INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 5 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

THE FUTURE OF PRIVACY: IS SURVEILLANCE LAW TECHNOLOGY? PROTECTING INDIVIDUAL PRIVACY

AUTHOR - SHREYA PANDEY* & DR. SHOVA DEVI**

* STUDENT AT AMITY LAW SCHOOL, AMITY UNIVERSITY

** PROFESSOR AT AMITY LAW SCHOOL, AMITY UNIVERSITY

BEST CITATION - SHREYA PANDEY* & DR. SHOVA DEVI, THE FUTURE OF PRIVACY: IS SURVEILLANCE LAW TECHNOLOGY? PROTECTING INDIVIDUAL PRIVACY, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 5 (5) OF 2025, PG. 806-813, APIS – 3920 – 0001 & ISSN - 2583-2344

ABSTRACT

This article critically examines whether current legal frames adapt to rapid advances in digital surveillance technologies such as artificial intelligence, biometric authentication, and the Internet of Things (IOT). The study is based on global regulatory models such as the GDPR and CCPA, and examines the growing gap between legislative reform and technological innovation. We examine the legal and ethical implications of mass surveillance, algorithmic monitoring, and data control profiling to assess the extent to which individuals' rights are protected in the digital age. Through case studies and comparative analysis, this paper highlights the need for proactive legal reform and international cooperation to create an adaptive and responsible monitoring framework with a focus on privacy. The investigation concludes that without timely and future-oriented intervention, the imbalance between state surveillance capabilities and individual freedoms could significantly undermine our legal rights to future privacy.

1. Introduction

In an increasingly digital world, the concept of privacy is undergoing major changes. Privacy is no longer confined to physical realms, and is now extended to virtual spaces, with personal data being constantly collected, stored and analysed by state and private actors. At the heart of this digital expansion is a key concern as to whether existing surveillance laws respond to the rapidly developing technological landscape. These tools improve national security and management efficiency, but also raise urgent questions about individual autonomy, data security, and rights to be neglected. Traditional legal framework conditions, which are often more responsive than aggressive, are more difficult to respond to these challenges and create regulatory gaps between innovation and protection. To assess the response to technological change, we will examine the adequacy of global data protection laws, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), along with national laws in India. Comparative case studies and legal analysis seek to highlight key issues and propose reforms to the more robust future monitoring framework.

2. Development of surveillance and data protection laws

The legal perception of privacy as a fundamental right has evolved significantly over the past century. Traditionally rooted in the principle of physical and territorial integrity, data protection laws were originally intended to protect individuals from any national interference. However, with the advent of the digital age, privacy has expanded to include information protection rights. The right to

control the collection, use and distribution of personal data. Warren and Louis d. Title Right to Privacy Right to Privacy Brandeis speaks for legal protection against unauthorized publications of Private Fact. Over time, the idea has evolved into constitutional and legal protections in various countries. Puttaswamy (Retd.) V. Union of India (2017), Article 21 of the Constitution, the Supreme Court bench with nine judges is essentially about life and individual freedom. The European Union's General Data Protection Regulation (GDPR) of 2018 set a global benchmark for data protection protection, with principles such as data protection, restrictions on purpose, and right to delete. Additionally, strict declarations of consent and substantial penalties for non-integration have been decided.

The CCPA (California Consumer Privacy Act) issued in 2020 reflects many of the GDPR principles, but emphasizes consumer rights in a market-oriented environment. Give California the right to know which data is collected to avoid sales and apply for deletion. Act Information Technology Act 2000 offers limited protection measures in accordance with Sections 43A and 72A, but a comprehensive data protection law is still anticipated. Digital Personal Data Protection, 2023 Acts. However, one step was criticized for giving exceptions to the state and lacking a strong enforcement mechanism. In India, the The Telegraph Act, 1885 and Information Technology Rules (Digital Media Mediation Guidelines and Ethics Code), 2021 rule oversight practices, but there are no independent supervision. In the United States, programs such as prism and legal provisions as part of the foreign intelligence (FISA) surveillance laws provide mass surveillance with minimal transparency. The lack of adaptive and comprehensive legal safeguards left a significant gap in privacy protection in the context of surveillance.

