International Journal of Advanced and Applied Sciences

Journal homepage: http://www.ijaas.in

'AI surveillance technologies and the right to privacy: a constitutional law perspective'

Jyotika [1*]

[1] *Assistant Professor, Department of UILS, Chandigarh University, Chandigarh, India*

ARTICLE INFO

Article history:
Received: 28-04-2025
Received in revised form: 21-05-2025
Accepted: 26-06-2025

Keywords:

AI surveillance, constitutional law, right to privacy, facial recognition, biometric data, civil liberties, state surveillance, digital rights, predictive policing.

ABSTRACT

The rapid proliferation of Artificial Intelligence (AI) surveillance technologies such as facial recognition, predictive policing, and biometric data collection has significantly reshaped the landscape of state surveillance. While these tools promise enhanced public security and administrative efficiency, they also raise urgent constitutional concerns regarding the right to privacy. This paper explores the legal and ethical tensions between AI-driven surveillance and privacy rights, with a specific focus on constitutional protections in democratic societies. Drawing on landmark judicial interpretations, comparative constitutional frameworks, and emerging jurisprudence, the study critically evaluates the extent to which current legal doctrines can safeguard individuals from unwarranted state intrusion. It argues that existing constitutional provisions must be reinterpreted or updated to respond to the unique challenges posed by AI, ensuring a balance between technological innovation and civil liberties.

Introduction

Although the use of AI offers enormous advantages in terms of efficiency, automation, and decision-making, there are also significant ethical and legal concerns, primarily with regard to privacy rights (Cath et al., 2018). As AI systems get more advanced, they have the ability to gather, process, and evaluate enormous volumes of personal data often without the participants' express agreement (Villaronga, Kieseberg & Li, 2018). This has sparked intense discussion about whether current legal frameworks are sufficient to safeguard basic privacy rights [1]. AI-powered techniques, including as face recognition software, algorithmic spying, and predictive policing, have created problems that violate constitutional rights, calling for a review of privacy regulations and legislation (Roberts et al., 2021).

However, by enabling widespread monitoring, data mining, and predictive analytics with no human control, AI-based technologies challenge conventional legal interpretations of privacy ideas (Adams-Prassl, 2019). Governments, businesses, and other organizations now have unprecedented access to personal data, which increases the risk of abuse, a lack of transparency, and the degradation of fundamental freedoms. It is yet unclear whether the threats posed by AI can be adequately addressed by the current constitutional safeguards or if new legal frameworks are required to strike a balance between privacy and innovation. Furthermore, various legal methods have distinct effects on AI when it comes to privacy[1].While many nations have strengthened their data privacy legislation the European Union, for example, has the GDPR others take a more laissez-faire position (Amann et al., 2020). This disparity necessitates some kind of worldwide legislative consensus about AI governance; otherwise, technological progress would trample on people's rights to their private information. Furthermore, in the era of artificial intelligence, constitutional courts play a crucial role in interpreting and upholding privacy rights. According to Latonero (2018), judicial involvement will establish accountability procedures for AI-driven choices, define the limits of privacy, and establish precedents that will influence future legislative frameworks.

It will determine how AI affects the basic right to privacy, evaluate current legal safeguards, and provide potential legislative and policy solutions for new issues. By analyzing significant court rulings, legislative advancements, and ethical issues, this research aims to add to the continuing discussion on AI regulation and constitutional protections (Safdar, Banja & Meltzer, 2020). Legal experts, legislators, and tech developers must collaborate as AI advances to guarantee that privacy is upheld as an unalienable right in the digital era [2].

Artificial Intelligence's Increasing Impact on Privacy

The rapid development of artificial intelligence (AI) in all its forms has drastically changed data collecting and processing, monitoring, and decision-making procedures[2]. Users' rights to privacy are violated by these technologies' frequent usage in automated decision-making, face recognition, and predictive analytics without their express authorization (Greenstein, 2022).In light of these developments, it is necessary to assess whether current legal and constitutional safeguards are sufficient to ensure that advancements in AI do not jeopardize basic rights and private privacy.

Constitutional Defense of Individual Rights in the Age of AI

According to the landmark ruling in K.S. Puttaswamy v. Union of India (2017), the right to privacy is a basic component of Article 21 of the Indian Constitution. This right is facing additional difficulties as AI-powered monitoring and automated decision-making become more prevalent. In the guise of face recognition, data profiling, and predictive analytics, mass data collecting occurs in an unregulated manner, increasing the likelihood of privacy violations [3]. These worries are replaced by more robust legislative protections that prioritize the preservation of privacy under constitutional law and control how AI affects individual liberties[3].

