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

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur.Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time &Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

 ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

DIGITAL PRIVACY IN INDIA: THE NEED FOR PROTECTION IN A DATA-DRIVEN SOCIETY.

AUTHORED BY: RIDA FATEMA MOLEDINA

ABSTRACT:

Privacy is not an alienated concept in India moreover it is a deep-rooted custom of the rich cultural heritage of India. The provision of the right to privacy is governed by *Article 21* of the Indian constitution. The provision of *Article 21* says that no person shall be deprived of his *life* or *personal liberty* except according to the procedure established by law.

The concept of privacy is not new in society. A past analysis of *history* gives an adequate amount of evidence that shows that privacy prevailed as a *social value* in every *civilization.*

Keywords: privacy, Article 21, life, personal liberty, history, social value, civilization.

INTRODUCTION:

The concept of privacy can be traced back to ancient Hindu texts. In Hitopdesha it says that certain issues like worship, sex, and family matters should be protected from disclosure.

गोपनीयं गोपनीयं रहस्यं कथयेद्धि यः। स सर्वत्र वधं याति यथा गन्धः शुचौ जले॥"

(Book 1, Verse 3)

Translation: *"One who reveals a secret is destroyed everywhere, just as fragrance is lost in clean water."*

The word privacy is derived from the word '*Privatus'* which means separated from the rest. Thus, the word 'privacy' entails the sense of something belonging to oneself, something that the individual would not want to share with others.

The first attempt to define privacy was made in 1890 by Warren and Brandy in the article 'Right to privacy' in which they defined privacy as the right to be left alone.

How privacy is protected online is one of the most pressing issues of our time.

 ISSN: 2582-6433

Aadhaar and the Right to Privacy:

The Aadhaar system, launched in India as a unique identification project, has ignited significant debates about the balance between state objectives and individual rights, particularly the right to privacy. By centralizing a multitude of personal data into a single, accessible database, Aadhaar poses considerable privacy risks, especially in a world where technology is increasingly integrated into everyday life. Here are some examples that illustrate these concerns further:

1. Consolidation of Personal Data and Its Risks:

Aadhaar consolidates a person's demographic details, biometric data (fingerprints and iris scans), and other personal identifiers into a centralized database. This aggregation of data creates the potential for unprecedented surveillance. Currently, information such as voter IDs, PAN numbers, or ration cards is maintained by separate governmental entities. However, Aadhaar merges all these into one, creating a unified, highly detailed profile of each individual. The fear is that, with breach or misuse, this data could be exploited for surveillance, identity theft, or even social manipulation.

Example: If an individual's Aadhaar details were leaked or accessed maliciously, personal information such as income, addresses, and transaction history could be pieced together by cyber criminals. This could lead to targeted fraud or even unauthorized access to banking and government services.

2. Biometric Data and Privacy Infringement:

One of the most significant concerns surrounding Aadhaar is the use of biometric data (fingerprints and iris scans). Biometric data is inherently permanent and unique to each individual. Unlike passwords or PINs, biometrics cannot be changed if compromised, making any leak of such data especially harmful.

Example: In 2018, reports surfaced about the unauthorized access to biometric data of several Aadhaar holders. In one instance, hackers allegedly sold Aadhaar data, including fingerprints, to private agencies, raising concerns about misuse. The fact that biometric data cannot be reset like a password or credit card number makes this a particularly dangerous form of privacy violation.

3. State Surveillance and the Creation of a "Surveillance State":

The centralization of sensitive personal data through Aadhaar also increases the risk of a surveillance state. Governments could potentially use the Aadhaar database to track citizens'

 ISSN: 2582-6433

movements, behavior, and patterns, leading to concerns about state overreach. When Aadhaar is linked with various services such as mobile phones, bank accounts, or social welfare schemes, it becomes easier for authorities to monitor individuals continuously.

Example: In countries with authoritarian regimes, centralizing data in one system can be used to track individuals' activities, location, and even their political preferences. While the Indian government claims that Aadhaar is used to deliver better services to citizens, there is growing concern that the data could be misused by authorities to suppress dissent or target specific groups.

4. Data Privacy and Cybersecurity Risks:

As more services in India shift to digital platforms, the collection of personal data is becoming a central part of interactions with the government. However, the rapid digitalization of India comes with cybersecurity vulnerabilities. Sensitive information is increasingly being stored and transferred online, which can expose individuals to risks like data breaches, hacking, and misuse of their private information.

