IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Artificial Intelligence Surveillance Technologies: A Research On The Tradeoff Between National Security And Privacy Rights

- Sakshat Mahajan, LL.M, University Institute of Legal Studies, Chandigarh University

-Dr. Shailja Thakur, Assistant Professor, University Institute of Legal Studies, Chandigarh University

ABSTRACT

The blistering evolution of Artificial Intelligence (AI) has already reshaped the history of surveillance with the unparalleled opportunities in data analysis, pattern recognition, and foresight surveillance. The use of AI-based systems is growing among governments and security agencies to ensure national security, prevent terrorism, and order in the streets. Nonetheless, widespread AI application in surveillance creates important issues regarding the personal privacy of individuals, data security, and the possibility of personal data abuse. Finding the balance between the requirements of national security and the maintenance of the fundamental rights has thus become an acute legal and ethical problem. The research paper analyzes how AI plays a twofold role in improving security and at the same time being a threat to civil liberties. It examines the dangers of mass data gathering, the constitutional and human rights consequences of the surveillance, and regulatory methods that aim to introduce accountability, transparency, and reasonableness in AI technologies use. The discussion highlights the necessity to have a strong legal framework and ethical considerations to help the successful application of AI in surveillance without compromising the democratic ideals of privacy and personal freedom.

Keywords: AI, Surveillance, National security, Data Protection, Privacy rights, Human Rights, Ethical issues, Legal Frameworks, Accountability, and Transparency

1. Introduction

1.1 Background of AI in Surveillance

Artificial Intelligence has been the greatest change-maker in the evolution of modern surveillance by the way governments and institutions watch over activities and keep the order. In the past, the strategies revolved around observation and human intelligence. These days, AI systems can quickly and accurately identify threats by analyzing vast amounts of data. Many of the tools-such as facial recognition-are being put into use by governmental security agencies and police forces in the pursuit of establishing security. While the technology, if deployed well, stands to elevate the operational efficiencies, it also opens the doors to several questions regarding equality, accountability, or misuse of private information.[1]

1.2 Relevance of National Security and Privacy in the Digital Age

In the digital age, national security and privacy are both competing and complementary interests. Government authorities would always stress that prevention of terrorism, cybercrimes, and cross border threats is the goal of any surveillance undertaken by AI.[2] Safety provided by technology, however, seriously infringes on the private facts of individuals, with their privacy deemed to be the weakest. As an essential human right enshrined in international laws and constitutional provisions, this right is threatened more as the volume of data increases and, more importantly, with predictive monitoring systems becoming more pervasive.[3] The Supreme Court of India appeared to have passed the landmark judgment in which it was decided that the right to privacy is an independent fundamental right under Article 21 of the Constitution. Therefore, the fundamental challenge is finding governance models where technology can be integrated into the defense of democracy and human.[4]

2. Historical Background of Surveillance and Privacy

2.1 Initial Approaches for State Control and Surveillance:

Surveillance is vastly ancient, much comparatively to modern technology, and hence always proved to be more than just handy in governance. Like other ancient empires, both Rome and China depended on broad networks of spies and informants to keep under control so many people and were also ever vigilant against outside dangers, with institutionalized systems like wiretapping, postal inspections, and secret police, surveillance increased in the modern nation-state. The British Empire in colonial India, for instance, had set

[1] Daniel J. Solove, *Understanding Privacy*, Harvard University Press (2008), p. 109.
[2] David Lyon, *Surveillance Studies: An Overview*, Polity Press (2007), pp. 45–47.
[3] Universal Declaration of Human Rights, 1948, Art. 12; International Covenant on Civil and Political Rights, 1966, Art. 17.
[4] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

up huge intelligence networks that monitored every form of dissent and opposition activities. Such controls work very effectively for state control but do not allow for individual liberties and privacy.[5]

2.2 The Development of Privacy as a Constitutional and Human right

Modern concept on privacy came about as a result of increasing power of states and emergence of technology. The protection of the Fourth Amendment that prohibited warrantless search and seizures was the initial defense of personal liberty under the Anglo-American legislation. The 1948 Universal Declaration of Human Rights and the 1966 International Covenant on Civil and Political Rights protect people all over the world against unreasonable intrusion and is the basis on which privacy is recognized as a basic human right.[6] In the landmark case of Justice K.S. Puttaswamy (Retd.) Vs Union of India, the Supreme Court of India has held privacy as a constitutionally guaranteed right, as it is an indispensable element of dignity, personal autonomy, and individual liberty.