Resolving Privacy Concerns Associated with AI: The Need for Legislative Changes

In terms of data privacy regulations, India's Digital Personal Data Protection Act, 2023, is a tremendous step forward. However, it contains no mention of rules pertaining to artificial intelligence (AI), which raises many worries about things like mass monitoring, automated decision-making, and profiling. Regulations such as GDPR, for example, impose stricter requirements for openness and responsibility in relation to AI. In India, there is a lack of clear laws pertaining to AI, which increases the possibility of privacy violations. Complete legislative changes are necessary to ensure that AI technologies function morally and within the parameters of constitutional privacy protections in order to defend individual rights.

Due to rapid technological advancements, almost everyone today takes preserving their privacy and personal information seriously[4]. It has been observed that the idea of duty is less essential to the Indian Constitution than the idea of right, as the fundamental legal requirement of any new phenomena may first be verified by consulting the Constitution [4].

---

[1] B. C. Stahl & D. Wright, Ethics and Privacy in AI and Big Data: Implementing Responsible Research and Innovation, 16 IEEE SEC. & PRIVACY 26 (2018).
[2] C. Cath et al., Artificial Intelligence and the ‘Good Society’: The US, EU, and UK Approach, 24 SCI. & ENG’G ETHICS 505 (2018).
[3] E.F. Villaronga, P. Kieseberg & T. Li, Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten, 34 COMPUT. L. & SEC. REV. 304 (2018).
[4] H. Robertsetal., The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, and Regulation, in SPRINGER INTERNATIONAL PUBLISHING 47-79 (2021).

India is a rapidly growing nation, hence it will take longer for the legal sector to change. The Indian laws pertaining to criminal justice, national security, intellectual property, business affairs, consumer rights, privacy rights, and information rights are the primary areas of focus on the data protection issue. Some rights may be directly addressed, but due to their fundamental nature, others may be communicated via interpretative techniques. One of the most significant and noble of these is the right to privacy. It controls third parties from delving into sensitive information or private topics. Numerous international agreements, such as the "Universal Declaration of Human Rights, the Convention on the Rights of the Child, and the International Covenants on Civil and Political Rights," recognize this right[5]. The right to privacy is the most essential aspect of human life. In India, it is seen as essential to other rights like the freedom, right to life, and right to free expression.

Although everyone believes that individuals should have the right to privacy regarding their personal information, this right has not been sufficiently defined by international human rights protection mechanisms. Determining how to apply the conditional right to privacy makes it challenging to define the public interest and organize the private sector. This has made its implementation and enforcement difficult [5]. Human rights violations in the field of mass communication have drawn public attention. The "privacy of communications" hypothesis states that individuals may converse and exchange information in a setting that is protected from prying eyes from the government, corporations, and the general public. These safeguards are limited to a certain communication technology and do not cover the whole Internet.

The middle of the 20th century saw the first recognition of the right to privacy. The relevance of technology has increased as it has been more widely available. Every aspect of human existence has been impacted by technology. Modern technology is becoming more and more integrated into daily life. Calls for stricter laws governing the collection and use of personally identifiable information are sparked by the surveillance capabilities of powerful computer systems [6].

[5] J. Adams-Prassl, What If Your Boss Was an Algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at Work, 41 COMP. LAB. L. & POL'Y J. 123 (2019).

According to the rights theory, data security is an essential human right. Inspired by the necessity to safeguard people's privacy, the world's first data protection law is regarded as the forerunner of modern data protection legislation.

Cybercrimes pertaining to personal information

Nowadays, the majority of individuals have at least one social media account, and the majority of them often update it with details about their days, locations, and other activities. Social media account holders who publicly reveal this information make it easier for criminals to harm them later on, either by hacking or simply by kidnapping them once they find out where they are. Unfortunately, hacking has grown so widespread that websites run by government organizations are at risk, not to mention the social media accounts of private users! When a victim clicks on a link sent to them via email or social media, the hacker has access to the victim's computer. This is how most hacks happen. For example, we sometimes get unsolicited emails asking for our banking information in exchange for a claim that we have won a large quantity of money. This is a trap that even knowledgeable people may fall into. These types of cybercrimes are regrettably widespread. According to research, the great majority of Internet users (about 80%) have at some time been caught in the traps of these criminals [7].

