ICRC) insists that humans must always stay in charge of any system that can use deadly force and this principle is called “meaningful human control”.

To make AI safe and ethical in peacekeeping, some important steps are needed. First, AI should always have a human “in the loop”, meaning humans make the final decisions. Second, every country should check new AI or weapon systems under Article 36 of Additional Protocol I to ensure they follow international law. Third, nations should follow ethical standards like the UNESCO 2021 recommendation on the Ethics of AI, which promote fairness, transparency,and respect for human rights.

[19]https://www.icrc.org/en/document/international-humanitarian-law-and-new-weapon-technologies

4. Legal frameworks in India

(A) Constitutional framework

When the government uses surveillance or AI based monitoring in the name of national security, these actions must be measured against the Constitution, particularly Articles 14,19,21, which is often called the golden triangle of Fundamental Rights.

1. Article 14 – Equality before law and equal protection against arbitrary action[20]

State shall not deny person equality before the law or equal protection of the laws. It forms the foundation for non arbitrariness which means that every government action must be fair, reasonable and based on legal authority.

AI systems deployed in military or border surveillance must operate without discrimination. Algorithmic bias in facial recognition or patterns matching systems could violate equality if they disproportionately target specific communities or regions.

2. Article 19 – Freedom of speech and Expression

Article 19(1)(a) guarantees freedom of speech and expression, while Article 19(2) allows that government to impose "reasonable restrictions" on this right in the interest of sovereignty, integrity, or public order.

Prevalent or predictive surveillance by military intelligence agencies can suppress dissent, restrict protection, and create a "chilling effect" on free expression. The chilling effect means the discouragement of expressing oneself or engaging in a certain activity due to fear of negative consequences.

The court in Anuradha Bhasin vs Union of India (2020) [21]Emphasized that national security cannot justify indefinite restrictions on communication. In this case the Supreme Court examined the legality of the indefinite shutdown of the internet in Jammu and Kashmir following the abrogation of Article 370. The court held that the restrictions on communication and expression, even for national security, must meet the tests of legality, necessity, and

[20] Constitution of India – Article 14
[21] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637

proportionality. It ruled that indefinite suspensions are unconstitutional and all such orders must be temporary, reviewable, and published for transparency.

The judgment is highly relevant to AI based military surveillance, as it establishes security measures, including automated or predictive surveillance. They must be proportionate and subjected to oversight. The court emphasizes on transparency and periodic review means that AI systems used by the military cannot operate under unchecked executive control.

3. Article 21 – Right to privacy and liberty

The Supreme Court in K.S Puttaswamy vs Union of India (2017) [22]affirmed that privacy is intrinsic to life and liberty. Even when the surveillance is justified on grounds of security, it must satisfy the tests of legality, necessity, and proportionality. This principle is directly relevant to AI driven monitoring of citizens or military zones.

(B) Statutory Framework

1. Indian Telegraph Act 1885

Section 5(2) permits interception "in the interest of public security or national security". This provision, though central to defense communications monitoring, was never designated for algorithmic or satellite surveillance.

In PUCL vs Union of India 1997,[23] the Supreme Court demanded safeguards yet oversight remains internal and Non Judicial. In the context of military AI, this means the Armed Forces or intelligence agencies may use predictive AI tools under an outdated legal cover, without external checks. [24]

2. Information Technology Act 2000[25]

This Section 69 extends interception powers to digital communication and cyberspace. Through projects like the Central Monitoring Systems (CMS) and NATGRID, the government can control and analyze vast datasets integrating AI for threat assessments. However the system

[22] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1
[23] PUCL v. Union of India, (1997) 1 SCC 301
[24]https://student.manupatra.com/Academic/Studentmodules/Judgments/2022/Aug/MANU_SC_0149_1997.pdf
[25] Information Technology Act, 2000 – Section 69

operates without specific Legislative mandates for AI governance, leaving civil liberties exposed to unchecked algorithmic surveillance.

3. **Section 66E – Punishment for Violation of Privacy (Information Technology Act, 2000):**

This provision punishes the person who is intentionally capturing, publishing, or transmission of images of a person's private areas without consent

Modern AI-driven military surveillance systems such as drones, facial recognition cameras, and satellite imaging can automatically capture, store, and analyze images and videos of individuals, sometimes even in private or sensitive areas (like homes, border villages, or restricted zones).

