SECURING THE RIGHT TO PRIVACY AGAINST THE STATE SURVEILLANCE

Mohd. Faiz Khan, Research Scholar, Integral University

Abstract

This research paper gives an overview on right to privacy as a fundamental and human right of every citizen and the important aspects are being covered subject to restrictions imposed by state. Privacy as a fundamental right has been upheld by the apex court of the nation and the activities of state which violates this essential and basic right needs to be considered by the judiciary under their power of judicial review and judicial activism Data in today's society is used by the Big Tech companies to make millions of dollar and this trade of data undermines the basic right of citizens who do not want their nasty algorithm to affect the privacy of citizens. A number of cases has been heard by judiciary and the landmark judgments have provided for protection of right to privacy. Article 21 of Indian constitution has a very wide scope and the intent of the framers of the constitution when they framed this article was not to limit its applicability to life and liberty but also cover various other facets of it. This paper will further provide a comprehensive analysis on right to privacy in India.

Introduction-Right to Privacy(RP) :Preface

It is difficult to grasp what privacy and the right to privacy mean. Natural rights theory is used to support privacy, which in general adapts to new information and communication technology. The right to privacy gives us the freedom to decide which parts of this domain can be accessed by others and to manage the scope, mode, and timing of the use of those parts we choose to disclose. This domain includes everything that is a part of us, including our body, home, property, thoughts, feelings, secrets, and identity.

"The condition or state of not being subject to public notice to intrusion into or interference with one's conduct or decisions" is what privacy refers to.Right to privacy is the same as "Right to self-determination.A person's and their property's right to be shielded from unwelcome public attention or exposure.In contrast, invasion of privacy is defined as "an unauthorised use of one's personality and interference into one's private affairs." Privacy is often used interchangeably with the "right to be alone."

Indian law is quite adaptable. It functions in accordance with societal demands. The acknowledgement of rights in our nation is a result of numerous changes in the political, economic, and social spheres. Our constitution has granted us a number of rights that cannot be expressed in words, but the Honorable Supreme Court upholds them nonetheless.

"The common law has a tendency to expand along with society's expanding requirements. By that point, it had been realised that in addition to physical security, spiritual security, as well as security of the heart and mind, was also necessary."[1] The Indian Constitution's Article 21 guarantees our right to life, liberty, and the pursuit of happiness, and it acknowledges that this right also includes the right to privacy.

Statement of Problem

This study aims to provide clarity on the debate surrounding India's right to privacy. This research paper outlines the development of the right to privacy and numerous other aspects of it. The right to privacy cannot be seen as being unrelated to Article 21 because it is an essential part of the right to life and liberty, as has been repeatedly stated.

Objective

The purpose of this study is to shed light on the controversy surrounding India's right to privacy. This research paper describes the history of the right to privacy as well as a number of its other facets. The right to privacy is an essential component of our lives and various judgments have upheld the same. The aim of this research paper includes covering the historical judgments and relevant statutes and committees and provide a comprehensive analysis on the same.

[1] Lachmayer, K. and Witzleb, N., 2014. The challenge to privacy from ever increasing state surveillance: a comparative perspective. UNSWLJ, 37, p.748.

 DOI : 10.36893.DRSR.2022.V12I10N03.121-126

Review of Literature

1. Bhatia, G., 2014. State surveillance and the right to privacy in India: A constitutional biography. Nat'l L. Sch. India Rev., 26, p.127.
2. Chatterjee, S., 2019. Is data privacy a fundamental right in India? An analysis and recommendations from policy and legal perspective. International Journal of Law and Management.
3. Basu, S., 2010. Policy-making, technology and privacy in India. Indian JL & Tech., 6, p.65.
4. Kumaraguru, P. and Cranor, L., 2005, May. Privacy in India: Attitudes and awareness. In International workshop on privacy enhancing technologies (pp. 243-258). Springer, Berlin, Heidelberg.
5. Tripathi, S. and Tripathi, A., 2010. Privacy in libraries: The perspective from India. Library Review, 59(8), pp.615-623.
6. Gupta, A., 2010. Balancing online privacy in India. Indian JL & Tech., 6, p.43.
7. Das, I., 2021. Is Privacy Negotiable?: A Critical Analysis of Right to Privacy in India. Issue 2 Int'l JL Mgmt. & Human., 4, p.1660.
8. Nair, S., George, C.A. and Banerjee, N., 2022. Historical Analysis of Right to Privacy. Journal of Legal Studies & Research, 8(3), pp.112-126.
9. Verma, A., 2021. Counterbalancing the Right to Privacy and State Surveillance in India.

