INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

ANALYSING RIGHT TO PRIVACY UNDER ARTICLE 21 IN THE AGE OF STATE SURVEILLANCE: A COMPARATIVE STUDY OF INDIA, THE UNITED STATES, AND EUROPE

AUTHORED BY - DR ANKIT SOURAV SAHOO
Assistant Professor (S-II)
Lajpat Rai Law College, Sambalpur

Abstract:

This article analyses the evolution and contemporary relevance of the Right to Privacy under Article 21 of the Constitution of India in the context of expanding state surveillance technologies. Historically, Article 21 guarantees that no person shall be deprived of life or personal liberty except according to procedure established by law. Judicial interpretation has significantly broadened this provision, particularly after the landmark judgments in Maneka Gandhi v. Union of India and Justice K.S. Puttaswamy v. Union of India (2017), where the Supreme Court recognized privacy as a fundamental right intrinsic to human dignity and personal liberty. The study critically examines India's existing surveillance framework, which relies on outdated legislation such as the Indian Telegraph Act, 1885 and provisions of the Information Technology Act, 2000. These laws grant wide powers to the executive to intercept and monitor communications, often without adequate judicial oversight. Contemporary developments, including the Pegasus spyware controversy and the growing use of facial recognition technologies, demonstrate how rapidly advancing technology has intensified concerns regarding privacy violations and democratic freedoms. Through a comparative analysis of India, the United States, and the European Union, the article highlights differing constitutional and regulatory approaches to balancing privacy with national security. While the United States relies on Fourth Amendment jurisprudence and judicial warrants, the European Union provides robust statutory protection through instruments such as the GDPR and strong data protection authorities. The article argues that despite constitutional recognition of privacy, India still lacks effective institutional safeguards and transparent oversight mechanisms. Ultimately, it emphasizes the urgent need for comprehensive surveillance reform, stronger accountability, and judicial authorization to ensure that technological advancement does not undermine the fundamental right to privacy.

ISSN: 2582-6433

Keywords: Right to Privacy, Article 21, State Surveillance, Data Protection, National Security

Introduction:

Imagine crafting a private journal. You hide it under your pillow, locked away with a tiny key. In the tangible world, authorities typically necessitate a warrant, a court-approved rationale, to gain entry to that diary. However, in modern times, your "journal" is embodied by your mobile device. Your location history, private communications, health information, and even your heartbeat data are all included within it. Imagine a situation where authorities have the ability to "see" into your digital space using undetectable software, facial recognition technology in public gatherings, and mechanisms that track every financial transaction. This concept is commonly known as the Surveillance State.

In the context of Indian legal principles, the concept of the "Right to be Let Alone" represents a fundamental element of personal freedom. Nonetheless, with the progression of technology, the state's ability to monitor has increased at an even more accelerated pace. This paper examines the effectiveness of Article 21 of the Indian Constitution in protecting individuals against the extensive monitoring by the state.

The Significance of Article 21 in Judicial Interpretation

Understanding surveillance requires an initial grasp of Article 21. This statement is concise but carries significant weight: No person shall be stripped of life or personal freedom except through processes defined by legal standards. During the early phase in India (A.K. Gopalan v. State of Madras, 1950), the Supreme Court took a limited view. They contended that provided the government passed any laws via Parliament, it could potentially infringe upon your freedom. They showed little regard for the justice of the law; their only focus was on its mere presence. The case of Maneka Gandhi v. Union of India (1978) represented a pivotal shift. The Court concluded that any "procedure" utilised by the state to restrict an individual's freedom must be "just, fair, and reasonable." The law must be substantive and non-arbitrary, rather than merely nominal.[1]

At present, "Life and Liberty" embodies your Digital Identity. When the government monitors your phone, they are not just reviewing information; they are analysing your very existence.

[1] Vajiram Editor. (2025, January 27). *Right to Privacy, Evolution, Significance, Challenges*. User's Blog; vajiramandravi. https://vajiramandravi.com/upsc-exam/right-to-privacy/

ISSN: 2582-6433

The Puttaswamy judgement (2017) affirmed that privacy is not merely a privilege; it is fundamental to authentic liberty.