Literature review

B. Murdoch (2021) [1] Murdoch investigates the intersection of artificial intelligence (AI) and health data privacy. The article underscores how AI technologies challenge traditional norms and regulations surrounding patient confidentiality. Murdoch emphasizes the inadequacy of existing data protection frameworks in addressing the scope and scale of AI-driven health data analytics. He calls for reform in legal and ethical standards to better safeguard individual privacy rights in the context of increasingly intelligent health systems. The work is critical for understanding the ethical imperatives that must accompany the technological growth in health AI.

H. Roberts et al. (2021) [2] This chapter provides an in-depth examination of China’s unique strategy toward AI development, focusing on the blend of state-driven policy, regulatory structures, and ethical considerations. Roberts et al. analyze how China's centralized governance influences AI policy, contrasting it with Western regulatory models. The work evaluates the

country's national AI development plans, data governance policies, and the role of ethics in AI governance. It also discusses how China's policies on health-related AI may raise both opportunities and concerns regarding surveillance, privacy, and individual rights. This comparative analysis is vital for contextualizing global AI governance trends.

J. Amann et al. (2020) [3] Amann and colleagues explore the critical role of explain ability in AI applications within healthcare settings. They adopt a multidisciplinary lens to examine how technical transparency, legal accountability, and ethical trust converge in the concept of explainable AI (XAI). The paper discusses the tension between performance and interpretability in machine learning models and calls for frameworks that make AI systems both powerful and understandable for clinicians and patients. The authors advocate for collaborative efforts among developers, healthcare providers, and policymakers to ensure responsible AI deployment in healthcare. This work contributes significantly to the discourse on trust and usability in health-related AI systems.

Surveill Atlas (2021) [4] Surveill Atlas, a project by the Electronic Frontier Foundation, provides an open-source framework for tracking the deployment of surveillance technologies by law enforcement across the U.S. It documents the spread of tools such as facial recognition, license plate readers, and predictive policing software. This resource emphasizes transparency and civic engagement by empowering communities to understand and monitor technological encroachments on civil liberties.

Bloch-Wehba, H. (2021) [5] Bloch-Wehba explores the paradox of technological transparency in modern policing. While police departments adopt surveillance and data technologies that increase operational visibility, these tools often evade public scrutiny due to proprietary protections and lack of oversight. The article argues for regulatory reforms to ensure democratic accountability and highlights the growing tension between public interest and technological opacity in law enforcement.

Brayne, S. (2021) [6] Sarah Brayne's book provides a comprehensive sociological analysis of how data-driven technologies are transforming policing practices. Through ethnographic research within the Los Angeles Police Department, Brayne examines how predictive analytics

and surveillance systems reshape discretion, accountability, and power in policing. The work highlights systemic implications, particularly concerning racial bias, civil liberties, and institutional trust.

Burke, G., Mendoza, M., Linderman, J., &Tarm, M. (2021) [7] This investigative report sheds light on the wrongful arrest of a man based largely on unreliable AI-powered surveillance technology. The case illustrates the real-world consequences of deploying opaque algorithms in criminal justice, particularly in contexts with minimal evidentiary standards or oversight. The article raises questions about due process, evidentiary integrity, and AI accountability in policing.

Feathers, T. (2021) [8] Feathers exposes troubling practices involving ShotSpotter, a gunshot detection AI used by police departments. The report reveals instances where law enforcement allegedly pressured the company to modify reports to align with prosecutorial narratives. This calls into question the objectivity and legal reliability of AI-generated evidence in criminal cases.

Government Accountability Office (GAO) (2021) [9] This official GAO report critiques the fragmented and uncoordinated use of facial recognition technologies by federal law enforcement agencies. It highlights gaps in oversight, tracking, and transparency, recommending that agencies improve system accountability and public reporting. The report is significant in informing federal policy debates on surveillance reform and civil liberties.

Haskins, C., Mac, R., & McDonald, L. (2020) [10] This article investigates Clearview AI, a controversial facial recognition firm known for scraping millions of images from social media platforms without consent. The ACLU's legal and ethical criticisms are central to the story, emphasizing privacy violations and the risks of surveillance capitalism. The report helped catalyze public discourse on biometric data rights and corporate surveillance practices.