The digital revolution has created multiple complex surveillance technologies that collect, analyze and use personal data in real time. These products are often justified in the name of national security, urban planning, or public health, but are threatened by individual privacy. As surveillance becomes increasingly an umbrella, the challenge is to enable the conditions of the legal framework to address the risks of these rapid development technologies.

3. New Surveillance Technology

The digital revolution has resulted in many complex surveillance technologies that collect, analyze and use personal data in real time. These products are often justified in the name of national security, urban planning, or public health, but are threatened by individual privacy. As surveillance is increasingly intrusive, the challenge is to enable the terms of the legal framework to improve the risks of these rapidly developed technologies. Algorithms can process large amounts of data to identify and suspect patterns. However, these systems work without transparency and are susceptible to distortion embedded in training data, leading to targeting marginalized communities. Despite its potential efficiency, AI-controlled surveillance raises important concerns about proper procedures, accountability and discrimination. In particular, facial recognition technology (FRT) was used in public spaces, airports and law enforcement agencies. In India, the implementation of the Aadhaar system, which collects fingerprints, iris scans and facial data, sparked debate over consent, data abuse and elimination. These devices often passively collect personal data and transfer it to remote servers without the user's explicit recognition or control. If this data is aggregated, such data can indicate intimate patterns, overviews, and risks of behavioral manipulation regarding the individual's life.

Big -data often analyzes and broker the marketing of personal data by data brokers without consent. It often undermines privacy and strengthens power trauma between individuals and institutions. In the surveillance context, big data analysis allows for the construction of detailed digital profiles that can

be misused or injured. These tools can access encrypted messages, turn on camera and microphones, and extract sensitive data without user knowledge. Such software's confidential provisions undermine the rule of law and democratic accountability.

These technologies also offer management and security benefits, providing substantial data protection risks. Legal systems need to address not only the technical skills of these tools, but also the socially legitimate meaning.

4. Gap in existing surveillance laws

Despite the widespread data protection laws and data protection laws, most surveillance laws are outdated, unfragmented and underequipped to respond to the complexity and degree of modern surveillance technology. These gaps create legal gaps where individual rights are not adequately protected, and state or business surveillance is often not checked. Static legal definitions and close interpretations of data or data protection do not include the nature of the developmental nature of personal information or digital IDs. For example, the 2000 Indian Information Technology Act is a widespread social media and intelligent technology that does not properly address monitoring through algorithms and automation. However, in many jurisdictions, surveillance activities are subject to enforcement agencies with little or no independent supervision. In India, intercepting according to the Telegraph Act or monitoring according to IT regulations can occur without judicial sanctions or parliamentary exams, which raises concerns about arbitrar sex and abuse. Mechanisms such as judicial review, transparency reports, and data protection assessments are weak or missing. This is particularly problematic in systems where surveillance is embedded in the provision of public services or national security functions. Individuals may not have actual choices or knowledge of how to collect, store, or use data. Furthermore, the broader national security exceptions water the accountability of national actors. Conflict legal standards between jurisdictions create uncertainty and enable surveillance actors to use gaps. For example, data collected in a country can store or process other data due to weak protection, enforcement and compensation. Disclosure of surveillance activities is rare and legal challenges are hampered by process barriers and state immunity claims. The lack of robust whistleblower protection and data injury obligations combine the issues further. These exceptions are often used without proper justification or protection measures. Furthermore, legislative extensions of surveillance capabilities (such as the Emergency Act and Counter Terrorism Act) are rarely subject to sunset clauses or independent audits. Because surveillance is embedded in everyday life, the law needs to develop to ensure that it provides democratic value rather than undermine it.

