RIGHT TO PRIVACY IN THE DIGITAL AGE: A CRITICAL EXAMINATION

Harshita Singh*

ABSTRACT

The development of technology has immensely benefited humanity. Nevertheless, many of our liberties are now in danger as technology advances. As the modern age advances and involves data that is continuously collected and processed in the marketplace, the right to privacy is becoming an increasingly pressing matter. The digitalization process has led to the emergence of several illegal practices, including data fraud, fake contact, cyber harassment, etc. When users' private information is sent to websites for digital networking, businesses, interaction intelligence companies, state agencies, and others, it is often treated improperly. The collection, preservation, monitoring, recording, access, processing, dissemination, upkeep, etc. of data are not specifically governed by any laws in the country.

Keywords: Right To Privacy, Digitalization, Legal Frameworks, Data Breach, Cyberattacks, Surveillance.

INTRODUCTION

The freedom of conscience, the right to personal security, and the right to refuse self-incrimination are all based on the right to privacy[1]. According to the contemporary digital era, the "right to privacy should be seen as an independent right that deserves legal protection in itself"[2] and the concept of privacy is expanded to include "privacy in the digital environment (e-privacy)." The following working definition of a "right to privacy" can be put forth in this regard: "The right to privacy is our right to keep a domain around us, which includes all those things that are part of us, such as our body, home, property, thoughts, feelings, secrets, and

*BA LLB, FOURTH YEAR, BANASTHALI VIDYAPEETH UNIVERSITY, JAIPUR,RAJASTHAN.

[1] `Radi P. Romansky and Irina S. Noninska, Challenges of the digital age for privacy and personal data protection (2020)'17 Mathematical Biosciences and Engineering <https://www.aimspress.com/article/doi/10.3934/mbe.2020286?viewType=HTML> accessed 26 January 2025.

[2] *Ibid.*

identity." [3]The right to privacy allows us to decide which aspects of our domain are accessible to others and to regulate the scope, mode, and timing of how those aspects are used. The way we interact, communicate, and conduct business has been transformed by the digital revolution. Although technology offers unprecedented opportunities for innovation and connectivity, it also raises significant concerns over individual rights. One of the most prized characteristics of human life and a basic component of personal liberty is the frequently used phrase privacy.[4] A person's right to privacy is a complex concept. It refers to an internet user's special right to control the collection, archiving, and sharing of his personally identifiable information. A person's private information includes things like identification, interests, and preferences, as well as information about other people they are related to, education, health, and financial information. Private information may be creatively used for several purposes, including business profit-making and government surveillance.

The right to privacy began in the 1890s when prominent intellectuals like Louis Brandeis and Samuel D. Warren suggested that the "right to privacy "should be included in the scope of the right to life[5]. The acknowledgment of the “right to privacy” as a fundamental right in India took time and was subject to judicial scrutiny from the inception of the Indian[6]

In the 1954 case M.P. Sharma v. Satish Chandra[7], an eight-judge Supreme Court panel denied the existence of a right to privacy, arguing that as the Indian Constitution contains no provisions addressing the right to privacy, it cannot be infringed upon. The 2017 case of K.S. Puttaswamy v. Union of India[8], is the cornerstone of the ‘Right to Privacy’ jurisprudence in India. The nine Judge Bench in this case unanimously reaffirmed the right to privacy as a fundamental right under the Constitution of India. The Court held that the right to privacy was integral to freedoms guaranteed across fundamental rights, and was an intrinsic aspect of dignity, autonomy.[9]

---

[3] `B.Rathore ,`The Right to Privacy in the Digital Age: Legal Implications and Challenges (2024), `The Amicus Qriae < https://theamikusqriae.com/title-the-right-to-privacy-in-the-digital-age-legal-implications-and-challenges/> accessed 26 January 2025.
[4] *Ibid.*
[5]`Shreeya Patil, `Navigating the Digital Frontier: Right to Privacy in the Age of social media `The Society for Constitutional Law Discussion (January 08 2024) < https://www.tscld.com/right-to-privacy-social-media> accessed 26 January 2025.
[6] *Ibid*
[7] *M.P. Sharma v. Satish Chandra* (1954) AIR 300.
[8] *Justice K.S.Puttaswamy(Retd) vs Union of India,* AIR 2018 SC (SUPP) 1841.
[9] *Justice K.S.Puttaswamy(Retd) vs Union of India, `Privacy* Law Library (2017) < https://privacylibrary.ccgnlud.org/case/justice-ks-puttaswamy-ors-vs-union-of-india-ors> accessed 26 January 2025

HISTORICAL CONTEXT OF PRIVACY

The concept of privacy can also have a practical application in ancient Hindu literature. The Hitopadesh enumerates topics such as religion, sex, and family matters that ought to be kept out of the public eye.