2.3 Rise of AI as a Non-Transformative Surveillance Technology

One change in the 21st century is the introduction of AI to surveillance systems. The artificial intelligence powered tools are capable of doing things impossible with the oldfashioned approaches such as seeking patterns, manipulating large volumes of data and predictions. At this point these technologies are more commonly applied to facial recognition, biometric authentication and predictive policing. Governments rely on such systems in combating threats such as terrorism and cybercrime yet the same technologies have people concerned with the loss of their civil liberties, mass surveillance and misuse of data. According to researchers, AI-enabled surveillance might turn invasive surveillance into a normal practice and damage democratic principles unless stringent barriers are established.[7]

3. Acknowledging AI in the Surveillance Context

3.1 Interpretation of AI-Powered Surveillance:

Surveillance powered by Artificial Intelligence refers to the scenario in which computers employ machine learning algorithms, neutral networks, and systems of automated decision-making to monitor, analyze, and make guesses about the behavior of individuals. Unlike the past, where traditional surveillance methods are

[5] Christopher Bayly, *Empire and Information: Intelligence Gathering and Social Communication in India, 1780–1870*, Cambridge University Press (1996), p. 214.

[6] Universal Declaration of Human Rights, 1948, Art. 12; International Covenant on Civil and Political Rights, 1966, Art. 17.
[7] Andrew Guthrie Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, NYU Press (2017), pp. 45–50.

largely observational and reactive, AI-based systems are proactive and predictive and can process large volumes of data in real-time. The applications of AI surveillance are in counterterrorism and city governance, border security and law enforcement. Although it is often purchased at the cost of personal privacy and freedom, its distinctiveness is the ability to make the surveillance processes more automated and reduce the number of human errors and enhance efficiency.[8]

3.2 Important technologies include biometric data analytics, predictive policing, and facial recognition:

One of the most common AI surveillance tools in use is the facial recognition technology. It maps out unique biometric features in order to assist in determining individuals in both a society and intimate context. On the same note, predictive policing involves machine learning and data analytics to determine areas or individuals that are more prone to crime. Another variable that should be considered is biometric data analytics that include voice, iris, and fingerprint recognition technologies. Although all these developments offer governments truly remarkable surveillance capabilities, it also brings up crucial concerns about the reliability, the bias of algorithms, and the tendency towards abuse that happens to marginalized groups at a disproportional rate.

3.3 A Brief Comparison of Authoritarian and Democratic Surveillance:

The purpose of AI in surveillance is hugely different in terms of the kind of political system that is present. These surveillance activities are usually justified in democratic nations as necessary in national security, crime prevention, and the security of the people. They are, however, typically supposed to comply with constitutional rights, pass through judicial scrutiny, and be guided by the principle of proportionality. On the other hand, totalitarian regimes are more likely to use AI-powered surveillance to tighten control over their authority, introduce social scoring, and suppress dissent. In comparison, authoritarian governments also often use AI-driven surveillance to consolidate political authority, impose the social scoring system, and crackdown on dissent. A Social Credit System, like that in China, is an example of using AI based monitoring to check the behavior of its citizens, where surveillance is directly connected to receiving government services. Whereas democracies underline the impact of the security versus the privacy, authoritarian regimes normalize the mass surveillance, thus posing basic difference in the significance of surveillance in society.[9]

[8] David Lyon, *Surveillance After Snowden*, Polity Press (2015), pp. 21–24.
[9] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

4. Literature Review

1. Artificial Intelligence as an Instrument to Improve National Security:

The impacts of AI as a force multiplier to the national security have been widely covered in literature. Through machine learning and data analytics, security agencies are able to quickly sort through massive amounts of data to identify suspicious patterns and threaten others faster than otherwise possible through traditional approaches. Such are fair illustrations of efficiency benefits that have been handed by these applications- proactive state resource planning and deployment- cyber defense systems, biometric border control systems, and predictive policing. These facilities when developed in a manner that presents the public interests will promote the safety of the people as well as curbing crime by means of evidence based policing and pre-emptive measures.[10]