5. Comparative Case Study

To better understand the effectiveness and limitations of existing monitoring laws, this section presents comparative case studies from different jurisdictions. These case studies highlight the challenge that countries are opposed in developing monitoring practices with data protection and provide valuable lessons for the development of global data protection laws. The system, introduced in the 2010s, integrates data from a variety of sources, including financial transactions, social media, criminal history behavior, and more, assigns individuals to social credit effects. This number of points affects access to state services, loans, and even travel reports. Although this system was promoted as a means of promoting trust and social order, it was criticized for its lack of transparency, the possibility of arbitrary punishment, and its impact on individual freedom. The lack of checks and compensation, such as independent oversight and judicial review, addresses the erosion of China's privacy and bourgeois freedom. The system also raises questions about the potential technical overload and the consequences of conferring states widespread authority to monitor and

manage citizens. Under PRISM, the NSA has collected a large amount of data from large technology companies such as Google, Facebook and Apple, including e-mails, phone records, and internet browser history, often without individual consent or judicial surveillance. The revelation, primarily from whistleblower Edward Snowden, sparked a global debate in 2013 about the balance of national security and privacy. Critics argue that massive records of data, especially without separate arrest warrants, violate the constitutional protections against inappropriate searches. Public protests led to the adoption of the US Freedom Act in 2015, reforming certain aspects of surveillance, but many argue that it is not enough to fully protect individual data protection rights. The world's largest biometric identity system, the aadhaar project collects demographic and biometric data for more than 1.3 billion citizens. Aadhaar aims to streamline public services and has been criticized for enabling mass surveillance for his potential. Integrating your system into various state services increases the risk of data injury and the misuse of sensitive personal information. However, the court also confirmed the Aadhaar program with some restrictions. It allowed its use in certain contexts, such as welfare programs, but its essential applications were limited to others. Nevertheless, there are concerns about system implementation and potential data abuse. Spyware can access your smartphone from afar and enable actual tracking of messages, calls and locations. The lack of appropriate legal surveillance and accountability mechanisms for such surveillance has sparked serious ethical and constitutional concerns. GDPR principles such as data minimization, purpose restrictions, and removal rights aim to protect people from unnecessary or excessive surveillance. However, regulations allow certain exceptions, especially in the context of national security and public order. In countries such as France and the UK, laws that allow far more continuous surveillance for national security purposes have expressed concerns about overcontrol and erosion of civil liberties. Despite GDPR's robust framework for data protection, regulations still struggle to keep up with new technologies such as AI and facial recognition, which underscore the need for ongoing legal reform. The national legal frameworks reflect their own socio-political context, but they all illustrate the challenges facing surveillance laws in a rapidly progressive technological landscape. Important teaching from these cases shows that surveillance laws must be adaptable, transparent and subject to strict supervision in order to effectively protect individual rights.

6. Law and Ethical Implications

The rapid development of surveillance technology poses profound and ethical challenges. As governments and businesses increasingly use extended surveillance methods, tensions between public safety, technological advancements, and individual privacy become more complicated. This section considers legal and ethical considerations regarding the impact of monitoring practices and data protection laws. The right to privacy is supported by various constitutions and international human rights instruments, such as the Universal Declaration of the Individual and Article 21 of the Constitution of India, the right to privacy is important to ensure the autonomy and dignity of the individual. Surveillance undermines these rights, particularly when implemented without proper procedures or judicial supervision. While national security or public safety concerns can justify certain surveillance measures, they need to be weighed carefully against potential damage to individual rights. Legal teachings such as proportionality and require closely coordinate surveillance measures and not overly invasive. For example, if there is no strong protection measures, individuals may not have reasonable reliance on personal data if they are misused or illegally accessed. Continuous surveillance could lead to what Shoshana Zuboff describes as "surveillance capitalism." This undermines individual freedom to make autonomous