The Indian Surveillance Framework:

One of the most intriguing facets of Indian jurisprudence is the utilisation of "ancestor laws" to govern "space-age technology." The Indian Telegraph Act of 1885, Section 5(2) This statute was established in the age of telegrams. However, it remains applicable for the interception of phone communications. It authorises governmental interception under circumstances deemed as "public emergency" or "public safety." The question at hand is Who holds the authority to define what constitutes a "emergency"? Generally, this responsibility falls to a high-ranking government official, such as the Home Secretary, rather than to the judiciary. This suggests that the executive branch is assessing its own actions. The Information Technology Act of 2000, Section 69 represents the modern version of the Telegraph Act. It allows the government to intercept, monitor, or decrypt any information generated, transmitted, or stored within any computational resource. It includes grounds such as "sovereignty of India," "defence," and "prevention of incitement to an offence."[2]

While there are established guidelines regulating this procedure, they often encounter scrutiny due to their opacity. If your phone is being monitored, you remain uninformed. How can an individual challenge a violation of their rights if they are oblivious to its existence?

The Pegasus Controversy:

In 2021, a noteworthy global news event revealed that a software called Pegasus, created by the NSO Group in Israel, was utilised to surveil journalists, activists, and politicians in India. Many spyware programs require user interaction, such as clicking a link. In contrast, Pegasus functions as a "Zero-Click" exploit. It can infiltrate a device through a missed WhatsApp call that remains unrecorded in your call history. This capability turns your phone into a constant surveillance tool, capturing audio through the microphone and visual data via the camera. In the case of Manohar Lal Sharma v. Union of India[3], the Supreme Court underscored that "National Security" cannot serve as a blanket justification for unchecked governmental power. The administration refrained from confirming its use of the software, citing national security

[2] Gupta, A. (2018, August 5). *Phone Tapping In India: A Need To Revisit Law?* Livelaw.in; Live Law. https://www.livelaw.in/phone-tapping-in-india-a-need-to-revisit-law
[3] AIR 2021 SC 5396

ISSN: 2582-6433

as the reason. The Court asserted that while the state may hold certain secrets, this does not grant it immunity from scrutiny regarding violations of citizens' rights. Despite an investigative committee's efforts, the results were labelled "inconclusive" due to insufficient cooperation from the government. This raises a critical question: If the state wields cutting-edge technology, can the legal framework ever truly keep up?[4]

Facial Recognition and Its Impact on Personal Freedoms

Facial Recognition Technology (FRT) can often be seen in surveillance systems at airports and railway stations across India. Law enforcement argues that it facilitates the capture of criminals. Nevertheless, from a legal perspective, this issue presents a multifaceted and precarious landscape. Currently, there is no specific law in India that regulates the use of facial recognition technology (FRT). Its implementation is based on executive orders, which fails to meet the "Legality" requirement of the Puttaswamy triadic assessment. The impact of the "Chilling Effect" on freedom of expression under Article 19. Article 19 guarantees the fundamental right to express oneself freely. Imagine being present at a peaceful gathering focused on the issue of climate change. If you knew that your facial image would be recorded, linked to your Aadhaar card, and result in your inclusion on a "watch list," would you still choose to go ahead? It is exceedingly improbable. This occurrence is known as the "Chilling Effect." When people observe surveillance, they stop exercising their rights. Surveillance not only erodes privacy; it fundamentally dismantles democratic principles.[5]

When the government claims, "We must monitor all individuals to prevent a single terrorist," they face a challenge regarding proportionality. In the Puttaswamy case, the Court emphasised that the state is required to show that its actions are "proportionate." Is there a legitimate aim? (for example, neutralising a bomb). Is this the only approach? Is it possible to neutralise the threat without delving into individuals' private communications? Is the benefit greater than the harm? Currently, in India, the rationale of "National Security" is often seen as a "black box." When the government utters those two words, the courts often hesitate to delve deeper. True reform requires that a judge, rather than just a government official, must approve each request for monitoring.

[4] *Pegasus Spyware Probe - Supreme Court Observer*. (2025, July 16). Supreme Court Observer. https://www.scobserver.in/cases/manohar-lal-sharma-v-union-of-india-pegasus-spyware-probe-case-background/

[5] Raj, H. (2026, March). *Facial Recognition Technology and the Right to Privacy in India - The Cyber Blog India*. The Cyber Blog India. https://cyberblogindia.in/facial-recognition-technology-and-the-right-to-privacy-in-india/

ISSN: 2582-6433

The advent of the digital era has significantly transformed the dynamics between citizens and governmental authority. Previously, surveillance methods were confined to physical observation or wiretapping; however, contemporary administrations possess the ability to scrutinise extensive data sets, including metadata, location tracking, and private correspondence. In both India and the United States, the legal discourse surrounding privacy revolves around constitutional safeguards against governmental intrusion. Nevertheless, the two countries have reached their present legal stances via distinct historical and judicial trajectories.