Research Methodology

This research offers a thorough examination of Indian law by examining the causes, consequences, and connections between them. It operates in line with societal expectations. Many changes in the political, economic, and social sectors contributed to the recognition of rights in our country. In this study, only secondary data were employed. It is important to consider the functions and duties of the executive, legislative, and judicial branches in order to assess the right to privacy and take appropriate action to protect it.

Constitutional protection of Right to Privacy

The Supreme Court's extension of Article 21's scope in the post-Maneka era is a highly intriguing development in Indian constitutional law. According to the Supreme Court, Article 21 is the foundation of the Fundamental Rights. Article 21 has shown to have many facets. Giving the words "life" and "liberty" in Article 21 a wider connotation has allowed for the expansion of its parameters. It is not appropriate to read these two words in Art. 21 narrowly. These are organic concepts that must be understood in their proper context.

According to the Supreme Court, a right need not be specifically identified as a fundamental right in the constitution in order to be treated as such. New rights are recognised as a result of the country's political, social, and economic changes. In its unending youth, the law develops to satisfy societal needs.

One such right that has emerged as a result of expanding the scope of Article 21 is the right to privacy. Private life is not specifically protected by the constitution as a right. However, the Supreme Court has taken such a right from Article 21 and several other constitutional clauses when they are interpreted in conjunction with the Directive Principles of State Policy.

No person "should be deprived of his life or personal liberty unless in accordance with the method prescribed by law," according to Article 21 of the Indian Constitution. “After reading Article 21, it has been determined that the term life refers to all those elements that contribute to a man's life being meaningful, complete, and deserving of being lived.”[2]

Like anything humankind has ever accomplished, there were both good and bad aspects to it. We cannot be certain whether what we say has been heard by a third party, whether that was desired or not, as technology has infiltrated every aspect of our lives, whether that invasion was desired or not.

[2] Bhatia, G., 2014. State surveillance and the right to privacy in India: A constitutional biography. Nat'l L. Sch. India Rev., 26, p.127.

 DOI : 10.36893.DRSR.2022.V12I10N03.121-126

Puttaswamy Judgement- The Magna Carta of Right to Privacy

In the historic case of KS Puttaswamy v. Union of India, often known as the Right to Privacy Judgement, a bench of nine Supreme Court of India judges unanimously determined that every citizen in India had a well-established and guaranteed right to privacy under the Indian Constitution. Additionally, the Supreme Court ruled that the Right to Privacy is just as important as the other Fundamental Rights enumerated in the nation's Constitution.

"Puttaswamy, a retired judge from the High Court, took the issue before the Supreme Court of India, raising concerns about whether it should be a requirement for all citizens in order to use government services and receive benefits. The Aadhar Scheme was proposed by the Indian Central Government (Uniform Biometrics Based Identity Card)."[3] The government maintained that the right to privacy was not expressly protected by the Constitution. According to the Court, privacy is a basic right or freedom protected by Article 21, which states that "No person shall be deprived of his life or personal liberty except in accordance with the method established by law."

The Central Government refuted this claim, claiming that the Indian Constitution does not give the right to privacy any particular or special protection or consideration. While the Supreme Court stated that privacy is essentially a necessary component of liberty and a fundamental freedom that are guaranteed to and accorded to every Indian citizen under Article 21 of the Indian Constitution

It was a historic decision that opposed laws on the consumption of alcohol and beef in various Indian states as well as same-sex laws, raising the bar for constitutionality challenges (i.e. LGBTQ). As a result, people began to anticipate that the Indian government would also pass legislation to safeguard individual privacy in addition to data protection. This sparked heated discussions on social media and news channels as Indians made fun of the government's actions by mentioning privacy laws and regulations in other nations around the world.

State Surveillance Activities violating Right to Privacy

In everyday speech, surveillance refers to seeing someone closely or being in a condition of observation. Different governments around the world, particularly in developed nations, employ a variety of tactics to monitor their citizens. "These kinds of actions are taken by governments to safeguard their nation from external dangers, to keep crime and criminals in check, to conduct investigations, etc. In today's technologically advanced times, surveillance includes watching over text messages, emails, phone calls, and CCTV footage, among other things."[4] Despite the fact that governments give a number of logically solid justifications for conducting surveillance operations, it is unquestionably a violation of privacy and personal data.

The Indian Government is now equipped with the most contemporary and up-to-date tools and mechanisms to conduct surveillance on its inhabitants at all levels through multiple agencies following decades of IT revolution. "For the purpose of monitoring its residents and gathering data about them, the government has developed and given authority to a number of agencies and ministries, including the Central Monitoring System and National Intelligence Grid."[5] We must read about the various government departments and agencies that carry out the functions of surveillance or are otherwise involved in the overall process if we are to properly comprehend the methods and systems of surveillance in India.