decisions without external influence or control. In a society where all behavior is observed, people begin to secure their actions and meet social expectations rather than authentic. This can choke creativity, objections and political expression, and has a frightening effect on democratic participation. Surveillance systems operated by AI are as fair as the data they are trained. If historical data reflects social bias, these distortions can be enhanced by surveillance systems, which lead to discriminatory outcomes. This raises the ethical question of whether the use of such technologies affects certain groups, particularly marginalized communities. In authoritarian or semi-authorized states, government surveillance techniques can allow governments to monitor objects, control opposition, and donate freedom of language, associations, and assembly. Chinese Social Credit SystemFor example, it shows how surveillance can be used to control social behavior and punish political or ideological opposition. The ethical principles of human dignity emphasize that people should not reduce to the surveillance of objects and controls. This system of violating dignity puts a society at risk where individuals are no longer valued for their intrinsic values, but is assessed for their conformity with the norms imposed by the state. This principle seeks to restore control of a particular measure of digital identity, especially in a world where information is collected and stored indefinitely. gdpr includes this principle in its framework, but make it practical, particularly how the rights of concern about the public interest and the need for historical records and expressions harmonize. Ethical surveillance practices should prioritize this principle to limit the scope of monitoring to what is needed for legitimate purposes and reduce the risk of donation and data abuse. On the other hand, monitoring national security protection, crime prevention and public security assurances is essentially important. On the other hand, ugly and invasive surveillance is the risk of being violated by individual freedom. Designological Ethics emphasizes that individuals should not be sacrificeed for the goal of utilitarianism, especially when these rights are fixed in international human rights law. The challenge is therefore to find proportional responses that minimize damage and at the same time achieve legitimate social goals. As surveillance technology advances, the need for a differentiated, ethically sound legal approach is becoming increasingly urgent.

7. Legal Reform Recommendations

When surveillance technology is developed, it is essentially important to adapt data protection laws to protect individual rights and tackle threats at the same time. In this section, many recommendations on reforming surveillance laws have been proposed to balance innovation with data protection. These recommendations are based on legal principles, ethical considerations and international best practices.

Establishing a clear legal framework for generational technologies

Monitoring methods must be developed to take into account the rapid advances in technologies such as artificial intelligence (AI), facial recognition, and the Internet of Things (IoT). Legal frameworks need sufficient flexibility to capture new technological developments without being too restrictive. For example, certain regulations regarding the use of AI should be implemented in surveillance that treats issues such as algorithm transparency, accountability, and distortion. These laws must ensure that the use of AI technology does not carry out data protection rights or discrimination. This approach allows laws to remain relevant when technology is developed without requiring constant updates to the legal framework. A robust supervision framework must be determined to monitor the use of surveillance technology by both government and private units. This would look like this:

- Judicial Approval: Surveillance measures, particularly those relating to large amounts of data records, must require approval of judicial

approval prior to implementation. This ensures that surveillance is legally justified and carried out in a manner proportional to the risk. This ensures that monitoring authority is exercised within a clear legal framework and not expanded without proper review. Mechanism of Declaration of Consent. This is especially important in digital rooms where individuals can unconsciously agree to surveillance through services or data protection guidelines. These guidelines are as follows:

- Clear and transparent: You should not fill your consent with long right-wing terminology. Individuals need to understand which data is collected, how it is used, and which data is relevant. Purposes are collected. This reduces the risk of mass surveillance and unauthorized data consumption. Include Comprehensive Data Protection Act: Comprehensive framework conditions such as the European Union's General Data Protection Ordinance (GDPR) must act as models. The law must include regulations for data portability, data removal and access to personal datagovernment or private units. Law Enforcement Surveillance

National security and law enforcement require monitoring measures, but these powers must be settled with strict legal safeguards to prevent abuse. guarantee. control.

- transparency and accountability: Government surveillance activities should be disclosed regularly, and national security authorities should be subject to external supervision to ensure that surveillance measures are proportional to the threat. and ethical standards.

Promoting harmony between international cooperation and law

Observation often exceeds limits, and the lack of international legal cooperation can pose challenges for enforcement. To address this, countries should work to harmonize data protection laws and surveillance frames. This includes:

- Trans-Border Data Protection Contract: Countries must create unified contracts, regulate cross-border data flows, and cooperate to ensure privacy protection across jurisdictions. Face recognition and AI. This includes

- Ethical Review Committee: establishing a committee to assess the ethical implications of new surveillance technologies before the committee is deployed, ensuring that it does not infringe on human rights or permanent harm.