Even if the intention is national security, the effect may be that personal images or biometric data are captured without consent, which is precisely what Section 66E prohibits.

4. **Digital Personal Data Protection Act 2023**[26]

The Digital Personal Data Protection Act, 2023 (DPDP Act) aims to protect personal information in the digital space.

Under Section 4, it allows processing of personal data only for a lawful purpose, and Section 6 says that such processing must be based on the free, informed, and clear consent of the person whose data is being collected.

In the context of AI-based military surveillance, this law becomes important because AI systems often collect and analyse personal or biometric data from drones, CCTV, and satellite feeds. The Act reminds that even when data is gathered for security reasons, it must be used fairly, stored safely, and limited to what is necessary.

However, the Act still does not clearly explain how consent or data protection will apply when AI is used by defence or intelligence agencies. Therefore, constitutional safeguards under Articles 14, 19, and 21 continue to play a major role in making sure that national-security

[26] Digital Personal Data Protection Act, 2023 – Government of India

measures do not override citizens' privacy and liberty.

(C) The gap in India's military- AI regulation

Unlike the U.K's Investigatory Powers Act 2016 or the U.S Foreign Intelligence Surveillance Act (FISA), India lacks a United law governing military and intelligence surveillance.

This results in

- Overlapping authorities (such as defense intelligence agency, RAW,IB) with little coordination,
- Executive dominance without judicial approval and
- Technological opacity where AI algorithms operate without transparency or audit.

Such a fragmented framework risks transforming military AI surveillance into a permanent, automated security apparatus that undermines Democratic oversight

Legal Relationship Between IT Act Section 69 and DPDP Act Sections 5 & 9

Section 69 of the Information Technology Act, 2000, which empowers the Government to lawfully intercept, monitor or decrypt digital communications in the interest of national security and public order, directly interacts with Sections 5 and 9 of the Digital Personal Data Protection Act, 2023, because any interception under Section 69 must still satisfy the DPDP Act's obligations of lawful processing, purpose limitation and deletion norms, while also falling within the statutory exemptions granted to the State for national security—thereby creating a legal balance between surveillance powers and data-protection safeguards.

5. Comparative study

5.1 United States

The United States uses a sectoral model that involves judicial authorization under the Foreign Intelligence Surveillance Act (FISA)[27] and oversight by independent review bodies such as the Privacy and Civil Liberties Oversight Board (PCLOB). The PCLOB reviews national security

[27] https://www.justice.gov/nsd-fisa

programs, releases declassified reports, and ensures compliance with the Constitution, particularly the Fourth Amendment (privacy) and First Amendment (speech).

While the U.S. does not have a comprehensive Al law, federal agencies provide guidance on Al ethics, bias, and transparency. All technologies employed in counterterrorism and military surveillance such as pattern recognition and predictive analytics are open to a limited but gradually increasing court and oversight scrutiny.

Connection to India:

The U.S. model highlights the role of judicial authorization and independent oversight in secretive programs for India's growing military use of Al (e.g., autonomous drones, border surveillance). Creating an Indian counterpart of the PCLOB with technical expertise and access to classified information would provide a way for the public to be informed and reassured without compromising the secrecy of operations.

5.2 United Kingdom

The Investigatory Powers Act 2016 (IPA) consolidates numerous laws related to surveillance and establishes a comprehensive oversight structure by the Investigatory Powers Commissioner's Office (IPCO) and Judicial Commissioners who approve and audit surveillance warrants. The system is very thorough in terms of procedures as it requires a judge's approval for the interception of data and also has very strict data-retention limits.

Although the IPA does not directly regulate Al, its technology-neutral framework allows oversight bodies to evaluate the use of new technologies, including algorithmic surveillance or biometric analysis as tools, in order to ascertain that they are proportionate and that the rights of the persons concerned as per the Human Rights Act 1998 and Article 8 of the ECHR (right to privacy) are respected.[28]

Connection to India:

India's legal framework is like a jigsaw puzzle of pieces comprising the Telegraph Act, IT Act, and executive projects like NATGRID, thus lacking the statutory coherence of the UK model.

