

# INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary  
Peer Reviewed

[www.ijlra.com](http://www.ijlra.com)

## DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.  
All rights reserved.**

## 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IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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.

## ***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.

# **PRIVACY UNDER THREAT IN THE DIGITAL ERA: A HUMAN RIGHTS PERSPECTIVE**

AUTHORED BY - SRINKA DAS

## **ABSTRACT**

The modern society has completely changed because of the 21st century's rapid development of digital technologies. At the same time, it has also posed some threats for the protection of human rights and individual's privacy by AI, surveillance technologies, large number of data collection by multinational companies and governments. There are significant concerns regarding misuse and security of data because this large number of data collection happens without the consent of the consumers. Privacy is considered as a fundamental human rights. Despite various protections, digital monitoring techniques increase threats to civil liberties.

While companies gather massive data for commercial purposes, governments also justify digital monitoring under the pretext of national security. Individual's freedom of expression, democratic participation are threatened because of these practices. This paper provides a critical analysis of how various laws and judicial rulings protect privacy rights. That's why strong laws, independent regulatory bodies, fair practices should be needed to tackle this ongoing issue.

## **KEYWORDS**

Digital Privacy right, Human Rights, Surveillance, Digital Technologies, Data Protection, Legal Safeguards.



## I. INTRODUCTION

**“All human beings have three lives: public, private and secret.”<sup>1</sup>**

**- Gabriel Garcia Marquez**

Privacy is not just an option; it is a basic human right that is essential for both human dignity and individual's freedom. Since, personal information is continuously monitored through various platforms that's why it is important to protect privacy rights specially in the technological advanced era. Although Indian constitution does not provide any definition of 'privacy' but it is recognised as a part of article 21 of the Indian constitution. It has also been interpreted by the judiciary.

In the technological advanced era, various technologies like AI, location tracking has transformed everyone's life by improving efficiency. But these advancements create threats of data breaches, identity theft, unauthorised digital monitoring. While various legal measures were introduced to maintain the digital ecosystem in spite of that this matter became a serious issue for now a day.

This paper critically analyse privacy right from the human rights perspective also focuses on the need for strong legal structure, proper implementation, and better public awareness.

### A. RESEARCH PROBLEM

The ongoing technological advancement has created major challenges for the protection of individual's privacy. Now a days, Governments and private companies use a variety of digital platforms, social media, internet services to gather and store large numbers of personal information. This massive data collection often occurs without the consent and full awareness of individuals, raising major concerns about constant surveillance and misuse of personal information. However, GDPR in the European Union provide strong safeguards for personal data, but many countries still lack extensive privacy laws or effective enforcement mechanisms. Additionally, international exchange of data and the global operations of multinational corporations make it even more difficult for the national governments to protect and regulate individuals' data effectively. These developments create various problems related to weak legal protection, unregulated data collection, lack of public awareness, and the challenge of

---

<sup>1</sup> <https://theamikusqrae.com/privacy-rights-in-digital-age/> (last visited on March 2, 2026).

controlling multinational corporations over digital spaces. As a result, the protection of personal freedom, human dignity, and fundamental rights is under threat. That's why it is necessary to examine how stronger human rights policies and frameworks can safeguard individual's privacy.

## **B. RESEARCH OBJECTIVES**

The main purpose of this paper is to comprehend how individual's privacy is under threat in the technologically advanced era and how human rights policies can help individual to protect their privacy in the technologically advanced environment.

**Thus, this paper is primarily intended:**

- To analyse privacy as a fundamental human right at national and international level.
- To examine how digital technologies create threat on individual's privacy in the modern digital age.
- To study the effectiveness of existing data protection policies and laws, including regulations, in safeguarding right to privacy.
- To identify various challenges created by multinational corporations and cross-border data flows in protecting citizens' right to privacy.
- To suggest various legal and policy measures for strengthening privacy protection while balancing the technological development and innovation.

## **C. HYPOTHESIS**

This paper hypothesizes that the ongoing development of digital technologies, global data flows and data-driven platforms has significantly increased threats to individual privacy in the digital environment. Although privacy right is recognized globally as a basic human right. The existing legal frameworks are often insufficient to protect individuals' privacy effectively from surveillance, misuse of personal data and unauthorized data collection. Therefore, stronger legal protections, improved data protection policies are essential to ensure individual's privacy in the digital era.