The Indian Viewpoint:

In India, the concept of privacy is deeply intertwined with Article 21 of the Constitution, which ensures the right to life and personal liberty. For many years, the Indian judiciary showed reluctance to formally recognise privacy as a fundamental right. This changed with the pivotal 2017 ruling in Justice K.S. Puttaswamy v. Union of India, where a nine-judge bench of the Supreme Court unanimously affirmed privacy as a fundamental right. The court has determined that privacy constitutes an essential aspect of human dignity, yet this right is not without limitations. The state may encroach upon privacy rights provided it satisfies a three-part criterion: Legality (an existing law must be in place), Need (the action must pursue a legitimate state objective), and Proportionality (the intrusion should be the least restrictive means to achieve the intended outcome). Despite this stringent requirement, the current era of state surveillance illustrated by initiatives such as the Aadhaar project and facial recognition technologies poses significant challenges. The absence of a strong, independent data protection authority often results in the state's assertions of "national security" remaining largely unchallenged, thereby creating a disparity between constitutional principles and the actual practices of mass data collection.

The American Perspective:

Across the ocean, the United States navigates the concept of privacy through a more fragmented yet historically grounded legal framework. In contrast to the Indian Constitution, the U.S. Constitution does not explicitly reference "privacy." Rather, this right is derived from several amendments, particularly the Fourth Amendment, which safeguards citizens against "unreasonable searches and seizures." The legal framework in the United States is fundamentally based on the "reasonable expectation of privacy" standard that emerged in the

ISSN: 2582-6433

1960s. Historically, the "Third-Party Doctrine" permitted government access to data maintained by companies, such as phone records or bank statements, without the necessity of a warrant, positing that individuals relinquished their privacy by sharing information with service providers. However, the advent of the digital era necessitated a re-evaluation. In the landmark case of Carpenter v. United States (2018), the Supreme Court determined that a warrant is generally required for the government to obtain cell-site location information, acknowledging that digital data can disclose intimate aspects of personal life. Although the U.S. has enhanced judicial oversight through the FISA Court, the post 9/11 landscape has witnessed significant expansions in surveillance initiatives that frequently circumvent conventional warrant requirements under the pretext of counter-terrorism efforts.[6]

In examining the liberty and security, the most notable distinction lies in the origin of the right. The privacy right in India is derived from a singular, contemporary, and comprehensive judicial interpretation of "Life and Liberty," providing it with a wide philosophical foundation. Conversely, the right in the U.S. emerges from a historical perspective, developed over centuries through case law that emphasises property rights and safeguards against physical encroachment.

When examining state surveillance, both countries face challenges related to the "National Security" exception. In India, surveillance is frequently regulated by executive orders under the Telegraph Act or the IT Act, which do not require the stringent judicial "prior-authorization" present in the U.S. system. In contrast, an American agent typically must persuade a judge of "probable cause" to monitor a domestic target, whereas an Indian official can often initiate surveillance through internal departmental procedures.

Moreover, the approach to remedies for violations varies significantly. In the United States, the principle of excluding illegally obtained evidence from court proceedings is firmly established. Conversely, India does not adhere to this principle with the same rigour; evidence obtained through privacy violations may still be considered admissible if it is relevant to the case at hand. This results in a less effective deterrent against unlawful state surveillance within the Indian framework.

[6] *Data Protection Frameworks of India and the US: Data Sovereignty vs Market Flexibility - MP-IDSA.* (2025, March 24). MP-IDSA. https://idsa.in/publisher/issuebrief/data-protection-frameworks-of-india-and-the-us-data-sovereignty-vs-market-flexibility

ISSN: 2582-6433

The European Perspective:

The European Union regards privacy as a fundamental human right, stemming from the post-World War II aim to avert state oppression. This right is enshrined in both the European Convention on Human Rights (Article 8) and the Charter of Fundamental Rights of the EU. In contrast to India, where the right was recently interpreted into the Constitution by the judiciary, European law has a well-established, codified dedication to data protection.

The core of the European legal framework is the General Data Protection Regulation (GDPR). Although the GDPR mainly addresses commercial data, it establishes a stringent benchmark that affects state surveillance legislation. European judicial bodies, notably the Court of Justice of the European Union (CJEU), have demonstrated considerable courage in nullifying state surveillance provisions. In landmark cases such as Digital Rights Ireland, the court deemed laws mandating the extensive retention of telecommunications data as invalid, asserting that mass, indiscriminate surveillance is fundamentally disproportionate. The legal principles in Europe maintain that even with a valid security concern, the state cannot presume all citizens to be suspects by default. Comparing liberty and necessity and examining the two, the most notable distinction lies in the development of the regulatory framework. India is currently undergoing a "transformative" phase; it possesses a strong constitutional declaration from the Supreme Court, yet its legislative framework is still in the process of evolving.[7] The Indian government frequently depends on antiquated laws, such as the Telegraph Act of 1885, to sanction surveillance, which does not incorporate the contemporary protections present in European legislation.