With the adoption of the US Constitution in 1789[10], the debate over the right to privacy got underway. Despite not specifically guaranteeing a right to privacy, the Supreme Court has ruled that the First, Third, Fourth, and Fifth Amendments of the Constitution do, in reality, create such a[11]

Although privacy has been prized since time immemorial the Universal Declaration of Human Rights (UDHR) in 1948[12] marked its official acknowledgement as a right. Protection against arbitrary interference in privacy is guaranteed under Article 12 of the UDHR and Article 17 of the International Covenant on Civil and Political Rights (ICCPR)[13].

A few Supreme Court decisions occurred later in the 1960s and 1970s. The well-known Griswold v. Connecticut (1965)[14] case involved a Connecticut "Comstock law" that prohibited the use of birth control of any type. The Supreme Court set the precedent for the right to private about personal habits, etc., by rejecting the Act by a vote of 7–2, citing the "right to marital privacy."

The evolving regulatory landscape reflects the ongoing efforts to combine the benefits of advanced technology with the need to protect security, privacy, and other democratic values. The advent of the digital age, however, has introduced complexities not envisioned by these early frameworks.

[10] The United States Constitution of 1789.
[11] `B.Rathore ,`The Right to Privacy in the Digital Age: Legal Implications and Challenges (2024),'The Amicus Qriae < https://theamikusqriae.com/title-the-right-to-privacy-in-the-digital-age-legal-implications-and-challenges/> accessed 26 January 2025.
[12] Universal Declaration of Human Rights of 1948.
[13] International Covenant on Civil and Political Rights of 1966.
[14] *Griswold v. Connecticut*, (1965) 381 U.S. 479.

LEGAL FRAMEWORKS FOR DIGITAL PRIVACY

International Regulations

The 1948 Universal Declaration of Human Rights: Article 12 of the UDHR[15] guarantees the right to privacy, stressing that no one should have their correspondence, family, home, or private arbitrarily interfered with. This fundamental idea lays the framework for later privacy regulations by emphasizing the value of shielding private life from unwarranted invasions.

The General Data Protection Regulation (GDPR)[16]: is regarded as the gold standard for data protection rules. It was put into effect by the European Union in 2018. It imposes stringent guidelines on the gathering, storing, and handling of personal information. The need for clear consent, purpose limitation, and data minimization are important guidelines. To ensure accountability and transparency, GDPR also gives people rights including data portability, access to their data, and the right to be forgotten.

The 2001 adoption of the Budapest Convention on Cybercrime[17]: targets offences perpetrated through computer networks, including the internet. It offers a framework for promoting international cooperation, enhancing investigative methods, and harmonizing national legislation. Although fighting cybercrime is its main goal, it also highlights the necessity of striking a balance between the protection of individual privacy and the ability of law enforcement.

National Laws

The California Consumer Privacy Act, 2020 (CCPA)[18]: gives Californians authority over their personal information. It gives customers the right to know what personal information is being gathered about them, to have that information deleted, and to refuse to have their information sold. Businesses must be honest about how they gather data, and noncompliance will result in sanctions.

Digital Personal Data Protection Act of 2023 in India[19]: This law seeks to strike a balance between economic development and the requirement for data protection. It establishes duties

[15] Universal Declaration of Human Rights of 1948.
[16] The General Data Protection Regulation of 2018.
[17] Budapest Convention on Cybercrime of 2001.
[18] The California Consumer Privacy Act of 2020.
[19] Digital Personal Data Protection Act of 2023.

for data custodians, including getting consent before collecting data, guaranteeing data accuracy, and protecting data from security breaches. It also prompts questions about possible government overreach and state entity exclusions, though.

C**hinese law protecting personal information (PIPL)[20]:** The PIPL is one of the strictest data privacy regulations in the world and has been in effect since 2021. It requires that the processing of personal data be justified, legal, and kept to a minimum. The law mandates that businesses get express consent, implement strong security protocols, and make sure that cross-border data transfers adhere to stringent guidelines. Serious consequences may follow non-compliance.

