INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 4 AND ISSUE 2 OF 2024

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Free and Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 4 and Issue 2 of 2024 (Access Full Issue on - https://ijlr.iledu.in/volume-4-and-issue-2-of-2024/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education (Established by I.L.E. Educational Trust)

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in

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

VOLUME 4 AND ISSUE 2 OF 2024

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

Published by

Institute of Legal Education

https://iledu.in

PRIVACY CONCERNS IN THE ERA OF SURVEILLANCE TECHNOLOGIES: NAVIGATING THE NEW FRONTIER

AUTHOR - VIKAS KUMAR* & DR. AMAN MALIK**, RESEARCH SCHOLAR* & ASSISTANT PROFESSOR**, DEPARTMENT OF LAW, JAGANNATH UNIVERSITY

BEST CITATION - VIKAS KUMAR & DR. AMAN MALIK, PRIVACY CONCERNS IN THE ERA OF SURVEILLANCE TECHNOLOGIES: NAVIGATING THE NEW FRONTIER, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 4 (2) OF 2024, PG. 1304-1311, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

In the contemporary landscape, the intersection of privacy concerns and advanced surveillance technologies has emerged as a critical issue, reshaping the boundaries of personal autonomy and data security. As surveillance technologies, including AI-driven monitoring systems, facial recognition, and data analytics, become increasingly sophisticated, they offer unprecedented capabilities for monitoring and analyzing individuals' behavior. While these advancements can enhance security and streamline various processes, they also pose significant risks to privacy. This research article explores the multifaceted privacy challenges introduced by the proliferation of surveillance technologies. It delves into how these technologies collect, process, and disseminate personal data, often without explicit consent or adequate transparency. The analysis includes a review of current privacy laws and regulations, assessing their effectiveness in addressing the rapidly evolving technological landscape. Particular attention is given to the limitations of existing legal protections and the need for more robust and adaptive frameworks to safeguard privacy in the digital age.

Keywords: Privacy, Surveillance, AI, Data Protection

INTRODUCTION

Artificial intelligence (AI) is a branch of computer science and engineering that focuses on developing intelligent machines that can perform tasks that typically require human intelligence, such as visual perception, speech recognition, decision-making, and language translation.[1359] AI systems are designed to learn from experience, adapt to new situations, and improve performance over time without being explicitly programmed. The ultimate goal of AI is to create machines that can simulate human intelligence, including reasoning, problem-solving, and creativity.

With the growing technological innovation surveillance technologies and artificial intelligence (AI) have profoundly transformed the way personal data is collected, analyzed, and utilized. This paradigm shift has introduced unprecedented privacy concerns, necessitating a comprehensive examination of the implications for individual rights and freedoms. "Privacy Concerns in the Era of Surveillance Technologies: Navigating the New Frontier" delves into the intersection of technological advancement and privacy, highlighting the growing challenges in protecting personal information.

The rapid evolution of surveillance technologies ranging from ubiquitous data collection tools to sophisticated AI-driven analytics has enabled an unprecedented level of monitoring and data aggregation. These technologies, while enhancing efficiency and innovation, have also led to significant intrusions into personal privacy.

[1359] Edwin Olorondu, AI in Surveillance 44 (ASIN Publication, 3rd edn., 2024)

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

VOLUME 4 AND ISSUE 2 OF 2024

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

Published by

Institute of Legal Education

https://iledu.in

CONCEPTUAL ANALYSIS OF THE RIGHT TO PRIVACY

Privacy is a fundamental element of personal freedom, originating from the Latin term 'privatus,' which signifies something private, secret, or personal, distinct from public or state ownership.[1360] This concept entails the control over one's personal affairs, allowing individuals to decide what aspects of their lives to keep confidential. Globally, the right to privacy is acknowledged as a basic human right under Article 12 of the Universal Declaration of Human Rights Act of 1948.[1361] In India, this right is enshrined as a fundamental right under Article 21 of the Constitution, a status that was affirmed by the Supreme Court in the landmark 2017 case **Justice K.S. Puttaswamy v. Union of India**[1362]

The Puttaswamy case stands as a landmark judgment for several reasons, and one the facet for which it is remembered is its emphasis on recognizing and protecting informational privacy in India. The Supreme Court of India held that to make the right to privacy meaningful, the state must establish a robust data protection framework and give due respect to the informational privacy.[1363] This framework should not only safeguard citizens from threats to their informational privacy posed by both state and non-state actors but also serve the common good. The Court outlined the state's duty to ensure that such protections are in place, thereby guiding the committee responsible for creating the data protection framework to prioritize these principles. This judgment has significantly shaped the legal landscape concerning privacy and data protection in India, highlighting the necessity for comprehensive measures to protect personal information in the digital age.