Example: In 2017, there were multiple reports of data leaks from government agencies, which were linked to Aadhaar. Such leaks could expose critical information about individuals, leading to identity theft or unauthorized financial transactions. Additionally, there are fears about how Aadhaar data could be targeted in international cyberattacks, especially regarding its potential use in elections or political campaigns.

5. The Role of the Judiciary and Legislative Action:

The recognition of the right to privacy as a fundamental right by the Indian Supreme Court, through its landmark 2017 judgment, shifted the legal framework on privacy. Previously, privacy was not explicitly defined as a fundamental right under India's Constitution, but this decision reinforced the notion that privacy is intrinsic to human dignity and liberty. If the right to privacy were to be weakened by a future ruling or lack of proper safeguards, individuals would have limited legal recourse if their privacy is violated.

Example: The case of *K.S. Puttaswamy vs. Union of India* (2017) illustrated the Supreme Court's shift in recognizing privacy as a fundamental right. Despite this, Aadhaar remains controversial, as many believe the system fails to sufficiently protect citizens' data. If legal frameworks are not updated to reflect contemporary privacy concerns, people could remain vulnerable to the misuse of personal data.

 ISSN: 2582-6433

6. Digital Age and Increasing Reliance on Aadhaar:

With the growing adoption of digital technology in both the public and private sectors, the need to safeguard privacy becomes even more crucial. Initiatives like the Digital India program and the push for cashless transactions rely heavily on digital identity systems like Aadhaar. The move to a cashless, paperless economy hinges on the availability of an efficient identification system, but this also makes the need for robust privacy protections more pressing.

Example: In the digital era, where financial transactions, government subsidies, and access to healthcare are linked to an individual's Aadhaar number, any breach of the system can potentially affect millions of people. The case of fraudulent financial transactions through compromised Aadhaar numbers shows how breaches can extend beyond simple data theft, affecting real-world financial stability.

7. The Need for Legislation to Address Privacy Concerns:

While the Supreme Court has affirmed the right to privacy, there remains an urgent need for legislation that can provide clarity on the scope of privacy protections in the age of digital surveillance. This legislation would need to define the limits of data collection, impose strict penalties for data breaches, and ensure transparent practices by government agencies and private corporations that handle Aadhaar-linked data.

Example: The *Personal Data Protection Bill*, of 2019, proposed measures to protect the privacy of Indian citizens, but there are still concerns about provisions within it that could potentially dilute privacy rights. While the bill could strengthen privacy protections, its passage and enforcement remain critical to safeguarding the digital rights of citizens in the future.

The Aadhaar system is one example where privacy concerns are significant, but there are several other situations, technologies, and initiatives globally that also raise similar issues regarding the balance between privacy and technology or governance, they are as follows:

8. Facial Recognition Technology:

Facial recognition technology, used by governments and private entities for identification and surveillance, has sparked privacy concerns due to its ability to track individuals without their consent. It can be used in public spaces, such as airports, malls, and even on the streets, to identify people in real-time, leading to concerns about constant surveillance and the erosion of anonymity.

Example: In China, the government has employed facial recognition in public places for a variety of purposes, including identifying and tracking people associated with certain behaviors

 ISSN: 2582-6433

(like protesters). While it is argued that this technology helps with security and law enforcement, it also raises concerns about excessive state surveillance, particularly in authoritarian contexts. In other countries, such as the US and UK, facial recognition is being used by law enforcement agencies for crime prevention but has been criticized for its potential to infringe upon individual rights.

9. Social Media and Data Privacy:

Social media platforms like Facebook, Instagram, and Twitter collect vast amounts of personal information from users, often without their full understanding of how this data will be used. From location data to personal interests and relationships, these platforms have a wealth of information that can be exploited for advertising purposes, influencing elections, or even selling user data to third parties.

Example: The Cambridge Analytica scandal, where Facebook data of millions of users was harvested without their consent and used for political profiling and targeted ads, demonstrates the risks associated with social media platforms handling sensitive data. Although Facebook took some corrective measures after the scandal, concerns remain over how these platforms collect and use data without transparent consent from users.