2. Invasion of Privacy and Surveillance on a Massive Scale.

After the advantages, there are opponents who present the threats of mass surveillance supported by AI. Lacking the need to follow a person 24/7, 7 days a week, AI systems are able to provide detailed profiles of movement, association, and behavior, in contrast to the previous methods of surveillance. This led to the issue of the surveillance society where people are self-disciplined and they are constantly monitored. Literature reveals inaccuracy drawbacks with facial recognition and biometric technology with disparate errors warranting women and minorities, thereby introducing discriminatory outcomes in law enforcement. The legal academia also notes that the majority of privacy and data-protection systems lack the capacity to manage massive automated profiling, therefore creating massive loopholes in responsibility.[11]

3. Accountability, Ethics and Proportionality.

The doctrines permit constitutionality principles and ethics in order to settle these contentions. The two principles of proportionality and necessity say that the surveillance mechanism applied must encroach on the rights only in cases when there is a narrowly limited purpose on doing so that refers to valid state interests. Other mechanisms suggested by scholars to achieve accountability include impact assessment, judiciary oversight, and algorithm audits among others. Ethical frameworks emphasize the importance of transparency, fairness, and respect of human dignity implying that democratic states have to embrace stronger governance structures before entirely accepting AI based surveillance.[12]

[10] Karen Yeung, "Regulating AI for Security," *Law & Policy* (2020), pp. 3–18
[11] Kuner et al., "Machine Learning with Personal Data," *International Data Privacy Law* (2020).
[12] Virginia Dignum, *Responsible Artificial Intelligence*, Springer (2019).

5. Consequences of AI's for Privacy Rights and National Security

5.1 Beneficial Improvements: Crime Prevention, Terrorism Control, Cybersecurity, and Public Safety:

Artificial intelligence can be revolutionary in the field of national security. AI based predictive policing tools can help law enforcement organizations better allocate their resources and are able to detect potential crime hotspots. Counterterrorism applies data analytics and machine learning to aid in the recognition of extremist activity networks by analyzing online behavior patterns and communication.[13] The other application of AI in improving cybersecurity is in the case of anomaly detection systems, which assist governments and other stakeholders to react promptly to cyberattacks and protect critical infrastructure. Additionally, AI technologies are involved in the wider effort to manage population safety such as crowd management and traffic control to disaster-response infrastructures and enhance the general security and resiliency in society.[14]

5.2 Negative Implications: Mass Data Collection, Abuse of Personal Data and Chilling Effects on Freedoms:

Although AI monitoring is associated with valuable advantages, some professionals caution that it is dangerous. Collecting data on a big scale enables the creation of elaborate personal profiles, leading to the risk of entering the realms of overdoing, and using them in the wrong way. In the absence of a sound supervision, the data can be manipulated into their hands to serve political interests, center of businesses so that they can earn more profit or to serve up discriminating outcomes. The failure, wrong use and lack of transparency in the operations of the algorithms put a person at risk of being deprived of their freedom of choice, as well as their confidence in institutions is undermined.[15]

5.3 The Crisis of Tradeoffs between the Common Good and the Sovereign Self:

The conflicting nature of AI in surveillance is an unabated issue that allows the fulfillment of the good side of AI to safe the people and also preserve the human rights intact. Partisans argue that the government really does owe a moral duty to defend the citizens against emerging threats, and since the surveillance without restraint will, in fact, empower the tyranny, even in the democratic world. This has resulted in these legal norms including necessity, proportionality, and reasonableness to be no longer an abstract conception but a measure of the legality of AI based surveillance activities.[16] The objective is to develop

[13] Karen Yeung, "Regulating AI for Security: The Promise and Perils of Automated Analysis," *Law & Policy* (2020), pp. 7–9.
[14] National Academies of Sciences, *Artificial Intelligence and National Security* (2019), p. 32.
[15] Kuner et al., "Machine Learning with Personal Data: Is Data Protection Law Up to the Task?" *International Data Privacy Law* (2020), pp. 112–115.
[16] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

governance, oversight, and legal systems that find a balance between the protection of privacy, dignity, and liberty and the concerns of collective security and not necessarily ban AI.[17]

6. Ethical and Legal Challenges in Surveillance Technologies

1. Discrimination and Algorithmic Bias:

Most AI-based surveillance systems like facial recognition systems tend to be biased in the results of their work due to the composition of the datasets they are trained on. Research also indicates that such technologies may experience more difficulty in determining the characteristics of dark-skinned women compared to light-skinned males. As a result, a chain of negative social consequences may develop where there is a possibility of the subjects involved being mishandled or given discriminative outcomes. The bias contains among others, concerns which are of great concern that border ethics and the law framework touching against equality and nondiscrimination.[18]