## **D. RESEARCH METHODOLOGY**

The research method applied in this study is fully doctrinal. The study also focuses on secondary sources like research articles, books, legal documents and court judgments. Doctrinal research focuses on legal propositions and doctrines. This doctrinal method is based

on the analytical and critical examination of statutes, their inter-relationships, and the interpretations made by the Indian judiciary.

## E. RESEARCH QUESTIONS

1. How does surveillance and massive personal data collection by governments and multinational corporations create threat to privacy right in the digital era?
2. How does informed consent, inadequate public awareness and transparency in digital platforms contribute to the misuse and exploitation of personal data?
3. Why do various legal and policy frameworks across different countries fail to effectively protect individuals' privacy?
4. How far does technological innovation conflict with the protection of human rights?

## F. LITERATURE REVIEW

1. This article<sup>2</sup> argues that although privacy is firmly recognized in international law, it is increasingly weakened by large-scale data practices and digital surveillance. It focuses the gap between traditional legal protections and rapidly emerging technologies which creates serious ethical concerns. Moreover, global frameworks must be updated to effectively tackle privacy related challenges of the digital era.
2. This book<sup>3</sup> provides a detailed framework of human rights entrenched in international law, emphasizing liberty, dignity, and equality. It explains privacy right as a basic human right under UDHR and ICCPR.
3. "Indian Constitutional Law" by M. P. Jain is a timeless classic text<sup>4</sup> on Indian constitutional law. It offers a detailed explanation of the principles, structure, and functioning of the Constitution, supported by important Supreme Court judgments and comparative perspectives. The book is divided into seven parts with forty-five chapters. It gives particular emphasis to Fundamental Rights, especially Article 21, explaining its judicial interpretation and wide scope. The author explains how Article 21 has evolved to include various aspects of life and personal liberty.

---

<sup>2</sup> Brahimi Smail, "The Erosion of the Right to Privacy in International Law: Legal and Ethical Implications in the Digital Age" 14 Journal of Law, Society and Authority (2025).

<sup>3</sup> Dr. H.O. Agarwal, International Law & Human Rights (Central Law Publications, Allahabad, 23<sup>rd</sup> edn, 2021).

<sup>4</sup> Mahabir Prashad Jain, Indian Constitutional Law (Lexis Nexis, 7th edn, 2014).



## II. CONCEPTUAL FRAMEWORK

### MEANING OF PRIVACY

Privacy means individuals' ability to keep their valuable information, activities and relationships private. Privacy means every person has the right to protect their privacy.<sup>5</sup> It also helps to control how an individual's personal data is collected, stored, and shared digitally. UDHR<sup>6</sup> and ICCPR<sup>7</sup> recognized privacy as a fundamental human right. It comprises a distinction between the private and public life, an idea explained by the great philosopher Aristotle. It means that the personal and family matters should be protected from any unnecessary interference by state.

### CONCEPT OF DIGITAL PRIVACY AND DATA PRIVACY IN THE DIGITAL AGE

Digital privacy means the ability of a person to control and protect their activities, personal information, when they use various digital technologies. It also ensures that every person should have the liberty to decide what information about them is collected, who can access it, how the information is used, and how long it is stored. Digital privacy assures that every person's personal data is not accessed, shared or monitored without their consent. Digital technologies help individual to share information, access education, express opinions, and advocate for their rights. However, digital advancements also create risks like censorship, surveillance, online harassment, data breaches, which may violate individual rights.<sup>8</sup>

In our day-to-day life, Data is created everywhere. Mainly, there are two types of data- 1. The data we give willingly and 2. The data that is automatically created when we perform some activities. Due to the availability of the internet and technological advancements, data has become like a new type of currency. But it is unfortunate that most people do not fully realize the value of their data. But many multinational companies are ready to pay to access this data so that they can flourish their business.

### PRIVACY AS A HUMAN RIGHT AND DIGITAL SURVEILLANCE

Now a days, privacy has become an integral part of our life, especially in the digital age. That's why it is important to protect individual's privacy right. It means that individual's privacy should be protected from any unwanted interference related to their personal information and

---

<sup>5</sup> Ms. Aishwarya Pandey, "Right to Privacy in the Digital Age: Constitutional Implications in India" 32 ISSN 3 (2024).

<sup>6</sup> Universal Declaration of Human Rights, 1948, Art. 12.

<sup>7</sup> International Covenant on Civil and Political Rights, 1966, Art. 17.