10. Smart Home Devices (e.g., Amazon Alexa, Google Nest):

Smart home devices, such as voice assistants (Amazon Alexa, Google Assistant), smart speakers, and security cameras, collect a large amount of personal data to function effectively. These devices are constantly "listening" to conversations, collecting voice commands, and even monitoring behaviors in your home. While marketed as a way to improve convenience, the information they collect may be shared with third-party companies or even stored and used for data profiling.

Example: In 2019, it was revealed that Amazon employees had access to Alexa voice recordings to help improve the device's accuracy. While users are notified when they're using the device, many people are unaware of the extent of data collection and the potential for their private conversations to be accessed by external parties. Similarly, security cameras and smart doorbells can be hacked, giving cybercriminals unauthorized access to sensitive footage.

11. Google and Location Tracking:

Google's ability to track and store user location data through its maps, search, and other services has raised privacy concerns. Despite the company claiming to anonymize the data, it has been

 ISSN: 2582-6433

revealed that the data is often not fully anonymized, and users can be identified and profiled based on location patterns.

Example: In 2018, the Associated Press reported that Google continued tracking users' locations even after they had turned off location history. This discovery raised questions about whether users are fully informed of the extent to which their location data is being tracked. As smartphones increasingly serve as tracking devices, there are growing concerns about the scale of surveillance these companies can engage in without consumers' explicit consent.

12. Surveillance Capitalism:

The concept of "surveillance capitalism" refers to the business model employed by companies like Google, Facebook, and Amazon, which gather and monetize vast amounts of personal data. These companies often trade or sell data to third parties, while users are often unaware of the full extent to which their data is being used for profit. This results in a loss of control over personal information and the ability to make decisions about what is shared and with whom.

Example: Many mobile apps require access to a user's contacts, photos, location, and other private information in exchange for a free service. While the apps may not be malicious in intent, they often share this data with advertisers or data brokers, leading to a constant stream of personalized ads, and sometimes even influencing users' opinions and behaviors. The practice has raised significant privacy concerns about consent, transparency, and the right to control personal data.

13. DNA Databases and Genetic Privacy:

As DNA testing and genetic data collection have become more popular, privacy issues have emerged regarding who controls this sensitive information. While genetic testing services like 23andMe and Ancestry.com provide users with insights about their genetic traits, these companies have vast amounts of highly sensitive data about users' health, ethnicity, and family history.

Example: The controversy surrounding the use of genetic data by law enforcement highlights potential privacy risks. In the case of the Golden State Killer, investigators used public genetic databases to find a match to DNA collected from crime scenes. While this led to the identification and arrest of a serial killer, it also sparked debates about whether genetic information, even if submitted voluntarily for ancestry purposes, could be used for criminal investigations without proper consent.

 ISSN: 2582-6433

14. Healthcare Data and Privacy:

The digitalization of healthcare records has brought immense benefits, like improving patient care and reducing costs. However, it also poses significant privacy risks. As healthcare data becomes more digitized and shared across multiple platforms, there are increased concerns about how this sensitive information is stored, who has access to it, and how it can be misused.

Example: In 2017, the WannaCry ransomware attack targeted NHS hospitals in the UK, encrypting patient data and disrupting healthcare services. The attack exposed vulnerabilities in the healthcare system, showing how hackers could potentially exploit patient records for financial gain. While cybersecurity measures have improved, many people remain concerned about the long-term safety of their health data, especially if it is accessible by multiple parties, including insurance companies, pharmaceutical firms, and healthcare providers.

15. Public CCTV Surveillance:

Governments and cities worldwide have implemented public surveillance cameras in the name of security, but these raise significant privacy concerns. Public CCTV can track citizens' movements in real-time, potentially infringing on individuals' right to anonymity. The stored footage can also be accessed by government or private entities, posing the risk of misuse.

Example: In the UK, which has one of the highest densities of CCTV cameras, there are concerns about the constant monitoring of citizens. Though surveillance is justified as a means of improving public safety, critics argue that it erodes privacy rights, as it could lead to the unwarranted collection and sharing of personal data without consent, potentially creating a chilling effect on free expression and behavior.