2. Necessity and Proportionality in the restrictions of fundamental Rights

In Justice K.S Puttaswamy (Retd.) V. Union of India, the Supreme Court of India restated that privacy is the basic right as enshrined in Articles 14, 19 and 21 of the Constitution. The Court clarified that when the state intrudes into a person privacy, it should do so in accordance to the legality, necessity and proportionality rules. This implies that surveillance must be applied when really necessary, made as minimal as possible and effectively monitored.[19]

3. Moral Issues: Transparency, Fairness and Accountability.

To implement surveillance technologies in an ethical way:

1. **Transparency**: The participants should be educated on the data gathered, its use and goal.
2. **Fairness**: Surveillance must be practiced without discrimination and equal treatment of all the people.
3. **Accountability**: This should have measures of holding authorities accountable in case of misuse such as through independent audits and remedies are available.[20]

[17] Virginia Dignum, *Responsible Artificial Intelligence: Designing AI for Human Values*, Springer (2019), pp. 44–49.
[18] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proc. of Machine Learning Research 1 (2018), https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.
[19] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[20] United Nations, *Report of the Special Rapporteur on the Right to Privacy*, A/74/431 (2019),

7. Regulatory and Legal Frameworks

7.1 Indian Context

The historic decision of Justice K.S. Puttaswamy (Retd.), in India declared privacy as an essential right in Articles 14, 19, and 21 of the constitution. v. Union of India (2017). This decision set the principles of legality, necessity, and proportionality that should be used in regulating surveillance and the accumulation of personal data. Moreover, personal data protection Act of 2019 (later to be implemented in full) tries to control the process of data collection, storage and usage of personal data by states and non-governmental organizations, whereas the information technology act of 2000 provides the legal framework of electronic administration and cybercrime.[21]

7.2 International Frameworks

Countries across the globe have had different regulatory approaches to AI and surveillance. The European Union proposed AI Act (2021) introduces a risk-based operator of AI usage that presents such specifications as accountability, transparency, and human oversight. On the same note, data controllers have high standards of obligations under the general data protection regulation (GDPR) particularly in terms of user consent, data minimization, as well as the rights of individuals to access or erase their details. The Fourth Amendment prohibition on unwarranted searches and seizures in the US has been influencing the legal perception of government surveillance.[22]

7.3 Human Rights Standards

The international human rights institutions are also instrumental in the formulation of the ethical and legal standards of surveillance. Both the Guidelines of the United Nations on the Right to Privacy in the Digital Age and the OECD AI Principles focus on the need to embrace fairness, accountability, transparency, and proportionality when applying AI and other data-driven technologies.[23] These norms strengthen the duty of the states and other non-state actors to observe privacy, avoid discrimination, and make sure that the technological interventions do not contradict the basic human rights.

[21] The Personal Data Protection Act, 2019, No. 38, Acts of Parliament, 2019; Information Technology Act, 2000, No. 21, Acts of Parliament, 2000.

[22] U.S. Const. amend. IV; see *Katz v. United States*, 389 U.S. 347 (1967).

[23] United Nations, *Report of the Special Rapporteur on the Right to Privacy*, A/74/431 (2019); OECD, *Recommendation on Artificial Intelligence* (2019), https://www.oecd.org/going-digital/ai/principles/.

8. Case Studies

8.1 India: Privacy and Surveillance The Aadhaar Problems:

The Aadhaar program is the largest biometric identification system in the world and initiated by the Indian authorities and covers over a billion people. Although it has relieved service delivery and distributed social schemes, acute privacy concerns have been highlighted to do with the centralization of the data storage facility of sensitive biometric and demographic data. The case involving Justice K.S. Puttaswamy (Retd.) alleged by the Supreme Court. v. Union of India (2017) decreed that any gathering and usage of personal data should be carried out in harmony with the customary rules of legality, requirement and proportions, a deduction that has impacted the ongoing discussion regarding the privacy-related issues of Aadhaar.[24]