In India, the Right to Be Forgotten is derived from the right to informational privacy, which is a facet of the right to life and personal dignity under Article 21 of the Constitution. This connection was highlighted by the Supreme Court in the landmark **K.S. Puttaswamy v. Union of India**[1364] judgment.

Right to privacy recently got recognized as a Fundamental Right in the year 2017 however the idea of right to privacy is very ancient and remained a center of legal debate from past five decades.[1365] It took years to get recognized as Fundamental Right. Supreme Court many times encountered cases related to privacy issues but there was no solid outcome as to whether it is a fundamental right or not. However the concrete shape given to the right to privacy in India with time by a series of the judgments of the Supreme Court of India. The first judgment of the Supreme Court on privacy related issue was given in MP Sharma v. Satish Chandra8 case where court was in favor that right to privacy does not comes under the ambit of the fundamental right. Supreme Court of India again encountered a case on privacy related issue after the passing of nine years of this judgment in the famous case of Kharak Singh v. State of Uttar Pradesh9 Supreme Court again gave a judgment mocking down the idea of right to privacy as a fundamental right. However this case is of great importance in evolution of Right to Privacy because of the dissenting opinion of the Justice Subba Rao who opined that even though our Constitution is silent about the right to privacy being a fundamental right still it is a very essential component for the personal liberty of an individual. Later on after the passing of twelve years of this judgment Supreme Court faced a case titled Gobind v. State of Madhya Pradesh10 in which for the first time it was held that privacy comes under the ambit of the Fundamental Right and it is enshrined under Article 21 of the Indian Constitution. The Digital Personal Data

[1360] Payal Thaorey, "Informational Privacy: Legal Introspection in India" 2 *ILI Law Review* 161 (2019)

[1361] Aysem Diker Vanberg, *The Right to Privacy Revisited: Different International Perspective* 56 (Taylor & Francis Ltd, India, 1st edn., 2021)

[1362] AIR 2018 SC 1841

[1363] Ravinder Kumar, Right to Privacy in India: Concept and Evolution 78 (Lightning Source, India, 3rd edn., 2019)

[1364] AIR 2018 SC 1841

[1365] Pavan Duggal, Data Protection Law in India 76-94 (Universal Law Publishing, Allahabad, 4th edn.,2021)

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

VOLUME 4 AND ISSUE 2 OF 2024

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

Published by

Institute of Legal Education

https://iledu.in

Protection Act, 2023, further supports this right by including provisions that allow individuals to request the erasure of their personal data. This legislative framework provides a legal basis for enforcing the Right to Be Forgotten, thereby enhancing individuals' control over their personal information in the digital space.

AI DRIVEN SURVEILLANCE TECHNOLOGY

Surveillance refers to the systematic monitoring of individuals, groups, or environments, typically by government agencies, law enforcement, or private entities, to collect information about their activities, behaviors, or interactions. This monitoring can be done through various means, including physical observation, electronic data collection, and communication interception. Traditional forms of surveillance include methods such as CCTV cameras, wiretapping, and manual observation, which rely on human intervention and are often limited in scope and effectiveness.

The concept of surveillance had been ingrained in Indian society since time immemorial but however with the coming up of technological advancement this entire domain got a new boost. Chanakya's Arthasastra described that the Mauryan empire used to deploy spies and secret agents as a tool of military strategies. In the days of difficult communication, loyal and efficient bureaucracy was based on the spying and monitoring.[1366] Various methods of surveillance was heavily used during the Mughal and the British period. Use of professional spies and official snooper were very common in British India. By keeping a strong surveillance in India, British enhanced their control on villages and collected territorial revenues at large scale.