CONCLUSION:

The concept of privacy, deeply embedded in Indian cultural and legal traditions, plays a crucial role in safeguarding individual rights and freedoms in contemporary society. As evidenced in ancient texts such as the *Hitopdesha*, privacy has long been considered an important value in Indian society, particularly in the context of personal and familial matters. The assertion that "*One who reveals a secret is destroyed everywhere, just as fragrance is lost in clean water*" underscores the profound respect for privacy and the harm caused by its violation. Modern India, despite its rapid technological advancements, must therefore address the pressing issue of privacy protection within the framework of evolving digital realities.

 ISSN: 2582-6433

The Indian Constitution's Article 21, which guarantees the right to life and personal liberty, forms the bedrock of privacy protection in the country. The 2017 Supreme Court judgment in the *Puttaswamy case* reinforced the notion of privacy as a fundamental right, marking a significant step in recognizing privacy as intrinsic to human dignity. Yet, as India becomes increasingly digitalized, balancing the objectives of state governance with individual privacy rights remains a critical challenge. The Aadhaar system, while designed to streamline access to services and ensure equitable distribution of resources, raises significant concerns about the centralization of sensitive personal data, the risks of surveillance, and the potential for misuse.

The Aadhaar system consolidates biometric data and other personal identifiers into a single, accessible database, which, if compromised, can lead to severe privacy infringements. Biometric data, being permanent and unique, presents an especially troubling risk. The 2018 reports of unauthorized access to Aadhaar data highlighted the vulnerability of such systems to misuse. Similarly, the use of Aadhaar to link multiple services heightens concerns about state surveillance and the creation of a "surveillance state," where individual movements and behaviors can be monitored without consent. This increasing centralization of personal data, while intended to improve efficiency, has raised alarms about the potential for overreach and the erosion of individual privacy.

Moreover, the growing reliance on Aadhaar for various public and private sector services amplifies the need for robust cybersecurity measures. Data breaches, such as those reported in 2017, underscore the vulnerabilities of digital systems and the potential consequences for individuals whose private information is exposed. As the country embraces initiatives like Digital India, which depend on the efficient handling of personal data, the risk of misuse escalates. Without strong safeguards and legal frameworks, the increasing digitization of public services could lead to unforeseen consequences, including identity theft, fraud, and the exploitation of personal data for malicious purposes.

Internationally, privacy concerns are not unique to India. Globally, the advent of technologies like facial recognition, social media data harvesting, and surveillance capitalism has raised alarms about the erosion of privacy. The use of facial recognition technology by governments and private companies, for instance, has sparked debates about surveillance without consent and the loss of anonymity in public spaces. Similarly, data collection practices by social media platforms have led to issues of consent and transparency, as highlighted by the Cambridge

 ISSN: 2582-6433

Analytica scandal. These developments further emphasize the global nature of privacy concerns and the urgent need for comprehensive legal protections to safeguard individuals' rights.

In response to these concerns, legislative measures like the Personal Data Protection Bill of 2019 seek to address the challenges posed by data privacy in India's digital age. However, ongoing debates about the adequacy of these laws and the potential for dilution of privacy protections suggest that much remains to be done to ensure comprehensive safeguards. The legal framework must be continually updated to reflect the evolving nature of privacy risks, considering technological advancements and their impact on individuals' rights.

The balance between ensuring the efficient delivery of services and protecting citizens' privacy is a delicate one. While systems like Aadhaar offer convenience and efficiency, they also necessitate heightened vigilance to ensure that privacy is not compromised. In the digital age, where personal data is increasingly commodified, protecting privacy is not just about limiting access to information but also ensuring that individuals have control over how their data is used and shared. Privacy, as a fundamental human right, must be upheld through a combination of strong legal frameworks, technological safeguards, and ethical considerations. Only through a robust and forward-thinking approach can we navigate the complexities of privacy in an increasingly interconnected world.

BIBLIOGRAPHY:

1. https://indianexpress.com/article/india/supreme-court-aadhaar-verdict-some-right-to-privacy
2. Constitution of India (1950). Article 21: "Protection of Life and Personal Liberty."
3. Aadhaar and Privacy Concerns: A Study by the Centre for Internet and Society (CIS), 2017. https://cis-india.org/@@search?Subject%3Alist=Aadhaar
4. K.S. Puttaswamy (Retd.) vs. Union of India (2017) https://indiankanoon.org/doc/127517806/
5. Hitopadesha (Book 1, Verse 3), composed by Narayanan in the 12th century.