CHALLENGES TO PRIVACY IN THE DIGITAL AGE

Mass Surveillance

Laws about surveillance frequently do not adapt to new developments in technology. This allows the government to monitor people without any checks and creates gaps in legal protections. Privacy rights are being challenged by the increasing use of facial recognition, biometric data collecting, and algorithmic monitoring. Consequently, people's personal information is increasingly vulnerable to misuse and manipulation in the digital age.

The Big Brother Watch and Others v. UK case[21], for instance, dealt with violations of Articles 8 and 10 of the European Convention on Human Rights (ECHR)[22], including those about the freedom of expression and privacy.

The rulings provoked heated discussions about the fine balance between rights and interests as well as the need to review the criteria for judging whether the Convention has been violated considering significant technological advancements, the introduction of mass surveillance, and data processing.

Additionally, to successfully combat surveillance, policies that not only prevent it but also inform the public about the negative effects of digital surveillance and empower people to exercise their right to privacy must be put in place.

[20] Chinese law protecting personal information of 2021.
[21] *Big Brother Watch and Others v. UK (*2014) 58170/13.
[22] European Convention on Human Rights of 2021.

Artificial Intelligence (AI) and Big Data

Businesses gather enormous volumes of data for predictive analytics and targeted advertising. This data is frequently processed by AI systems, which raises questions regarding algorithmic bias and profiling.

The combination of big data and AI creates substantial privacy concerns, as these technologies rely on large-scale data collection and processing for decision-making and forecasts.

The following problems demonstrate their significance:

Volume and Variety of Data: Big data is frequently gathered from a wide range of sources, including public records, e-commerce sites, social media, and Internet of Things devices. Individuals' detailed profiles are produced by this massive data collection, frequently without their express agreement. Concerns regarding adherence to the GDPR's principles of data minimization and purpose limitation are raised by the vast volume of data.

Bias in AI Algorithms: AI programs that have been trained on huge datasets may inadvertently introduce and intensify preexisting biases. For example, discriminatory actions based on gender, color, or socioeconomic status may result from predictive algorithms applied in law enforcement or recruiting. Such biases might lead to legal repercussions or damage to an individual's reputation in addition to being against ethical standards.

False Conclusions: Trends and patterns that may not fully reflect a person's actions or intentions are frequently extrapolated by big data analytics. Data misinterpretation can result in inaccurate assumptions about a person's personality, way of life, or preferences, which could have negative effects on things like insurance, work, and credit approval.

Transparency Problems: People find it challenging to comprehend how their data is processed because big data analytics techniques and algorithms are frequently proprietary and opaque. The GDPR's mandate for easily understandable information regarding data processing is compromised by this lack of transparency.

Reidentification Risks: By cross-referencing datasets, sophisticated AI systems can frequently reidentify people even when personal data has been anonymized. This seriously jeopardizes privacy and calls into question the efficacy of conventional anonymization methods.

Surveillance capitalism: is when businesses utilize AI and big data to forecast and affect customer behavior for financial gain, frequently obfuscating the distinction between intrusive surveillance and lawful marketing. Trust is damaged by this monetization of personal information, which also calls into question the moral application of AI-driven insights.

Ethical Problems: Applying AI in delicate fields like criminal justice and healthcare can have profound effects. Errors in predictive policing algorithms or medical diagnostics, for instance, can disproportionately impact vulnerable communities, raising moral and legal questions.

Breach of Data

In today's digital world, personal and sensitive information is increasingly stored online. While this improves convenience and efficiency, it also creates significant vulnerabilities. Data breaches and cyberattacks are major threats to privacy in this context. A data breach occurs when unauthorized individuals gain access to sensitive, protected, or confidential information. These breaches often expose personal details such as names, addresses, financial records, health data, and passwords. In 2022, data breaches cost businesses an average of $4.35 million[23] – up from $4.24 million in 2021.2021 saw an average of $787,671 lost every hour due to data breaches.

- The UK had the highest number of cybercrime victims per million internet users at 4783 in 2022 – up 40% over 2020 figures[24].
- The country with the next highest number of victims per million internet users in 2022 was the USA, with 1494, a 13% decrease over 2020.[25]
- 1 in 2 North American internet users had their accounts breached in 2021.