Koepke, L. et al. (2020)[11] This report by Upturn details how U.S. law enforcement agencies frequently extract data from mobile phones, often without warrants. The authors highlight legal loopholes and lack of oversight that allow for mass digital surveillance. The report raises serious privacy concerns and calls for stricter controls on mobile phone searches by authorities.

Lee, D. (2021)[12] Lee reports on the rapid expansion of partnerships between Amazon's Ring and U.S. police and fire departments. The piece underscores the growing surveillance capabilities of private-sector technologies integrated with public safety systems, raising concerns over privacy, transparency, and the privatization of public surveillance infrastructure.

Lyons, K. (2021)[13] Lyons corroborates and expands on earlier reporting regarding Ring's surveillance network, examining how these partnerships impact community privacy and law enforcement oversight. The article raises ethical and legal questions around public-private surveillance and lack of community consent or input in Ring's integration with police departments.

MacArthur Justice Center (2021)[14] This press release summarizes findings that ShotSpotter, an AI-based gunshot detection tool, led to tens of thousands of ineffective police deployments. The MacArthur Justice Center critiques the technology's reliability and the burden it places on heavily surveilled communities, particularly in terms of false alarms and racial profiling.

Oliver, M. &Kugler, M.B. (2021)[15] Oliver and Kugler provide a comprehensive survey of the surveillance tools used by police departments across the U.S. The study covers facial recognition, license plate readers, drones, and more, and identifies patterns in deployment, oversight, and public transparency. Their findings highlight inconsistent regulation and the potential erosion of civil liberties.

Policing Project (2021)[16] This report evaluates ShotSpotter's effectiveness in detecting gunfire and influencing public safety outcomes in St. Louis County. The study finds limited or inconclusive results regarding its impact on crime reduction and questions the cost-effectiveness and accuracy of such surveillance technologies.

Prince, H., Lum, C., &Koper, C.S. (2021)[17] The authors synthesize research on effective investigative strategies in policing, including the use of surveillance and data technologies. While some technologies aid investigations, the study emphasizes the need for evidence-based deployment and cautions against overreliance on unproven tools that may violate rights or generate biased outcomes.

Robin, L., Peterson, B.E., & Sherman, D.S. (2020) [18] This empirical study evaluates the impact of Milwaukee's CCTV network on crime rates and case clearances. The authors find mixed results, suggesting that while cameras may aid in solving specific crimes, their deterrent effect is limited. The study raises questions about resource allocation and civil liberties in CCTV surveillance.

Slobogin, C. (2022)[19] Slobogin's book explores the legal and ethical implications of emerging surveillance technologies, focusing on the concept of "virtual searches." He proposes regulatory reforms for covert digital surveillance and argues for clearer legal standards that balance law enforcement needs with constitutional rights.

Whittaker, Z. (2021)[20] Whittaker highlights the increasing use of geofence warrants, which compel Google to provide data from all devices within a certain area. The article reveals the scale of government requests and raises significant privacy concerns about dragnet-style digital surveillance and the risk of wrongful identification.

Research methodology

The approach used in this study to examine how artificial intelligence affects the right to privacy from the perspective of constitutional law is qualitative legal research. The research primarily takes a doctrinal approach, relying more on the analytical interpretation of international privacy rules, legislative frameworks, judicial decisions, and constitutional requirements [8].

This calls for a thorough assessment of Indian legislation, particularly the planned Digital Personal Data Protection Rules, 2025, and the Digital Personal Data Protection Act, 2023, to determine whether or not they adequately address privacy issues brought on by AI. This paper examines whether India's present legislative provisions sufficiently protect individual privacy rights against the potential hazards of artificial intelligence (AI), given the technology's fast improvements and growing involvement in data processing, monitoring, and decision-making. It makes analogies to international legal systems[6], particularly the European Union's General Data Protection Regulation, to provide a correct context [9]. Setting greater requirements for data protection and ensuring AI is transparent and responsible, the General Data Protection Regulation is regarded as one of the most stringent data protection laws in the world. It

highlights India's strengths, areas that need revision under its privacy regulations, and shortcomings in the country's data governance, using the GDPR as a benchmark.