AI-driven surveillance technology represents a more advanced and automated approach to monitoring and data collection, utilizing artificial intelligence (AI) to enhance and expand traditional surveillance methods. AI-driven surveillance leverages sophisticated algorithms, machine learning, and data analytics to process and analyze large volumes of data from diverse sources. Key components of AI-driven surveillance technology include:

1. Facial Recognition: AI systems that can identify and verify individuals by analyzing facial features captured through cameras. These systems compare the features of individuals in real-time or from stored images with a database of known faces to determine identities.

2. Behavioral Analysis: AI algorithms that can monitor and analyze behavioral patterns, such as unusual movements or activities, to predict potential criminal behavior or security threats. This includes analyzing data from video feeds, social media, and other sources to identify suspicious patterns.

3. Predictive Policing: AI-driven tools that use historical data and statistical models to forecast where and when crimes are likely to occur. These tools assist law enforcement in allocating resources and deploying personnel to areas with a higher likelihood of criminal activity.

4. Data Aggregation and Analysis: AI systems that collect and analyze data from multiple sources, such as social media platforms, internet usage, and public records, to build comprehensive profiles of individuals and assess potential risks.

AI-driven surveillance technology offers significant advantages in terms of efficiency, scalability, and the ability to process vast amounts of data quickly. However, it also raises important ethical and privacy concerns, as the extensive collection and analysis of personal information can infringe on individual privacy rights and lead to potential misuse or abuse of the data collected.

AI-driven surveillance in India represents a complex and rapidly evolving aspect of the country's approach to security and public management. The integration of artificial

[1366] Artificial Intelligence: The New Eyes of Surveillance, *available at:* https://www.forbes.com/sites/forbestechcouncil/2024/02/02/artificial-intelligence-the-new-eyes-of-surveillance/ (Last visited on May 12, 2024)

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

VOLUME 4 AND ISSUE 2 OF 2024

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

Published by

Institute of Legal Education

https://iledu.in

intelligence into surveillance systems has significantly enhanced the capabilities of law enforcement and government agencies, enabling them to monitor vast amounts of data, detect patterns, and respond to incidents with unprecedented speed. In urban areas, AI-driven technologies, such as facial recognition systems and predictive policing tools, have been implemented to bolster security and public safety. These systems utilize algorithms to analyze video feeds from public cameras, identify individuals, and predict potential criminal activities based on behavioral patterns and historical data. This capability has led to increased efficiency in identifying suspects and preventing crimes before they occur. However, the deployment of these technologies has sparked considerable debate regarding privacy and civil liberties. The extensive collection and processing of personal data, often without explicit consent, raise significant concerns about the erosion of privacy and the potential for misuse of sensitive information. The lack of comprehensive data protection laws and regulations in India exacerbates these concerns, as there are limited legal safeguards to prevent unauthorized access or abuse of surveillance data.

PRIVACY CONCERNS RELATING TO SURVEILLANCE TECHNOLOGIES

The advent of artificial intelligence (AI) has brought transformative changes across various sectors, and one of the most significant areas impacted is surveillance. AI-powered surveillance systems have revolutionized the way monitoring and security operations are conducted, introducing capabilities that were previously unimaginable. These advanced systems utilize sophisticated algorithms to analyze vast amounts of data in real-time, enabling the detection and prediction of potential security threats with remarkable accuracy. From facial recognition technology to predictive policing, AI has enhanced the efficiency and effectiveness of surveillance mechanisms.

At the forefront of AI in surveillance is facial recognition technology, which has been widely adopted in public spaces, transportation hubs, and by law enforcement agencies. This technology uses sophisticated algorithms to identify individuals based on their facial features, enabling real-time monitoring and identification of people in crowded areas.[1367] While this has proven effective in enhancing security, particularly n tracking suspects and preventing crimes, it has also sparked considerable controversy regarding the erosion of personal privacy and the potential for misuse by authorities. Beyond facial recognition, AI is employed in video analytics, where it automates the review of extensive surveillance footage.[1368] Traditional manual video analysis is labor-intensive and time-consuming, but AI can quickly scan hours of footage to detect unusual activities, recognize patterns, and alert security personnel to potential threats. This capability is crucial in critical infrastructure security, such as airports, seaports, and power plants, where timely threat detection is paramount. AI-driven video analytics can also identify specific behaviors, such as loitering, aggressive movements, or the presence of unattended objects, providing an additional layer of security by enabling proactive responses to potential incidents. Moreover, AI's role in predictive policing is an evolving aspect of surveillance. By analyzing historical crime data, AI algorithms can forecast potential criminal activities and identify hotspots where crimes are more likely to occur. This predictive capability allows law enforcement agencies to allocate resources more effectively, potentially preventing crimes before they happen. In addition to enhancing physical surveillance, AI is extensively used in cybersecurity to monitor and protect digital infrastructure. AI systems can detect and respond to cyber threats in real-time, identifying anomalies in network traffic that