<sup>8</sup> <https://share.google/v5sKOTO9zcb46yzrt> (last visited on March 5, 2026).

personal life. UDHR<sup>9</sup> and ICCPR<sup>10</sup> recognized privacy as a basic human right, which say that right to privacy must be respected and protected by law. Privacy has different dimensions. It includes “physical privacy (protection from bodily intrusion), privacy related to information (control over individual’s personal data), and decisional privacy (freedom to make own choices)”. These dimensions are crucial for personal freedom and human dignity.

In the digital era, surveillance has become a constant part of everyone’s life through various technologies. Governments and private companies collect and analyse large-amount of personal data through facial recognition, biometric identification, and online tracking. While the main aim of these tools is to improve services, security, and efficiency. But most of the time, they do not maintain transparency as well as they operate without the full consent. The widespread of surveillance raises serious concerns.<sup>11</sup>

### **III. RIGHT TO PRIVACY: HISTORICAL PERSPECTIVE AND EVOLUTION**

#### **HISTORICAL DEVELOPMENT**

##### **Ancient Period (Up to 500 AD)**

In ancient time, privacy was all about keeping personal affairs hidden. The wealthy people had more to protect, while common people had few rights or property. Social norms and gossip helped to regulate behaviour, but privacy was not formally recognized as a right. Roman, Greek, and Indian traditions, including books (Dharmashastras and Arthashastra) strengthen domestic and personal boundaries, demonstrating early awareness of individual privacy.<sup>12</sup>

##### **Medieval Period (500 – 1800 AD)**

During the medieval period, the main focus was on human rights rather than privacy. Cultural practices, and legal documents like the Magna Carta, the Declaration of 1789<sup>13</sup> and the Bill of 1689<sup>14</sup> protected personal space and security. Though right to privacy was not explicitly codified, but individuals tried to safeguard the personal matters from governmental or public interference.<sup>15</sup>

---

<sup>9</sup> Supra note 6.

<sup>10</sup> Supra note 7.

<sup>11</sup> Dr. Vinayaka. K, “Digital Surveillance Vs. Right To Privacy: A Human Rights Perspective” 3 ISSN 2-3 (2025).

<sup>12</sup> Varun Pratap Singh Bhakuni & Dr. Nalnish Chandr Singh, “Historical Perspective on Privacy Rights and their Evolution in the Digital Era” 12 ISSN 4-5 (2025).

<sup>13</sup> French Declaration of the Rights of Man (1789).

<sup>14</sup> English Bill of Rights (1689).

<sup>15</sup> [https://www.nyulawglobal.org/globalex/right\\_to\\_privacy\\_international\\_perspective.html](https://www.nyulawglobal.org/globalex/right_to_privacy_international_perspective.html) (last visited on March 6, 2026).

### **Modern Period (1800 AD- Present)**

In the modern period due to the technological advancements, right to privacy became a formal legal concern. In the U.S., Warren and Brandeis's 1890 work and subsequent developments highlighted threats from surveillance, media, and electronic communication. Various laws and case laws gradually recognized privacy as a basic right. But new technological advancements create threats on privacy. Moreover, threats between individual privacy and public access persists today also.<sup>16</sup>

### **THE EVOLUTION OF RIGHT TO PRIVACY IN INDIA**

Although the Right to Privacy recognized as a Fundamental Right by the Supreme Court of India only in the last nine years but the concept has its deep historical roots. Ancient Indian texts (Dharma shastras, Ramayana, Manu smriti, Mahabharata, Upanishads, and Artha shastra) strengthened personal privacy in the matters of family, worship, and household affairs. As well as king were also bounded to uphold these protections.<sup>17</sup>

During the 19th and early 20th centuries, Indian laws like The Bill of 1895<sup>18</sup>, the Bill of 1925<sup>19</sup>, and the Report of 1928<sup>20</sup> also began to recognize the inviolability of the home and personal property which was associated with privacy. Privacy was not recognized as a fundamental right in the Indian constitution that's why during the Constituent Assembly (1946–1949) debates, Dr. B. R. Ambedkar tried to include it, but his proposal did not receive sufficient support.

Later on, the highest Court of India addressed privacy right through various landmark cases. In a case<sup>21</sup> emerged that Article 21 includes privacy right within the ambit of life and liberty, gradually establishing it as a constitutional principle.

### **IV. INTERNATIONAL PERSPECTIVES OF PRIVACY**

The threats regarding digital surveillance and privacy right became a global concern, varying across countries based on various laws, political priorities, and governance systems.

**United States:** In the United States, privacy is linked to the constitutional rights, yet creating concerns over national security have led to expanded surveillance. After the September 11 attacks, laws such as the USA PATRIOT Act increased monitoring powers of the government,

---

<sup>16</sup> Ibid.