The Indian Constitution's Article 21, which acknowledges the right to privacy as a basic right, is the subject of a very pertinent controversy. It enshrines this freedom via historic court rulings, including K.S. Puttaswamy v. Union of India (2017).The legislative architecture, including the Digital Personal Data Protection Act of 2023 and the draft Digital Personal Data Protection Rules of 2025, is also critically examined for its suitability in addressing concerns about the use of AI for the collection and processing of personal data. Using a comparison method, one may comprehend international instruments, especially the General Data Protection Regulation of the European Union [10]. Additionally, this might also provide India a way to comprehend the best privacy regulations. The research also includes a report on artificial intelligence, data protection, and constitutional law, as well as an assessment of peer-reviewed academic publications and legal commentary. Thus, all potential effects of AI on privacy rights and the legal frameworks that govern these contemporary privacy issues brought about by AI.

To examine how AI affects the constitutional right to privacy, the study uses doctrinal legal analysis, which deals with analyzing statutes, court decisions, and legal texts. It rests its claims on a review of significant court rulings and legislative actions to determine whether the existing legal frameworks adequately handle the privacy problems highlighted by AI-driven technology[7]. In addition to the doctrinal study, India's privacy laws are assessed in light of foreign legal frameworks such as the GDPR using a comparative legal methodology. Such a comparison analysis is justified by the idea that it would assist in identifying areas that need revision in the regulation of privacy hazards associated with AI and legal gaps [11]. Therefore, the study will provide suggestions for enhancing India's legal approach to AI governance by drawing on ideas from international best practices. Key themes include algorithmic bias, which can result in discriminatory outcomes that affect marginalized groups; data profiling, which raises concerns about unconsented data collection and potential misuse; mass surveillance, where AI-powered facial recognition and predictive policing pose risks to individual freedoms; and regulatory challenges, which draw attention to the absence of AI-specific legal provisions in India's data protection laws. As a result, it addresses every other pertinent ethical question that comes up in connection to algorithmic discrimination, governmental monitoring, and the interplay between

individual freedom and national security. In order to prevent AI from being used as a tool to violate the constitutional framework, the paper makes the case for the need for responsible AI governance and calls for judicial monitoring. Strong legal protections for privacy in an AI-run society center on responsibility, transparency, and the ethical use of AI.

For AI systems to work well, they need a lot of personal data, including biometric data. Intimate information about people's life may be revealed via this data, which might violate their privacy if it is exploited or not sufficiently safeguarded [12].Concerns over widespread monitoring and the degradation of private rights are raised by the indiscriminate and often clandestine data collecting by AI systems, which targets almost everyone using digital devices[8]. AI applications such as remote biometric identification systems, biometric categorization systems, and emotion recognition systems are especially worrisome. In order to avoid misuse and guarantee adherence to legal requirements, the use of AI for law enforcement's real-time remote biometric identification in publicly accessible areas requires strict regulatory control of biometric data processing. Concerns about privacy are further heightened by AI's ability to extract, re-identify, connect, and act upon sensitive data, which raises the possibility of personal information being misused and made public.[9]

The ethical gathering, storing, and use of personal data by artificial intelligence systems is the focus of AI privacy practices and concerns. It addresses the urgent need to preserve confidentiality and safeguard individual data rights as AI algorithms analyze and learn from enormous amounts of personal data. In a time where data is a highly desirable commodity, ensuring AI privacy requires striking a balance between technical progress and protecting individual privacy [13].

---

[6] J. Amannetal., Explainability for Artificial Intelligence in Healthcare: A Multidisciplinary Perspective, 20BMCMED. INFORMATICS & DECISION MAKING 1 (2020).
[7] M. Latonero, Governing Artificial Intelligence: Upholding Human Rights & Dignity, 38 DATA & SOC'Y (2018).
[8] M. Perc, M. Ozer & J. Hojnik, Social and Juristic Challenges of Artificial Intelligence, 5 PALGRA VECOMMC' NS1 (2019).
[9] N. M. Safdar, J. D. Banja& C. C. Meltzer, Ethical Considerations in Artificial Intelligence,122 EUR. J. RADIOL. 108768 (2020).

The intricacy and imperceptibility of gathering data AI systems use a variety of data collecting techniques that potentially provide serious privacy problems in order to enhance their algorithms and outputs. The methods used to acquire this data are often imperceptible to the subjects of the data collection, resulting in privacy violations that are difficult to identify or manage. Because of this invisibility, people may not be aware of how their data is being used, which makes privacy protection initiatives much more difficult.