[28] https://www.gov.uk/government/collections/investigatory-powers-bill

In case of Al-driven military surveillance, a secured consolidated national security and surveillance law based on the IPA would be able to provide the court's green light to the surveillance, specify the exact usages of data and ensure that an impartial body is in charge of auditing-all these would be the democratically elected officials' oversight powers that would be strengthened instead of the defense capabilities being weakened.

5.3 European Union[29]

The European Union augments stringent data protection under the General Data Protection Regulation (GDPR) with the upcoming EU Artificial Intelligence Act that features a risk-based classification of Al systems. For instance, the use of real-time biometric identification and predictive policing are either termed as "high-risk" or are directly prohibited.These structures highlight the human control, transparency, accountability, and monitoring of Al from development to its end-use.

National Data Protection Authorities (DPAs) are responsible for ensuring adherence to regulations and have the power to impose fines, thus, they guarantee that human rights even in case of state agencies as per the norms set by the Charter of Fundamental Rights of the EU (Articles 7 and 8) are followed.

Connection to India: On the other hand, India's Digital Personal Data Protection Act, 2023 is characterized by a series of broadly defined national security exemptions that largely dilute the rights protection aspect of the law. Transitioning to an EU-style risk-based Al framework would facilitate India in harmonizing technological deployment with privacy guarantees. In such a framework, defense applications of Al are categorized based on the possible impact on civil liberties, thus, military or surveillance Al tools would be assigned such categories accordingly. Besides, high-risk Al in the defense sector (e.g., large-scale facial recognition or predictive profiling) should be subject to compulsory inspections and human-in-the-loop decision-making in order to ensure constitutional rights under Articles 14, 19, and 21 are upheld

5.4 India

The surveillance system in India is still very much a scattered and executive which controlled function of the government, operating under laws from the colonial era and the early days of

[29] https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

the digital age the Indian Telegraph Act, 1885, Information Technology Act, 2000 (Section 69), as well as administrative frameworks like CMS (Central Monitoring System) and NATGRID. The DPDP Act, 2023 may set out privacy principles but the exemptions for national security purposes make the security of data less transparent and less accountable.

There is no legal framework concerning the use of Al in the military or for surveillance purposes which has resulted in serious issues concerning oversight, algorithmic accountability, and the right to judicial review. The lack of an independent review body and a risk-classification mechanism means that the use of Al for surveillance by the defense and intelligence agencies may lead to violations of privacy and the freedom of people without the presence of any kind of control

6. Ethical principles governing AI surveillance

AI enhances military surveillance through predictive analytics and real time monitoring but raises deep ethical concerns. The guiding principles of necessity, proportionality, transparency and accountability firsthand foundation for balancing security with liberty.

a. Necessity

The principle of necessity demands that AI surveillance must be strictly limited to legitimate and imminent security threats. As held in K.S Puttaswamy vs Union of India 2017, any restrictions on privacy must pursue a legitimate state aim and be necessary to achieve it.

In military contexts, AI based drone reconnaissance or communication intercepts at border regions may satisfy this principle when directed towards counter- terrorism or infiltration prevention. However, large scale social media monitoring or domestic sentiment analysis without individualized suspicion fails the necessity test, turning preventive defense into perpetual surveillance.

b. Proportionality

Even when necessary, surveillance must not exceed what is required to achieve its goal. The proportionality doctrine, affirmed in Anuradha Bhasin vs Union of India 2020[30], mandates that

[30]https://api.sci.gov.in/supremecourt/2019/28817/28817_2019_2_1501_19350_Judgement_10-Jan-2020.pdf

measures restricting rights be appreciated, time bound and reviewable. Applied to AI, this means data collection and algorithmic analysis should be limited to specific military operations, with automatic data deletion once the threat subsides. Continuous data retention or population wide surveillance violates proportionality by erasing the distinction between peacetime intelligence and citizens monitoring.

c. Transparency

Transparency does not mean publicly sharing defense secrets. It requires visibility within institutions and independent review processes to prevent misuse. In democratic systems, oversight helps justify the need for secrecy. Right now, India's surveillance authorizations are mainly controlled by the executive, lacking independent checks from the judiciary or parliament. Without algorithmic audits or external reviews, black-box AI systems operate without accountability.