<sup>17</sup> Supra note 12.

<sup>18</sup> Constitution of India Bill 1895.

<sup>19</sup> Commonwealth of India Bill 1925.

<sup>20</sup> Nehru Report 1928.

<sup>21</sup> Govind v. State of M.P. (1975) 2 SCC 148.

many of which operated secretly. The disclosures by Edward Snowden revealed large amount data collection by the National Security Agency in 2013, including activities that accessed citizens' data from major tech firms. Although reforms like the USA FREEDOM Act limited surveillance practices continue under broad security claims. Additionally, the U.S. does not have a single strong data protection law. They still rely on some fragmented sector-based regulations (like HIPAA and COPPA), which leaves significant gaps in privacy protection.<sup>22</sup>

**Europe:** In digital privacy protection, the European Union is considered a global leader. In 2018, it introduced the GDPR to protect personal data. The GDPR requires user consent and it grants some rights such as data portability and the right to be forgotten. It also applies to foreign companies handling EU citizens' data. However, it failed to protect data. In the Schrems II case (2020), the Privacy Shield agreement with the U.S. was declared invalid due to concerns over U.S. surveillance laws. As a result, international data transfers and data security continue to be important issues.<sup>23</sup>

**China:** In China, digital monitoring has become an essential part of governance. The government uses advanced technologies. Social Credit System evaluates citizens' behaviour regarding everything. In China, Surveillance is normalized as a tool for maintaining order and political control. However, this approach has created serious human rights concerns.<sup>24</sup>

## INTERNATIONAL FRAMEWORK FOR PRIVACY PROTECTION

The right to privacy was first recognized internationally by the Universal Declaration of Human Rights (1948). Since then, various international instruments especially those developed under the OECD and the United Nations have included some provisions related to privacy.

### UDHR, 1948

The UDHR is the first instrument of UN to treat privacy as a fundamental human right. According to Article 12 of UDHR: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."<sup>25</sup>

---

<sup>22</sup> Supra note 11.

<sup>23</sup> Supra note 11.

<sup>24</sup> Ibid.

<sup>25</sup> Universal Declaration of Human Rights, 1948 (adopted by the United Nations General Assembly on 10 December 1948).

### **ICCPR, 1966**

The ICCPR also strengthened the protection of privacy through Article 17. Article 17 affirms that “No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”<sup>26</sup>

### **The CRC, 1989**

The UN General Assembly adopted the Convention on the Rights of the Child (1989). It protects children’s rights, including their right to privacy. Article 16 of the CRC affirms that “No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation. The child has the right to the protection of the law against such interference or attacks.”<sup>27</sup>

### **International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, 1990**

It Protects migrant workers’ privacy by prohibiting unlawful interference with their personal life.

### **Personal Data Protection and Privacy Principles, 2018**

It Provides a modern framework for fair data processing within UN bodies, aiming to harmonize and strengthen the protection of privacy.

### **OECD Privacy Guidelines, 1980**

First major international effort to standardize data privacy principles. But it is voluntary in nature and not legally enforceable.

### **Revised OECD Privacy Framework, 2013**

It addresses modern digital risks, strengthening national strategies and breach notifications, though remains non-binding.

---

<sup>26</sup> International Covenant on Civil and Political Rights, 1966 (adopted by the United Nations General Assembly on 16 December 1966).

<sup>27</sup> Convention on the Rights of the Child, 1989, 1577 UNTS 3.

### **General Data Protection Regulation, 2018**

It ensures individuals' control over their personal data and imposes strict rules on its processing. Its strong enforcement and wide scope have made it a global benchmark for privacy laws.

### **CRITICISM**

These regional and international privacy guidelines and laws are not legally binding, so they are often not enforced effectively. Their effectiveness is also limited because not all countries follow or adopt them equally. Moreover, exceptions like national security may affect privacy protections. Some of laws are outdated or complex to implement, making them less effective.

## **V. AN ANALYSIS OF THE NATIONAL LEGAL FRAMEWORK: DIGITAL PRIVACY**

In India, legal structures relating to digital privacy has developed through laws, constitutional interpretation, and regulations.