Security and Ethical Issues It is impossible to overestimate the significance of privacy in the digital age. It is an essential human right required for individual liberty, safety, and equity [9]. The ability of increasingly complex AI technology to make conclusions based on minute patterns in data that are hard for humans to detect raises serious ethical and security issues. There are concerns over accountability and transparency in AI decision-making processes as people may not be aware that their personal information is being utilized to make judgments that impact them [14].

Result Case Analysis

As artificial intelligence (AI) technologies develop, they make it possible to handle large databases without seemingly needing or requesting user agreement, which raises serious privacy rights concerns. Artificial intelligence (AI)-enabled systems like face recognition, predictive analytics, and algorithmic decision-making will lead to more data exploitation, intrusive monitoring, and constitutional rights abuses. Despite efforts to improve data security, India's current legal framework still has gaps on privacy-related problems unique to artificial intelligence, according to a comparative study of Indian and foreign legal frameworks [15]. A positive step toward regulating personal data is shown by the Digital Personal Data Protection Act of 2023 and the planned Digital Personal Data Protection Rules of 2025.However, there are no explicit rules pertaining to automated decision-making, AI-based surveillance technology, or AI governance. Rather, stringent rules governing the processing of AI-driven data are found in international legal frameworks, particularly the European Union's General Data Protection Regulation, which emphasizes the values of responsibility, transparency, and individual rights.

These results fall under other categories of concern, such as algorithmic discrimination, data profiling, mass monitoring, and regulatory issues. The research comes to the conclusion that although AI has many positive social effects, its uncontrolled use might seriously jeopardize privacy. Therefore, in order to safeguard basic privacy rights, Indian law and regulatory structure do need immediate improvement via the adoption of AI-related legislative provisions, increased judicial scrutiny for governance, and policy alignment with the best international best practices.

Risks to Privacy Raised by AI Technologies

Significant privacy problems are brought up by the integration of AI across several domains, particularly in fields like predictive analytics, data mining, automated decision-making, and surveillance. While large-scale data mining often occurs without express user agreement, facial recognition and mass surveillance systems using AI-powered apps compromise individual rights to privacy [16]. Predictive analytics jeopardizes data security and individual liberty, while AI-driven decision-making often produces discriminatory consequences. This illustrates why robust legal frameworks are required to handle the privacy dangers posed by AI technology.

Table 1: AI Privacy Concerns and Their Legal Consequences

AI Domain	Privacy Concern	Legal Implication
Surveillance	Mass surveillance via AI-powered cameras and facial recognition	Potential violation of privacy rights under Article 21
Data Mining	Large-scale personal data collection without explicit consent	Breach of consent-based privacy protections
Algorithmic Decision-Making	AI-based pro filing leading to biased outcomes	Risk of discrimination and lack of accountability
Predictive Analytics	Use of personal data for behavioral predictions	Threat to individual autonomy and data security

Comparative Evaluation of Legal Structures

The capacity of Indian and international privacy laws to address privacy issues connected to artificial intelligence is compared, revealing both its advantages and disadvantages. In this sense, the Digital Personal Data Protection Act, 2023, which was approved within the Indian legislative framework, does not specifically call for AI control. With its increased accountability, transparency, and AI-specific criteria, international regulation like the European Union's General Data Protection Regulation is in a better position. It does highlight the pressing need for India to have a more robust legislative framework that can stop any privacy violations brought on by AI technology [17].

India's AI Privacy Protection Gaps

Although it represents a significant stride in India's data privacy environment, the Digital Personal Data Protection Act, 2023, makes no mention of AI-driven data processing or automated decision-making. Because of this legal vacuum, AI-driven technologies like algorithmic profiling, predictive analytics, and large-scale data collecting are subject to questions of responsibility, transparency, and supervision. India lacks a dedicated framework for AI governance, in contrast to the European Union, and its data protection legislation is still in its infancy. From a legal standpoint, AI applications are thus essentially uncontrolled. The incorporation of AI into surveillance technology, including face recognition software and predictive policing tools, which often operate with minimal legal control, has been one of the main causes for worry. These technologies raise serious privacy breaches and ethical issues by enabling widespread monitoring without express authorization. The likelihood of abuse, prejudice, and discrimination rises when there are unclear legal protections. Therefore, comprehensive AI legislation are urgently needed in order to strike a balance between basic privacy rights and technical growth.