The Intelligence Bureau is responsible for the Central Monitoring System (CMS) (IB). It is its job to carefully examine every piece of information, including text messages, phone calls, online activity, social media posts, etc., when it is necessary to do so. The organisation that gave us the special identification number known as AADHAAR is called the Unique Identification Authority of India, or UID. We must recall the day when we gave the government our fingerprint and retina scans so they could create our AADHAAR cards in order to comprehend the level of information this agency has about itself.

Pegasus Issue, Adhaar data breach and others

"To leave well enough alone, you should likewise conceal it from yourself"-George Orwell, 1984

[3] Kamil, M., 2017. Puttaswamy: Jury still out on some privacy concerns?. Indian Law Review, 1(2), pp.190-204.
[4] West, S.M., 2019. Data capitalism: Redefining the logics of surveillance and privacy. Business & society, 58(1), pp.20-41.
[5] Bayer, R. and Fairchild, A.L., 2000. Surveillance and privacy. Science, 290(5498), pp.1898-1899.

 DOI : 10.36893.DRSR.2022.V12I10N03.121-126

High Court orders don't typically begin with statements from George Orwell, yet its request for 27 October 2021 on the Pegasus matter does. The main passage of India's top court's legal request likewise utilizes the term 'Orwellian': "The current group of Writ Petitions raise an Orwellian concern".
"It was through this request that the court designated a three-part board of trustees to test charges of utilizing a digital weapon and penetrating security of 100 Indian regular folks, some involving high established workplaces."[6] Assuming the discoveries of the worldwide examination in 'The Pegasus Task' are to be accepted, it makes India the world's greatest vote based system with the most uncontrolled and unrestrained utilization of the military-grade spying cyberware, which the Israeli firm has kept up with it sells just to government.
The group delivered a draught report in February, but its final recommendations have not yet been received. Pegasus, as it has come to be known internationally, represents one of the most heinous invasions of the owner's and the phone's privacy. The scandal has rocked the Israeli elite, and there are now significant doubts about the parent corporation, NSO.

Not Just 'Elite' People Have Privacy Concerns
The basic presumption that privacy is not associated with democracy or individuals' rights in the public imagination underlies the notion that the government may get away with this. It is dismissed as a 'elite' or specialist issue. Eric Schmidt, the former CEO of Google, likewise slyly encouraged this fallacy because it benefited his data-sucking enterprise. "Perhaps you shouldn't be doing it in the first place if you have something that you don't want others to know," he added.

Criminal Procedure(Identification) Act,2022 : Provisions violating Right to Privacy
The Criminal Procedure (Identification) Act, 2022, which was approved by the Parliament in April 2022, recently went into effect.
It replaces the Identification of Prisoners Act of 1920, a colonial-era statute that allowed police to measure suspects who had been convicted, detained, or were awaiting trial.It gives the police the legal authorization to collect bodily and biological samples from suspects and criminal defendants alike.
"The 1973 Code of Criminal Procedure (CrPC) section 53 or section 53A permits the police to gather data.Fingerprints, palm prints, foot prints, photographs, iris and retina scans, physical examinations, biological samples and their analysis are some of the data that can be gathered. Behavioural characteristics, such as signatures, handwriting, or other tests."[7]
The CrPC is the main piece of legislation governing how criminal justice is administered procedurally.A police officer or a prison official will request "measurements" from anyone who has been found guilty, arrested, or imprisoned in accordance with a preventive detention statute.
The National Crime Records Bureau (NCRB) will keep, protect, share, and delete the national record of measurements with any law enforcement agency. The records may be kept for up to 75 years.It strives to make sure that criminals can be uniquely identified and to assist law enforcement in case closure.
Privacy Violation: Although it may seem technical, the legislative plan violates everyone in India's right to privacy, not only those who have been convicted of a crime.It contains facilities for collecting samples from demonstrators participating in political demonstrations.

DNA Technology Regulation Law
The parliamentary committee on science and technology presented its report on the DNA Innovation (Use and Application) Regulation Bill, 2019. The reason for the bill is to direct the utilization of DNA data for laying out the character of individuals. These profiles are then intended to direct policing in examinations. The board of trustees has underlined that it is vital that cutting-edge advancements are utilized in the law enforcement framework, however this should be managed without encroaching established freedoms, particularly the Right to Privacy.