- Public consultation and participation: The government must actively engage with citizens and civil society organisations to gather opinions on surveillance practices and to ensure that the law reflects public considerations regarding privacy and security.

By implementing these reforms, the government can create a surveillance and legal framework. This will keep your data protection rights transparent and accountable, while also addressing security challenges in the digital age. The developmental nature of surveillance technology requires a positive legal response that ensures that individual freedoms are protected and at the same time innovation and public safety are permitted.

Incorporating ethical considerations in surveillance law

Finally, ethical considerations should be integrated into the legal framework for surveillance. This includes:

ethical review committees: establishing committees to evaluate the ethical implications of new surveillance technologies before they are deployed, ensuring that they do not infringe upon human rights or perpetuate harm.

public consultation and participation: governments should actively engage with citizens and civil society organizations to gather input on surveillance practices and ensure that laws reflect public concerns about privacy and security.

By implementing these reforms, governments can create a surveillance legal framework that is transparent, accountable, and respectful of privacy rights while addressing the security challenges of the digital age. The evolving nature of surveillance technology demands proactive legal responses that ensure individual freedoms are protected while allowing for innovation and public safety.

8. Conclusion

The future of privacy in the age of rapidly advancing surveillance technologies presents a complex challenge for policymakers, legal professionals, and society at large. As new technological innovations continue to emerge, the tension between the need for security and the protection of individual privacy rights grows more pronounced. This research has explored the evolving landscape of surveillance law, highlighting the legal, ethical, and social implications of widespread surveillance in a digital world.

While surveillance technologies, such as ai, facial recognition, and the internet of things (iot), have the potential to enhance security and streamline services, they also present significant risks to privacy, autonomy, and human dignity. The challenge lies in balancing the benefits of innovation with the fundamental rights of individuals. The legal frameworks governing surveillance must evolve to ensure that these technologies are used in a manner that is transparent, accountable, and respectful of privacy rights.

The paper has proposed a range of recommendations for reforming surveillance laws, including strengthening oversight mechanisms, ensuring robust data protection, promoting international cooperation, and incorporating ethical considerations into surveillance practices. These reforms are essential for creating a legal environment that supports both technological progress and the protection of individual rights.

Ultimately, the future of privacy hinges on the ability of lawmakers to adapt legal frameworks that can keep pace with technological advancements while safeguarding the core values of democracy and human rights. As surveillance technologies become more pervasive, it is imperative that we foster an ethical and legal framework that ensures transparency, accountability, and respect for the privacy of all individuals.

As we move into an increasingly digital and interconnected future, the protection of privacy must remain a fundamental pillar of both national and international legal systems. This will require a continued commitment to refining and updating laws, fostering public awareness, and ensuring that privacy rights are respected, even in the face of technological advancements.

References

- Allen, a. L. (2011). privacy in the age of big data: a review of privacy law in the u.s. yale law journal, 120(3), 1234–1259. Https://doi.org/10.2307/22899374
- Binns, r. (2018). on the role of privacy in artificial intelligence. Journal of ethics and information technology, 20(2), 1-11. Https://doi.org/10.1007/s10676-017-9441-4
- Boyd, d., & crawford, k. (2012). critical questions for big data: provocations for a cultural, ethical, and technical agenda. Information, communication & society, 15(5), 662-679. Https://doi.org/10.1080/1369118x.2012.678878
- Cate, f. H. (2006). the failure of fair information practice principles. In d. L. Weitzner, p. M. Schermer, & g. M. Young (eds.), privacy and the law: an international perspective (pp. 137-152). Oxford university press.
- European commission. (2016). general data protection regulation (gdpr). Official journal of the european union, l119, 1–88. Https://eur-

lex.europa.eu/legal-content/en/txt/?Uri=celex%3a32016r0679

- Solove, d. J. (2021). understanding privacy (2nd ed.). Harvard university press.
- Zuboff, s. (2019). the age of surveillance capitalism: the fight for a human future at the new frontier of power. Publicaffairs.
- United nations. (2014). the right to privacy in the digital age: report of the united nations special rapporteur on the right to privacy. United nations general assembly, a/69/397.