### **Constitutional Protection: Right to Privacy**

The Indian Constitution does not explicitly mention right to privacy. But it has been recognized through judicial interpretation as a part of Article 21. In **Puttaswamy case**<sup>28</sup>, the Supreme Court declared privacy as a fundamental right. It also emphasized that privacy is an essential part of human dignity and personal autonomy which includes protection of personal information in the digital sphere. The Court further stated that any infringement with this right must be legal, necessary and proportionate.<sup>29</sup>

### **The Indian Telegraph (Amendment) Act, 2003<sup>30</sup>**

After extended to digital communication technologies, this act forms the legal basis for accessing private communications. Although it is allowed for public safety and national security but it must follow proper legal procedures and judicial oversight. However, questions still remain regarding its outdated nature and limited transparency.

---

<sup>28</sup> Supra note 5.

<sup>29</sup> M.P. Jain, Indian Constitutional Law 1349 (LexisNexis, Gurugram, 8<sup>th</sup> ed., 2018).

<sup>30</sup> The Indian Telegraph (Amendment) Act, 2003 (Act 8 of 2004).



### **Information Technology Act, 2000**

In India, cyber activities and digital offences are governed by this act. It has several provisions regarding digital privacy like Section 43A ensures compensation for data breaches because of poor security, Section 66E makes it illegal to share or capture private images without their consent, Section 69 allows government surveillance subject to safeguards, and Section 72 punishes anyone who disclose other persons' personal information without consent to ensure confidentiality.<sup>31</sup>

### **Digital Personal Data Protection Act, 2023<sup>32</sup>**

A consent-based framework was introduced for data processing by this act. It allows several rights like correction, access, and erasure of personal data, and also requires data fiduciaries to fulfil legal obligations and imposes penalties for non-compliance and data breaches.

### **CERT-In Guidelines**

In India, cybersecurity incidents are handled by the Indian Computer Emergency Response Team. For some cyber incidents, it requires proper data retention and timely reporting. In spite of the strong security and response systems, several privacy risks still remain due to prolonged data storage.

### **VARIOUS INCIDENT OF DATA PRIVACY BREACHES**

1. In **August 2022**, nearly 37,000 users were affected by **Bharatpay** data breach that exposed customers' sensitive data including transaction details and hashed passwords.
2. In **December 2022**, approximately 30 million users were affected by **RailYatri** data breach that exposed customers' personal information. This also highlights the ongoing challenges in the online transportation platforms.
3. In **October 2023**, near about 815 million Indians loses their personal data by a massive **Aadhaar data leak**. This increases serious risks to the government digital infrastructure and data security.
4. In **August 2024**, **The Star Health Insurance Breach<sup>33</sup>** shows that nearly 31 million customers affected by a cyberattack. It also revealed that such incidents not only expose

<sup>31</sup> The Information Technology Act, 2000 (Act 21 of 2000), s. 43, 66, 69, 72.

<sup>32</sup> Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

<sup>33</sup> <https://www-expresscomputerin.cdn.ampproject.org/c/s/www.expresscomputer.in/amp/exclusives/the-truth-behind-the-star-health-breach-a-story-of-cybercrime-disinformation-and-trust/117411/> (last visited on March 10, 2026).

customers' personal data but also damage reputation and trust by spreading misinformation and harming organizational credibility.

## VI. JUDICIAL APPROACH TOWARDS THE PROTECTION OF DIGITAL PRIVACY

Judicial interpretation has played a significant role in shaping the digital privacy law in India, with various landmark judgments expanding fundamental rights to address technological challenges.

1. **Justice K.S. Puttaswamy case<sup>34</sup>:** The landmark case established that under the Indian Constitution, the right to privacy is a fundamental right, protected under Article 21. The Supreme Court held that privacy is essential for autonomy, dignity, and personal freedom, and includes protection of personal and digital information. It also held that any interference with privacy must be necessary, lawful, and proportionate to a legitimate aim.
2. **People's Union for Civil Liberties (PUCL) case<sup>35</sup>:** The Supreme Court held that private telephone conversations are part of the right to privacy under Article 21, and any interception by the State must follow strict procedural safeguards like review and authorization.
3. **Puttaswamy (Aadhaar) case<sup>36</sup>:** The Supreme Court examined the constitutional validity of the Aadhaar scheme but imposed strict limitations on data use. It held that any collection of personal or biometric data by the State must satisfy the test of necessity, legality, and proportionality. The Court limited the use of Aadhaar to government and welfare purposes, struck down its mandatory linking with private and emphasized that privacy cannot be disproportionately invaded.
4. **Google Spain SL case<sup>37</sup>:** The Court of Justice of the European Union held that individuals have a "right to be forgotten" which means they can request search engines

---

<sup>34</sup> Justice K.S. Puttaswamy (Retd.) v. Union of India AIR 2017 SC 4161.