[1367] Edwin Olorondu, AI in Surveillance 44 (ASIN Publication, 3rd edn., 2024)
[1368] Advantages of using Artificial Intelligence in Video Surveillance, *available at:* https://www.infosysbpm.com/blogs/business-transformation/advantages-of-using-artificial-intelligence-in-video-surveillance.html (Last visited on May 2, 2024)

may indicate malicious activities. By continuously learning from data, these systems improve their detection capabilities, helping to safeguard sensitive information from cyber-attacks.

Despite the numerous benefits, the integration of AI in surveillance comes with significant ethical and legal challenges. The pervasive use of AI technologies for monitoring can lead to a surveillance state, where individuals are constantly watched, and their behaviors are meticulously recorded. This raises profound questions about the right to privacy and the extent to which surveillance is justified in the name of security. There are also concerns about data security and the potential for breaches that could expose sensitive personal information to unauthorized entities.

While AI Surveillance can enhance security, it also means that individuals can be monitored continuously without their explicit consent.[1369] This constant monitoring raises significant privacy concerns, as it erodes the anonymity that individuals once enjoyed in public spaces. People may feel like they are under constant scrutiny, which can have a chilling effect on their behavior and freedom of movement. Another significant challenge posed by AI surveillance is the risk of data breaches and unauthorized access to personal information. AI systems rely on large datasets to function effectively, often storing vast amounts of sensitive information, including biometric data like facial features, fingerprints, and voice patterns. If these systems are hacked or otherwise compromised, the data they contain can be exposed, leading to identity theft, financial loss, and other forms of personal harm. The centralization of such sensitive information in AI surveillance databases makes them attractive targets for cybercriminals. The use of AI for targeted advertising and marketing further complicates the privacy landscape. AI systems analyze individuals' online behavior, purchase history, and other personal data to deliver customized advertisements. While this can enhance user experience by providing relevant content, it also means that individuals' activities are constantly tracked and analyzed. This level of surveillance can feel invasive, as it involves the commodification of personal information without explicit consent. Moreover, the data used for targeted advertising can be repurposed for other forms of surveillance, blurring the lines between commercial and state monitoring.

RIGHT TO BE FORGOTTEN AS A TOOL FOR THE SAFETY OF THE DATA

The "Right to be Forgotten" or "Right to be Erased" essentially grants individuals the authority to request the removal of their personal data from the vast expanse of the internet.[1370] At its core, this principle operates on the premise that any use of data must be consensually authorized by the data owner. Consequently, upon withdrawal of this consent, the data owner retains the right to have their data expunged. Moreover, when the data controller lacks the legal basis to process the data, erasure becomes imperative. In the event of data erasure, all parties with access to or processing capabilities for the data are obligated to delete it, along with any associated links, copies, or replicas. The origin of this right can be traced back to French jurisprudence on the concept of the "right to oblivion," which aimed to facilitate the social reintegration of individuals who had served their sentence by preventing the publication of information about their past crimes. Building upon this foundation, the European Union Data Protection Directive of 1995 formally recognized the right to be forgotten through the introduction of Article 12.[1371] This provision stipulates that member states must afford individuals the ability to control, rectify, erase, or block data pertaining to them.

[1369] Artificial Intelligence: The New Eyes of Surveillance, *available at:* https://www.forbes.com/sites/forbestechcouncil/2024/02/02/artificial-intelligence-the-new-eyes-of-surveillance/ (Last visited on May 12, 2024)

[1370] Melissa Stock, *The Right to be Forgotten: The Law and Practical Issues* 34 (Law Brief Publishing, 1st edn., 2020)

[1371] EU General Data Protection Regulations, *available at:* https://www.hrw.org/news/2018/06/06/eu-general-data-protection-regulation (last visited on June 23, 2024)

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 2 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