8.2 China: Artificial Intelligence-Powered Social Credit System and Mass Surveillance.

The social credit system of China is a complex of financial, social and behavioral records that define the reliability of the citizens of the country and restricts the access of the citizens to certain services and movement. Combined with the technology of AI based surveillance, it causes concern around the world of authoritarian control, the mass assembly of information and individual rights. Those who are against it argue that there are ethical and human rights concerns due to the absence of transparency and accountability.[25]

8.3 Control and Discovering a Compromise between Privacy and Security in the U.S. and EU

Based on the rulings such as Katz v. The Fourth Amendment of the US (1967) has been known as the supervision of the judicial review that limits the arbitrary search and prevents government intrusion into the privacy of the citizen. Conversely, to ensure that the implementation of security and AI does not violate the individual privacy rights, but does not harm the safety of the population, the European Union has begun to develop comprehensive regulatory frameworks such as the General Data Protection Regulation (GDPR) and has even suggested the AI Act. These examples demonstrate some different, yet similar approaches to finding a balance between the needs of the security and the truth of privacy and human rights.

[24] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[25] Cong Cao, *China's Social Credit System: A Big Data Governance Approach*, 15 (2020), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3528325.

9. Discussion: The National Security and Privacy Rights:

The continued use of AI and surveillance technology as a means to ensure national security poses serious concerns on the safeguarding of the personal privacy of individuals. A balance between civil liberties and state security demands is an effective way to govern the people.

10. Courts and autonomous regulating agencies

10.1 Proportionality, Accountability and Transparency Models:

The key principles of legitimizing surveillance interventions revolve around principles of proportionality, accountability, and transparency. Proportionality entails that the state should not violate privacy without a good reason, which is to attain security goals. Accountability safeguards such as audits, reporting requirements and penalties against abuse hold the government authorities accountable. Transparency, as a result of openness of surveillance policies and data use, builds trust and allows citizens to participate in the governing process with information.[26]

10.2 Guarantees of Democratic Validity:

In order to maintain democratic legitimacy, procedural and substantive safeguards must be provided with surveillance practices. These include:

• Unambiguous legal requirements and boundaries to data gathering and processing.

• There must be independent redress and review of individuals subjected to surveillance.

• Biannual evaluation of technological instruments of prejudice, discrimination, and efficacy.

• Community participation and policy formulation to guarantee attainment of agreement with the societal values.

With these mechanisms combined, states will be able to balance national security demands and individual rights protection without sacrificing either the security of the population or democratic accountability.

[26] United Nations, *Report of the Special Rapporteur on the Right to Privacy*, A/74/431 (2019), https://undocs.org/en/A/74/431.

11. Methodology

This research paper takes the form of a doctrinal research approach whereby the researcher studies legal texts, such as provisions in the constitution, enactment of laws and decisions of the courts. The doctrinal approach enables one to examine legal principles, rights, and obligations in a more in-depth way to enable a conceptual insight into the legal framework that regulates AI and surveillance technologies.

Regulatory frameworks in different jurisdictions, such as India, European Union, the United States, and China are studied with a comparative legal analysis. Such an approach can be used in order to outline the best practices, the disparities in the legal standards and the techniques of addressing the conflict between the needs of national security and the right to protect the privacy.

Case studies also constitute an important component of the methodology, and allow conducting the practical analysis of the real-life examples, including the Aadhaar system in India, the system of social credit and mass surveillance in China, and the regulation in the EU and the U.S. These researches provide practical knowledge, emphasizing the practical issues, moral issues and the efficiency of legal protection in various settings.

Through a mixture of doctrinal research, comparative and case-study analysis, this work is aimed at offering a comprehensive insight into the legal, ethical, and regulatory landscape of AI driven surveillance, as well as providing recommendations of how to balance the security requirements with privacy concerns.

12. Findings and Analysis

12.1 Significant Conflicts Between Security and Privacy Rights:

There is a basic conflict that is recognized in the study between the responsibility of the state to provide national security and safeguard the privacy of individuals. The capabilities of AI-powered surveillance technology can increase security because they allow predictive policing, threat detection, and oversee sensitive regions. Nonetheless, their implementation usually implies the potential abuse of privacy, freedom of expression and other fundamental rights due to mass data gathering and constant surveillance.[27]

[27]United Nations, *Report of the Special Rapporteur on the Right to Privacy*, A/74/431 (2019), https://undocs.org/en/A/74/431.