Table 2: Evaluation of Legal Frameworks Controlling AI and Privacy in Comparison

Legal Framework	Key Provisions	Effectiveness in Addressing AI Privacy Risks
Indian Constitution (Article 21)	Recognizes the right to privacy as part of the right to life and personal liberty	Lacks specific AI-related provisions
K.S. Puttaswamy v. Union of India (2017)	Established privacy as a fundamental right	No direct focus on AI regulations
Digital Personal Data Protection Act, 2023	Regulates data processing and mandates consent	Limited provisions on AI governance
Draft Digital Personal Data Protection Rules, 2025	Strengthens compliance mechanisms for data protection	Still in draft stage, lax enforcement clarity
General Data Protection Regulation (GDPR) – EU	Strict data privacy, AI accountability, and transparency mandates	More comprehensive compared to Indian laws

Recommendations for Regulation and Ethics

This research study suggests important ethical and legislative changes to improve AI privacy governance in India in order to reduce privacy issues associated with AI. These reforms include increased judicial and regulatory oversight to prevent the misuse of AI-based surveillance, the implementation of AI-specific legal provisions to improve oversight over data collection and automated decision-making, and the development of transparency and accountability measures to foster public trust. By doing this, the legal loopholes will be filled and India would have a strong framework that protects people's right to privacy while encouraging moral AI innovation [18]. Furthermore, this gap will be closed by bringing Indian AI laws into line with global best practices, such as the GDPR.

Criminal Obligations Applications of AI have impacted many facets of contemporary life. However, the question of whether AI poses a threat to humans has gained urgency in recent

years. In 2015, over a thousand scholarly works, including Stephen Hawking's, suggested that the destruction may have been caused by AI-warfare. In the case that AI does such harm, the question of whether such situations may be governed by laws or ethics arises. The fact that AI entities are not regarded as legal people has been identified as one of the problems. However, this dilemma has been likened to the time when corporate crime was examined (manufactured topic).It is a fact that an entity may be liable to criminal law if two necessary conditions are met: criminal intent (mensrea) (mental or internal element) and conduct constituting crime (actusreus). But in order to hold AI accountable for crimes, Gabriel Hallevy came up with three prerequisites.

AI cannot be attributed human traits. AI is not thought to have any criminal intent. The actual criminal has been found to be the one who committed the crime. The creator of the AI program or the end user might be the criminal. Regardless of whether they intended to do harm or not, the creator or end user has criminal liability for an AI program. They will always be held accountable because of their mental condition at the time of the accident. AI would be legally liable for its deeds, according to this notion. According to this theory, AI creators or end users have some of the same criminal liability. Therefore, while considering AI's criminal liability, all three eventualities need to be taken into account at the same time. It is necessary to consider the specific circumstances while evaluating the issue of culpability [19].

Table 3: Suggested Legal and Ethical Changes for India's AI Privacy Governance

Recommendation	Expected Impact
Introduction of AI-specific legal provisions	Ensures better oversight of AI-based data collection and processing
Stronger judicial and regulatory oversight	Preventsm isuse of AI in mass surveillance
Adoption of AI transparency and accountability measures	Enhances public trust and compliance with ethical standards
Alignment of Indian regulations with international best practices	Bridges the gap between domestic and global AI governance frameworks

We can surely analyze and send vast amounts of data regarding societal and individual behavior with the help of AI. AI and improved computer algorithms with machine learning capabilities can analyze and optimize sensory data, such as a person's voice recordings, photographs of their face, vital signs, and DNA, more quickly and effectively than humans. Despite the serious privacy and security issues involved with AI, nations and governments are investing in the development of this technology, which will affect our DNA, looks, money, emotions, and surroundings. AI technology is now widely accessible and has impacted almost every aspect of contemporary life. AI may sometimes retrieve data without our knowledge or consent. The privacy of the person is therefore jeopardized when the information is sold to marketers.

Despite AI's advantages in speed and efficiency, concerns around data privacy are becoming more prevalent. Without the development of advanced machine-learning algorithms that can predict user behavior, products like Google Maps and Alexa would not be feasible. In contrast, they need vast amounts of experimental and real-world data on people's experiences, perceptions, and interactions that is, personal data in order to achieve deep learning [20].The growing conflict between AI's need for and use of vast amounts of personal data to train machine learning algorithms has highlighted the value of personal data as a protected commodity under recent US privacy laws like the "California's Consumer Privacy Act" (CCPA) and Illinois's "Biometric Information Privacy Act" (BIPA), as well as older privacy statutes like the "Health Insurance Portability and Accountability Act of 1996" (HIPAA). The alleged illegal use of personal data is often justified by goals like enhancing the ability of medical experts to predict future clinical events for particular patients or resolving discriminatory "bias" in machine learning algorithms.