The concept of the "Right to be Forgotten" originated in the EU and gained significant attention through the landmark **Google Spain case**[1372]. In this case, the European Court of Justice ruled that Google, as a major search engine, must remove links to private information upon request by European citizens if the information is deemed no longer relevant. This decision marked a pivotal moment in the development of data privacy rights. The principle of the RTBF was later solidified in Article 17 of the European GDPR of 2016, giving it formal statutory recognition. This regulation allows individuals to request the deletion of personal data that is outdated or no longer necessary, thereby enhancing their control over personal information in the digital realm. This legal advancement underscores the EU's commitment to protecting individual privacy in an increasingly interconnected world, setting a precedent for data protection laws globally. The incorporation of the RTBF into the GDPR has significant implications, emphasizing the importance of balancing individual privacy rights with the public's right to access information.

In the recent case of **TU & RE vs Google LLC**[1373], the European Court of Justice determined that the responsibility to prove the inaccuracy of information lies with the data principal. Only when this inaccuracy is established does the duty of the data fiduciary to remove the information arise. Moreover, the court extended the scope of the right to erasure defined in the Google Spain case, now including the removal of photographs or thumbnails even if they link to the original source. This removal, however, must be balanced against the rights and public interest involved.

The concept of the RTBF has not been explicitly mentioned under the Indian Constitution. However, through a series of judicial pronouncements, the judiciary has recognized and outlined that RTBF is intricately intertwined with the Right to Privacy. In various judgments, the courts have elucidated that the Right to Privacy encompasses not only the protection of personal information but also the right to control and manage one's digital identity. This evolution has been particularly pronounced in cases involving the removal of objectionable or outdated information from online platforms, where the courts have emphasized an individual's right to be free from unwarranted intrusion into their private affairs.

Close to that time, In 2017, the Supreme Court of India, in its **landmark K.S. Puttaswamy vs. Union of India**[1374] decision, recognized the right to privacy as a fundamental right under Article 21 of the Indian Constitution. This recognition came from a historic ruling by a Nine-Judge Bench, which underscored the significance of privacy in the digital age. The right to informational privacy has become increasingly critical as technology advances, with individuals leaving digital footprints across various platforms, whether private or governmental. Sensitive personal information is readily available on media platforms, particularly social media, which exposes individuals to potential misuse by malicious actors or exploitation by large corporations for personal gain. The "Right to be Forgotten" emerges as a vital mechanism, allowing individuals to control the spread of their personal information online, thereby preventing the rampant misuse of freely accessible data on the internet. Nonetheless, several High Courts have acknowledged its importance, drawing inspiration from the observations made by Justices Rohinton F. Nariman and Sanjay Kishan Kaul in the Puttaswamy judgment. These courts have issued interim orders that uphold the "Right to be Forgotten" as an essential component of the fundamental right to privacy, signaling a progressive shift towards its broader acceptance and implementation in India.

[1372] Google Spain, SL, Google Incv. Agencia Espanola de Protection de Datos
[1373] CJEU - C-460/20
[1374] AIR 2018 SC 1841

In the 2023 case of **Vyskh K.G. v Union of India**,[1375] the Court permitted the masking of names in family and matrimonial cases, citing the right to be forgotten as the basis for this decision.

In the recent case of **ABC v. Union of India and Others[1376],** the Bombay High Court ordered the removal of an acquittal order from the Court's website. This decision was made in response to a plea by an individual who had been acquitted but was facing difficulties in securing employment due to the publicly accessible acquittal order.

LEGISLATIVE ENACTMENT RELATING TO THE DATA SAFETY OF THE USERS

In various jurisdictions worldwide, specific laws and regulations are in place to govern data protection, delineating the rights and responsibilities of individuals and organizations in relation to the collection, storage, processing, and sharing of personal data. Around 70% of nations globally have implemented some form of data protection legislation, as reported by the United Nations trade agency UNCTAD. These regulations serve as frameworks for ensuring the privacy and security of individuals' personal information. Notable examples include the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) in the United States etc..The EU's General Data Protection Regulation (GDPR), enacted in 2018, is hailed as the most stringent privacy and security law worldwide, setting the standard for global data protection measures. Recent years have seen various countries, such as China and Vietnam, strengthening their laws concerning the transfer of personal data across borders. In a similar vein, Australia passed a bill in 2018 granting law enforcement access to encrypted data, reflecting a global trend towards heightened data privacy regulations and security measures.
In a significant 2017 ruling, India's Supreme Court recognized the right to privacy as a fundamental right and emphasized the need for a robust data protection framework that balances individual privacy with legitimate state interests. However, it took nearly six years after this landmark judgment for India to enact a comprehensive data protection law. The Digital Personal Data Protection Act, 2023, which has undergone several drafts, has been criticized for not adequately enhancing individual privacy rights or holding non-state entities accountable for data misuse. The Act also grants wide-ranging exemptions to the government and its instrumentalities, resulting in minimal accountability for state entities handling user data.