<sup>35</sup> People's Union for Civil Liberties (PUCL) v. Union of India AIR 1997 SC 568.

<sup>36</sup> Puttaswamy (Aadhaar) v. Union of India 2019 1 SCC 1.

<sup>37</sup> Google Spain SL v. Agencia Española de Protección de Datos (2014) ECR I- 317.

to remove personal information under certain conditions. In India, this right is not absolute and must create balance between privacy and freedom of expression.

5. **Anuradha Bhasin case<sup>38</sup>**: The Supreme Court held that access of internet is essential for freedom of speech and trade, and any restriction must be reasonable, temporary, and proportionate.

## VII. MAJOR CHALLENGES TO DIGITAL PRIVACY

### 1. Mass Surveillance

By using some digital surveillance tools like facial recognition systems, CCTV cameras, and internet monitoring programs, Governments may track individuals. These tools may help to maintain security but excessive surveillance can violate individuals' privacy and civil liberties.

### 2. Data Breaches

Security weaknesses and cyber-attacks can expose private information like bank details, passwords, and personal records. It may increase the risk of identity theft and financial fraud.

### 3. Data Collection by Corporations

Multinational companies collect large numbers of personal data without the consent of the users. For commercial purposes, this data may be shared or sold with third parties.

### 4. Artificial Intelligence

AI systems can easily predict user behaviour by analysing massive datasets. Such analysis may violate individuals' privacy and freedoms.

### 5. Social Media Privacy Risks

Now a days, social media is a very powerful platform. As well as, social media is one of the best platforms for entertainment. While seeking entertainment, many people share their personal information unknowingly which may be misused by hackers, advertisers, or even governments.

---

<sup>38</sup>Anuradha Bhasin v. Union of India AIR 2020 SC 1308.

## **6.Lack of Public Awareness**

Public is not well aware regarding the matter of protecting data. Many people click accept without reading them carefully and also ignore privacy setting. Consequently, they face greater challenges in exercising their digital rights.

## **7. Weak Enforcement Mechanisms**

Because of the weak enforcement such as lack of technical expertise, delays in investigation, Digital privacy laws are often remained ineffective. Strong enforcement and independent supervision can protect individuals' data effectively.

# **VIII. SUGGESTIONS**

1. Transparency should be ensured by the organizations strictly as well as they should classify collected data based on sensitivity.
2. Strong security measures such as access controls, encryption, and multi-factor authentication should be implemented.
3. Special laws should be enacted to address challenges raised by AI and new technologies.
4. Organizations and government should comply with data protection laws and stay updated from time to time on emerging cyber threats and also promote training on cybersecurity for their officials.
5. Clear surveillance laws should be enacted by the government with proper supervision to tackle the evolving digital threats.
6. Data minimization principles should be followed by collecting only necessary data.
7. By organizing various awareness programmes, Governments should improve digital literacy.

# **IX. CONCLUSION**

In today's digital environment, protecting privacy has become a concern because of the mass data collection. It creates threat to individuals' fundamental freedom and dignity. Although, there are various laws but they must be updated from time to time and actively enforced to tackle these challenges. As well as, different international privacy laws are also there. But for the improper implementation, they failed to tackle the challenges. That's why strong international cooperation is needed to address these problems. Ultimately, a rights-based and

transparent approach is very much essential for balanced technological development.

## X. BIBLIOGRAPHY

1. Brahimi Smail, "The Erosion of the Right to Privacy in International Law: Legal and Ethical Implications in the Digital Age" 14 Journal of Law, Society and Authority (2025).
2. Constitution of India, 1950.
3. Digital Personal Data Protection Act, 2023 (India).
4. Daniel J. Solove, Understanding Privacy (Harvard University Press, 2008).
5. Dr. H.O. Agarwal, International Law & Human Rights (Central Law Publications, 23<sup>rd</sup> edn, 2021).
6. Dr. Vinayaka. K, "Digital Surveillance Vs. Right To Privacy: A Human Rights Perspective" 3 Journal of Emerging Trends and Novel Research (2025).
7. General Data Protection Regulation (GDPR), European Union, 2016.
8. Information Technology Act, 2000.
9. International Covenant on Civil and Political Rights (ICCPR), 1966.
10. Mahabir Prashad Jain, Indian Constitutional Law (Lexis Nexis, 7th edn, 2014).
11. The constitution of India Bill 1895
12. The commonwealth of India Bill 1925
13. Universal Declaration of Human Rights (UDHR), 1948.