Internationally, transparency operates through oversight bodies like the Foreign Intelligence Surveillance Court (FISC) in the U.S. and the Investigatory Powers Commissioner's Office (IPCO) in the U.K. For AI-driven military surveillance, similar models should include:

- Algorithmic transparency (explaining AI decisions)
- Periodic audits by independent technical experts
- Legislative reporting on surveillance programs

d. Accountability

Accountability ensures that AI never becomes a shield for impunity. Every AI driven action that impacts a citizen's liberty must be traceable to a human or institutional authority. This principle prevents what legal theorists call "automated constitutional violations." Military and intelligence agencies must retain a human-in-the-loop for AI decisions, ensuring that machine-generated alerts undergo human verification. Moreover, grievance redressal mechanisms and penal provisions must exist for unlawful surveillance or data misuse.

7. Civil liberties challenges in military use of AI surveillance

AI-powered military surveillance inventions have serious implications for the civil liberties of

people, which not only affect their right to privacy but also their equality, dignity, and right to fair trial.

(a) Data Privacy and Mass Surveillance

AI surveillance mechanisms require large and extensive data sources including biometric databases, wiretapping of communications, and live tracking. If this is done without any legal measures, it signifies that people are being monitored all the time without their consent. As it is the case with India's Central Monitoring System (CMS) and NATGRID[31], the merging of national data for "security" is done without the control of the judiciary. Such systems have the potential to infringe upon Article 21 (Right to Privacy) and restrict the freedom of speech as per Article 19(1)(a).

(b) Algorithmic Bias and Discrimination[32]

AI algorithms often mirror the biases of the humans that are present in the data. There have been cases where facial recognition and predictive policing tools have exhibited discriminatory error rates that, in fact, have been directed towards those that have been target groups, especially, against the marginalized ones. In the context of military operations, this may lead to the identification of certain communities or areas as "high-risk" ones, thus, putting those communities at risk of being unjustly treated and at the same time it is a violation of Article 14 (Equality before Law). Consequently, fair AI control requires bias audits and fairness testing of all military algorithms to be conducted without exception.

Section 66E of the Information Technology Act, 2000 deals with violation of privacy. It says that if any person intentionally captures, publishes, or transmits the image of another person's private area without their consent, it is a punishable offence.

Although this section was mainly meant for individual online privacy such as protecting people from misuse of photos or videos, it also connects to AI-based military surveillance. When AI-powered drones, cameras, or data systems collect and store personal images or sensitive information without permission, it can amount to a privacy breach under this law.

[31]https://www.accessnow.org/wp-content/uploads/2022/03/Joint-UPR-Submission-India-2022.pdf
[32]https://scroll.in/magazine/1001836/facial-recognition-technology-isnt-wholly-accurate-at-reading-indian-faces-find-researchers

Such actions go against the spirit of Article 21 of the Indian Constitution, which protects the right to life and personal liberty, including the right to privacy (as recognized in the Justice K.S. Puttaswamy v. Union of India, 2017 case). Therefore, even in the name of national security, surveillance technologies must follow the boundaries set by Section 66E and ensure that citizens' privacy is not violated without lawful justification.

(c) Lack of Transparency ("Black-Box Decision-Making")

Artificial intelligence technologies frequently appear to be black boxes, with explanations that are unclear even to the developers. If employed in military intelligence, this disappearance of information can disorient the committee of citizens who would otherwise challenge a wrongful classification or targeting. This act violates the principles of natural justice and deepens the breach of the constitutional guarantee to freedom from arbitrary action of the State.[33]

(d) Absence of Oversight and Accountability

Unlike the US or UK, India does not have independent bodies that oversee AI or surveillance and ensure they are conducted ethically. In case AI mistakes are made such as wrong targeting, an individual misidentification, or data misuse. There is no responsible person who can be held accountable for such errors. This institutional lacuna escalates the ethical risk level as decisions by AI that impact citizens' freedom may come without any human intervention or redress.

(e) Security-Liberty Trade-Off

Probably the longest-lived of dilemmas is the one aiming to reconcile security with liberty. AI, undoubtedly, is a powerful tool that can help in defense but it at the same time can lead to an excessive extension of power. Even though history is filled with examples of spying on the public during emergencies that have gone on permanently, genuine national security can only be achieved if it is based on public trust, transparency, and the rule of law and not on fear-based control.