The legislature has actively contributed to the protection and regulation of digital personal data by enacting the Digital Personal Data Protection Act, 2023.[1377] This legislation aims to strike a balance between individual rights and public interest in the processing of digital personal data. Section 13 of the Act grants data principals the right to request correction and erasure of their personal data. It mandates that data fiduciaries respond to such requests by updating, correcting, completing, or erasing the data. However, requests for data erasure can only be honored if the data's original purpose has been fulfilled and it is no longer required for legal purposes. Additionally, under Section 16(4), data principals are obligated to provide verifiable and authentic information.

Section 18(1) of the Act outlines specific exceptions to this right, indicating instances where it will not apply. These exceptions include situations where the data is necessary for judicial or quasi-judicial functions, enforcement of legal rights or claims, prevention, detection, investigation, or prosecution of offences or law violations, and when data processed outside India by a person within India is pursuant to a contract. Furthermore, the Union Government has the authority under the second clause of this section to exempt the Act's application for

[1375] WP(C) 26500/2020
[1376] W.P. No. 3499 of 2021
[1377] Understanding India's New Data Protection Law, *available at:* https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en (last visited on June 25, 2024)

statistical purposes or to prevent incitement to cognizable offences related to public order, security, sovereignty, integrity, and friendly relations with other states.

The Act also establishes the Data Protection Board under Section 19, which is responsible for ensuring compliance with the Act's provisions, penalizing offenders, and performing functions as directed by the Central Government. Additionally, the Criminal Procedure (Identification) Rules empower investigating authorities to collect identifiable information such as biological samples and fingerprints, which are to be stored in digital or electronic form for 75 years. However, in cases of acquittal, this information must be destroyed unless a Court or Magistrate orders otherwise, providing reasons in writing. This rule imposes a limitation on the right to be forgotten and poses significant implications for the right to privacy.

CONCLUSION

AI-driven surveillance systems, increasingly adopted by governments and non-governmental entities, have led to significant privacy breaches, primarily due to the unrestricted and indefinite storage of vast amounts of personal data. These systems often collect data on a massive scale, ranging from location tracking to behavioral patterns, under the guise of enhancing security and operational efficiency. However, this unchecked accumulation of data poses a serious threat to individual privacy, as it allows for the potential misuse or unauthorized access to sensitive information. The lack of clear regulations and oversight exacerbates the problem, leaving individuals vulnerable to constant surveillance without their informed consent. Therefore, it is crucial to establish a balanced approach that ensures both privacy and security, with stringent data protection measures, transparency, and accountability in place to safeguard against the misuse of AI-driven surveillance technologies.

BIBLIOGRAPHY

Books

- Ravinder Kumar, Right to Privacy in India: Concept and Evolution 78 (Lightning Source, India, 3rd edn., 2019)
- Rakesh Chandra, Right to Privacy in India with Reference to Information Technology Era 120 (YS Books International, India, 2nd edn., 2020)
- Pavan Duggal, Data Protection Law in India 76-94 (Universal Law Publishing, Allahabad, 4th edn.,2021)

Journals

- Nikhil Aswani, "The Right to be Forgotten and its Enforcement in India" 6 *International Journal of Legal Development and Allied Issues* 107-123 (2020)
- Nivedita Harsh, "Right to be Forgotten: A Tug of War between Right to Privacy and the Freedom of Speech" 4 *International Journal of Legal Science and Innovation* 737-745 (2022)

Websites

- https://www.scconline.com/blog/post/2021/10/01/right-to-digital-privacy/
- https://www.scconline.com/blog/post/2021/06/15/protection-of-personal-data/
- https://articles.manupatra.com/article-details/Telephonic-Surveillance-as-a-Serious-Invasion-of-Right-to-Privacy-in-India