Conclusion

AI surveillance technologies present both transformative opportunities and profound constitutional challenges. While they offer tools for enhancing national security, law enforcement, and public administration, their unchecked deployment risks eroding fundamental rights most notably, the right to privacy. From a constitutional law perspective, the integration of AI into surveillance practices demands a reexamination of existing legal doctrines to ensure they remain robust in the face of evolving technological capabilities. Courts and legislatures must respond proactively by developing clear legal standards for the use of AI in surveillance,

ensuring transparency, accountability, and proportionality. Constitutional protections must not only address traditional forms of intrusion but also anticipate the nuanced and often invisible ways AI can infringe on personal autonomy, dignity, and freedom. A rights-based, constitutional framework is essential to prevent the normalization of mass surveillance and to safeguard democratic values in the digital age. Ultimately, the legitimacy of AI surveillance hinges on maintaining a careful balance: leveraging technology for public good while reinforcing constitutional guarantees that protect individuals from arbitrary and disproportionate state power.

Reference

1. B. Murdoch, Privacy and Artificial Intelligence: Challenges for Protecting Health Information in a New Era, 22 BMC MED. ETHICS 1 (2021).
2. H. Roberts et al., The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, and Regulation, in SPRINGER INTERNATIONAL PUBLISHING 47-79 (2021).
3. J. Amann et al., Explainability for Artificial Intelligence in Healthcare: A Multidisciplinary Perspective, 20 BMC MED. INFORMATICS & DECISION MAKING 1 (2020)
4. Surveill Atlas. 2021. Documenting police tech in our communities with open source research. Electronic Frontier Foundation.
5. Bloch-Wehba H. 2021. Visible policing: technology, transparency, and democratic control. Calif. Law Rev. 109:917–78
6. Brayne S. 2021. Predict and Surveil: Data, Discretion, and the Future of Policing. New York: Oxford Univ. Press
7. Burke G, Mendoza M, Linderman J, Tarm M. 2021. How AI-powered tech landed man in jail with scant evidence. Associated Press, Aug. 19.
8. Feathers T. 2021. Police are telling ShotSpotter to alter evidence from gunshot-detecting AI. Vice, July 26.
9. Gov. Account. Off. (GAO).2021.Facial recognition technology: federal law enforcement agencies should have better awareness of systems use. GAO, July 13.
10. Haskins C, Mac R, McDonald L. 2020. The ACLU slammed a facial recognition company that scrapes photos from Instagram and Facebook. BuzzFeedNews, Febr. 10.

11. Koepke L, Weil E, Janardan U, Dada T, Yu H.2020.Mass extraction: the widespread power of U.S. law enforcement to search mobile phones. Rep., Upturn, Washington, DC.

12. Lee D. 2021. US police and fire departments partnering with Amazon's Ring passes 2,000. Financial Times, Jan. 29.

13. Lyons K. 2021. Amazon's Ring now reportedly partners with more than 2,000 US police and fire departments. The Verge, Jan. 31.

14. Mac Arthur Justice Center. 2021. ShotSpotter generated over 40,000 dead-end police deployments in Chicago in 21 months, according to new study. Press Release, May 3.

15. Oliver M, Kugler MB. 2021. Surveying surveillance: a national study of police department surveillance technologies. SSRN Work. Pap. 3911442. 10.2139/ssrn.3911442

16. Polic. Proj. 2021. Measuring the effects of ShotSpotter on gunfire in St. Louis County, MO. Rep., Polic. Proj., New York.

17. Prince H, Lum C, Koper CS. 2021. Effective police investigative practices: an evidence-based assessment of the research. Polic. Int. J. 44(4):683–707

18. Robin L, Peterson BE, Sherman DS. 2020. How do close-circuit television cameras impact crimes and clearances? An evaluation of the Milwaukee Police Department's public surveillance system. Police Pract. Res. 22(2):1171–90

19. Slobogin C. 2022. Virtual Searches: Regulating the Covert World of Technological Policing. Cambridge, UK: Cambridge Univ. Press

20. Whittaker Z. 2021. Google says geofence warrants make up one-quarter of all U.S. demands. TechCrunch, Aug. 8.