12.2 Review of Existing Legal and Regulatory strategies:

The Indian legal framework, i.e. the Personal Data Protection Act, 2019, and judicial control in the aftermath of K.S. Puttaswamy v. Union of India (2017), provides the principles of necessity, proportionality and accountability. On the global scale, the GDPR of the EU and the proposed AI Act offer sufficient data protection, risk management, and compliance mechanisms, whereas U.S. Fourth Amendment law restricts excessive governmental encroachment. Even though these frameworks offer the necessary protection, they have some variation in their scope, enforcement, and scalability to fast-changing AI technologies.

13. Implementation Gaps and Problems.

Although legal and regulatory frameworks are provided there are several loopholes:

1. **Implementation gap**: One of the weaknesses that are common in the implementation of privacy protection is the lack of clearly defined procedural guidelines in the deployment of AI and the lack of monitoring systems.

2**. Technological Problems**: AI systems are either biased in their algorithm, they are not visible, or they are black boxes, thus they are hard to hold responsible and oversee.

3. **Cross-jurisdictional issue in transnational data flows and surveillance practices cross-border issues in data movement and surveillance can make it challenging to secure privacy in cross-national data flows and surveillance**: The legal norms in different countries can vary, thereby complicating the protection of privacy in the process of cross-border data flow and surveillance.

In order to address such loopholes, the need to refine the legislation is not only necessary, but also the inclusion of ethical issues, judicial checks and balances and accountability mechanisms are needed to ensure that surveillance technologies are employed in driving the security objectives that are achieved without compromising the fundamental rights.

14. <u>Future Ways and Suggestions</u>

14.1 Structural frameworks for Ethical AI Governance Suggestions:

To have safe use of AI in surveillance, elaborated systems of ethical governance should be developed. They must inculcate openness, equitability, responsibility and anthropocentrism. The bias and abuse of AI

systems could be contained through periodic audits, algorithmic impact audit and public reporting systems.[28]

14.2 Improving the Judicial Control and Autonomous regulation:

Judicial control and independent regulatory bodies should be strengthened to assist in ensuring a proper check is placed on surveillance practices is put in place. It is recommended that courts should continue with the use of the tests of legality, necessity, and proportionality and the application of the ethical and legal norms can be managed by the independent regulators, such as the data protection authority. The mechanisms of public complaints, redress and independent audits assure accountability.[29]

14.3 Social Policy Advice to the Security Rights Tradeoff:

The balance between national security requirements and the fundamental rights in democratic societies are supposed to be made by the policy interventions. Recommendations include:

1. **Surveillance Risk Based**: AI surveillance is to be adopted based on the level of security risk.
2. **Minimization of Data:** Data that is collecting should only be collected and retention and deletion policies established.
3. **International Cooperation**: Development plan international regulatory measures to regulate cross-border information flow and artificial intelligence implementations.
4. **Public Participation**: Work towards being transparent and involve the people in such a way that the governance legitimacy is enhanced and foster trust in the government.[30]

These strategies will ensure that governments can strike the right balance between the requirement of being secure as a nation and the requirement of safeguarding the privacy in a sustainable way where surveillance technologies will not only make the citizens safe and secure but also protect their privacy without undermining democracy.

15. Conclusion

The rapid development of AI-controlled surveillance technologies provides the essential need to protect the interests of national security against the protection of personal privacy rights and privileges. Although these technologies have demonstrated immense advantages in the field of crime prevention, threat detection

[28] OECD, *Recommendation on Artificial Intelligence* (2019), https://www.oecd.org/going-digital/ai/principles/
[29] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1; United Nations, *Report of the Special Rapporteur on the Right to Privacy*, A/74/431 (2019), https://undocs.org/en/A/74/431.
[30] European Commission, *Proposal for an AI Act*, COM(2021) 206 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206.

and ensuring the safety of the population, their use should be informed by the principles of legality, necessity and proportionality to avoid excessive violation of personal freedoms.

Democratic protections such as the judiciary, regulatory bodies and accountability structures by the people are necessary to make AI usage responsible. Ethical governance systems with a focus on transparency, fairness and accountability offer extra lines of defense, assisting in keeping the people on board and protecting human rights of technologically advanced societies.

Finally, to reach the point of sustainable security-privacy balance is a complex task that demands both effective legal and regulatory frameworks and constant review of technological instruments, compliance with global human rights norms, and participation of citizens. This practice will make AI-based surveillance to play a role in the safety of society without jeopardizing the very principle of democracy.