[6] Suresh, V., 2017. Scope of Personality, Celebrity or Image Rights in India in the Light of Landmark Judgement of Justice Puttaswamy's Case (2017). Celebrity or Image Rights in India in the Light of Landmark Judgement of Justice Puttaswamy's Case.
[7] Kumaraguru, P. and Cranor, L., 2005, May. Privacy in India: Attitudes and awareness. In International workshop on privacy enhancing technologies (pp. 243-258). Springer, Berlin, Heidelberg.
 DOI : 10.36893.DRSR.2022.V12I10N03.121-126

In spite of the fact that DNA innovation can help to police, in tackling violations, the public authority should alleviate fears over the utilization of the DNA Technology Bill, 2019.

Related Issues With the Bill

Infringement of Right to Privacy: There are reactions that the DNA profiling bill is an infringement of fundamental liberties as it could likewise think twice about the privacy of people.

Likewise, questions are being raised on how the bill intends to shield the security of DNA profiles put away in the databanks.

The DNA profiling bill follows an extensive rundown of bills being presented without the information security regulation set up.

Surveillance Actors : Secretly collecting users info, violating RP of the citizens.

Cybercriminals aim to obtain access to, alter, or remove private data for monetary gain, celebrity, personal vengeance, or to interfere with organisational operations . To carry out their attacks, these attackers take advantage of software flaws, employee inexperience and heavy workloads, as well as the diversity of security solutions used in a business. In this situation, businesses must create tactics that will enable them to withstand hostile attacks. Security mechanisms build defences and produce event logs that may be examined to spot and respond to potential intrusions. Security analysts can identify and respond to threats immediately by reviewing these logs as opposed to waiting weeks or months for a forensic investigation.

As a result, security logs are a vital instrument in the identification of attacks and data leakage. However, employing them presents a number of significant difficulties. “To identify anomalous components in a lengthy list of events, close attention to detail is necessary. Due to the enormous size of modern security logs, it is required to quickly examine a large amount of data.”[8] The complexity of log analysis is also influenced by the plurality of devices and systems in a modern corporate computer ecosystem, and consequently the heterogeneity of logs they produce.

Data Retention Policy - An apprehension of data breach

Like oxygen is to humans, data is to business.You risk dying if you don't have the correct quantity, which usually indicates your company will fail. But just as consuming too much oxygen may be fatal, so does consuming too much data.

Data retention for longer than necessary affects risk, adds expenses, and slows down how quickly an organisation can react to a breach. Data retention is a key component of your organization's incident response strategy, yet many fail to take this preventative measure to guard against damaging hacks, cyberattacks, and data breaches.

To totally erase data traces, businesses typically utilise data destruction software.

Need for the stringent Data Protection Law in India

Following demonetisation, the government has taken a timely and essential step to expand digital payment choices in an effort to eradicate corruption and black money from public life.

“The quality of life for individuals will change as a result of these measures, which are an essential component of the government's plan to move the nation toward a totally cashless economy. The need for a solid legal framework for privacy and security of data shared by individuals and entities is one area that requires immediate attention.”[9] Because legislative changes take longer than technology advancements, there is uncertainty about the viability of rights.

As a result, concurrent legislative revisions would be necessary as part of the programme for digitisation.Careful consideration must be given to the legal rights and obligations resulting from the management of data pertaining to individuals and entities. The IT Act, 2000 and the guidelines that follow it currently govern India's current data protection and privacy environment.

[8] Gupta, A., 2010. Balancing online privacy in India. Indian JL & Tech., 6, p.43.

[9] Das, I., 2021. Is Privacy Negotiable?: A Critical Analysis of Right to Privacy in India. Issue 2 Int'l JL Mgmt. & Human., 4, p.1660.

 DOI : 10.36893.DRSR.2022.V12I10N03.121-126

"The law governing data protection is embodied in Sections 43A, 69, and 72A of the IT Act. A law with a narrow emphasis, The Personal Data Protection Bill, 2014, was introduced in Parliament in 2014."[10]
The Indian Contract Act, 1872's legal framework, which takes the form of contracts, protects one's rights in the event that private rights are violated because these provisions are so modest.Every time a new piece of technology is developed, misuse and fraud techniques likewise advance. India lacks a specific data protection law, unlike nations like the UK, Australia, and other European nations.
The right to data protection may be included in the list of fundamental rights even if it is not mentioned in the Indian Constitution directly.

[10] Westin, A.F., 1966. Science, privacy, and freedom: Issues and proposals for the 1970's. Part I--The current impact of surveillance on privacy. Columbia Law Review, 66(6), pp.1003-1050.

 DOI : 10.36893.DRSR.2022.V12I10N03.121-126