Regarding the oversight of surveillance practices, the EU adopts a more stringent "prior-authorization" framework. In numerous EU member countries, surveillance activities necessitate independent judicial consent and are monitored by influential Data Protection Authorities (DPAs). Conversely, in India, surveillance is frequently sanctioned by executive officials, such as the Home Secretary. This arrangement allows the executive branch to essentially "regulate its own actions," leading to an increased likelihood of violations of Article 21.

[7] *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources - Global Freedom of Expression*. (2018, January 19). Global Freedom of Expression. https://globalfreedomofexpression.columbia.edu/cases/ecj-digital-rights-ireland-ltd-v-minister-for-communications-marine-and-natural-resources-c%E2%80%9129312-and-c%E2%80%9159412-2014/

ISSN: 2582-6433

Moreover, the application of proportionality varies significantly across jurisdictions. European courts have consistently emphasised that "national security" cannot be invoked as a blanket justification for overriding rights; they require concrete evidence demonstrating the necessity of mass surveillance. In contrast, the Puttaswamy judgement in India introduced the proportionality test, yet the judiciary tends to exhibit a higher degree of "deference" to the state regarding security issues. Consequently, this results in the Indian state possessing a broader latitude to engage in surveillance compared to its European counterparts.

India and the USA are currently facing the challenge of keeping pace with the rapid advancement of technology in relation to legal frameworks. While India boasts a contemporary and clearly articulated constitutional right, it struggles with the procedural mechanisms necessary to prevent excessive actions by the executive branch. Conversely, the U.S. benefits from a well-established procedural system and a robust litigation culture, yet its legal definitions often reflect an outdated eighteenth-century perspective on "searches," which finds it difficult to adapt to the complexities of cloud computing and artificial intelligence. Nonetheless, both India and the EU are confronting the challenge that technological advancements outpace legal frameworks. India possesses a contemporary and clearly articulated constitutional right under Article 21, yet it currently lacks the necessary independent institutional safeguards to prevent the executive branch from exceeding its authority. The EU, with its intricate and codified legal system, has a judiciary prepared to curtail state overreach; however, it is continually pressured by member states to enhance surveillance measures in the name of combating terrorism and cyber threats.

Ultimately, the current era of heightened oversight has placed both Article 21 and the European Charter in a precarious position. As metadata emerges as a key instrument of governance, the pressing challenge for democracies is to guarantee that the notion of "security" does not transform into an unchecked authority that undermines the essential human right to privacy.

We are currently in a period of change. The DPDP Act, 2023, as mentioned earlier, grants the government significant exclusions. To protect Article 21 in the modern era, we need: Reform in Surveillance: It is essential to replace the 1885 Telegraph Act with updated legislation that requires a judicial warrant for all types of surveillance.

While the government is unable to directly notify a spy about surveillance activities, it is

ISSN: 2582-6433

essential that an annual report reveals the number of individuals monitored, which could be in the thousands. Government officials who exploit monitoring for personal or political gain, such as illegal tapping, must face stringent penalties, as illustrated in cases like Vinit Kumar v. CBI. The law transcends mere statutes; it establishes the boundaries that limit state power. In the absence of privacy, dignity cannot be achieved; and without dignity, the "Life" promised by Article 21 is rendered void.

Conclusion:

The rapid advancement of digital technology has fundamentally transformed the relationship between the individual and the state, making the protection of privacy more complex and more crucial than ever before. In India, the recognition of privacy as a fundamental right under Article 21 by the Supreme Court in the landmark case of Puttaswamy judgment marked a historic step toward safeguarding individual liberty and dignity. However, constitutional recognition alone is insufficient if the legal and institutional mechanisms required to enforce that right remain weak or outdated.

Comparative insights from the United States and the European Union demonstrate the importance of robust judicial oversight, transparent procedures, and independent regulatory authorities in maintaining the balance between national security and individual rights. For India, meaningful reform requires modern surveillance legislation, mandatory judicial authorization for monitoring activities, and stronger accountability mechanisms. Ultimately, preserving privacy is essential not only for protecting personal autonomy but also for sustaining the democratic values embedded in Article 21.