8. Future Directions

To ensure a fair balance between national security and civil liberties, India should strengthen

[33] https://taxguru.in/finance/silent-observer-indias-unregulated-ai-surveillance-landscape.html

its existing legal framework to regulate the use of Artificial Intelligence in military surveillance. Provisions under the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023 can be expanded to include clear standards for transparency, human oversight, and accountability in AI-driven defense operations. Establishing an independent oversight mechanism within the existing structure would enhance public trust and prevent misuse. The Digital Personal Data Protection Act, 2023 should also narrow its broad national security exemptions and include judicial or parliamentary scrutiny. Learning from the EU Artificial Intelligence Act (2024), which excludes military and national security uses under Article 2(3), India can strengthen its current mechanisms to ensure that technological advancement in defense aligns with constitutional values and human rights.

Conclusion

AI in military surveillance is a double-edged sword. It strengthens national defense but also risks transforming democratic states into surveillance states. The only sustainable path forward is a balanced approach, where national security is pursued without sacrificing civil liberty. India's growing reliance on Artificial Intelligence in military surveillance has strengthened national defense but also exposed gaps in legal accountability and civil liberty protection. While AI enhances efficiency in border security, intelligence gathering, and counter-terrorism, its misuse, such as in the Pegasus spyware case, shows the danger of surveillance without oversight.

At present, India's framework under the IT Act 2000, Telegraph Act 1885, and DPDP Act 2023 offers only fragmented regulation. The absence of a specific law for military AI leaves issues of liability and accountability unclear. When AI systems make errors such as misidentifying civilians or breaching privacy where the state, not the machine, must remain answerable, supported by transparent review mechanisms and judicial scrutiny.

The EU AI Act (2024) provides a global benchmark for ethical AI governance, yet its exclusion of military and national security uses highlights the urgent need for comprehensive standards in this field. India can take the lead by creating an independent AI oversight authority, ensuring human control over lethal decisions, and embedding constitutional safeguards into defense technology policies.

REFERENCE

1. https://www.delhipolicygroup.org/publication/policy-briefs/pegasus-privacy-and-national-security.html

2. Al in the Indian Armed Services: An Assessment | CLAWS Journal https://share.google/zJAAJIQDj3MVvyjin

3. https://share.google/G1b0dkBDLJjaO3/MW

4. https://share.google/TVgJWKWYZlvd88FgL

5. Management & Humanities https://share.google/KGhfakxychizp7EUg

6. https://share.google/8M1al4R8SXzTzCJYh

7. https://www.nytimes.com/2021/09/10/us/kabul-drone-strike.

8. https://undocs.org/S/2021/229

9. https://share.google/8crX1nHTesONJmrvV

10.https://www.technologyreview.com/2019/04/09/136094/how-chinas-ai-surveillance-works/

11. https://main.sci.gov.in/pegasus-report-2022/

12. https://www.972mag.com/gospel-lavender-ai-israel-gaza/

13 https://peacekeeping.un.org/en/principles-of-peacekeeping

14. https://unite.un.org/digitalbluehelmets

15.https://www.icrc.org/en/document/international-humanitarian-law-and-new-weapon-technologies

17. Anuradha Bhasin v. Union of India, (2020) 3 SCC 637

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

19. PUCL v. Union of India, (1997) 1 SCC 301

20.https://student.manupatra.com/Academic/Studentmodules/Judgments/2022/Aug/MANU_SC_0149 1997.pdf

21. Information Technology Act, 2000 - Section 69

22.https://taxguru.in/finance/silent-observer-indias-unregulated-ai-surveillance-landscape.html

23. https://www.justice.gov/nsd-fisa

24. https://www.gov.uk/government/collections/investigatory-powers-bill

25. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

27. https://www.ohchr.org/sites/default/files/2022-03/UNESCO.pdf

28. https://www.accessnow.org/wp-content/uploads/2022/03/Joint-UPR-Submission-India-2022.pdf

29. https://scroll.in/magazine/1001836/facial-recognition-technology-isnt-wholly-accurate-at-readin