Cyberattacks are deliberate attempts by hackers to infiltrate systems, steal data, or disrupt digital operations. These attacks use methods like phishing, malware, ransomware, or distributed denial of service (DDoS). Cyber-attacks globally increased by 125% in 2021 compared to 2020, and increasing volumes of cyber-attacks continued to threaten businesses and individuals.[26]

23 `The Latest 2025 Cyber Crime Statistics, `Business IT Support that just works (January,2025) < https://aag-it.com/the-latest-cyber-crime-statistics/> accessed 26 January 2025.
[24] *Ibid.*
[25] *Ibid.*
[26] *Ibid.*

Phishing remains the most common form of cyber-crime. In 2021, 323,972 internet users reported falling victim to phishing attacks. This means half of the users who suffered a data breach fell for a phishing attack. During the height of the pandemic, phishing incidents rose by 220%.2021 saw nearly 1 billion emails exposed, affecting 1 in 5 internet users. This may partly explain the continued prevalence of phishing attacks. Ransomware attacks continue to pose a serious threat to individuals and organizations, with more advanced attack methods forcing payouts from victims. Around 236.1 million ransomware attacks were reported worldwide in the first half of 2022.[27]

Internet of Things (IoT)

The term is used to describe a set of objects and devices that are connected to the Internet to send and receive data obtained by using sensors for monitoring selected parameters and to capture and analyze values obtained to control processes in different spaces such as home, city, health, etc. It is possible that connected devices may disturb privacy and security and could undermine consumer confidence. In this connection, two main aspects of IoT for privacy and data protection could be defined:

a. **Confidentiality –** it could be disturbed because each physical or logical object or thing could receive a unique identification code and could freely communicate through the Internet or via other networks.[28] All data sent from the endpoints are not the target for strong confidentiality, but the analysis of these data which are usually received by many points could consist of sensitive information for a person. On the other hand, the increase in the number of sensors leads to the accumulation of data, which increases the risks to security and privacy. For example, when hacking smart sensors, accessing the collected data can lead to learning about certain habits, health and religion data, and more health and religion data, and more.

[27] *Ibid.*
[28] `Radi P. Romansky and Irina S. Noninska, Challenges of the digital age for privacy and personal data protection (2020) `17 Mathematical Biosciences and Engineering <https://www.aimspress.com/article/doi/10.3934/mbe.2020286?viewType=HTML> accessed 26 January 2025.

b. **Security of IoT –** a set of different computers and internet devices are configured by using traditional passwords that are not protected, and the things could be objects of different attacks. The attacks target components with low levels of "cyber-hygiene" and look for their vulnerability to hacking and tampering. Another problem with IoT security is identity verification - usually, a traditional approach is used which hardly provides the necessary level of access control. It is also possible to use devices that have factory default passwords that cannot be changed. Statistical studies show that IoT devices are susceptible to cyberattacks. For example, 56% of risk professionals report not keeping an inventory of IoT devices, and 64% report not keeping an inventory of IoT applications. Other 76% believe that the cyberattacks are likely to be executed through IoT.[29] Other statistics related to privacy show that 74% of global consumers worry about losing individual rights and only 45% of respondents require the third parties that have access to their sensitive and confidential information to implement measures to ensure reliable data security and protection. Other statistics presented related to privacy show that 74% of global consumers worry about losing individual rights and only 45% of respondents require the third parties that have access to their sensitive and confidential information to implement measures to ensure reliable data security and protection.

SOCIAL MEDIA AND DIGITAL PLATFORMS

Social computing (SoC) challenges

It is known that this technology permits to organizing of a dialog between individual computer users through the Internet by using different environments united under the term Social Networking Sites – SNS (social media, Social Networks, Social Bookmarking, Social Agammaegators, Blogs & Microblogs, Wikis, Multiplayer games, etc.). Practically the SoC is a useful instrument for connection between users and information sharing, but there is a possible risk to personal data protection because the information might be shared with an unauthorized person. In some cases, this can cause negative financial and psychological consequences to the owner of these data. A summary of the SoC negatives for user's privacy is presented below:

[29] *Ibid.*

In many cases, websites play the role of an "open door" – during the preliminary registration or at the first visit with just one "click" users can accept the Privacy Policy without reading the text.[30] The result is full acceptance of all conditions without the user being aware of them. In this case, she/he is not aware of exactly what will happen to her/his data in the created user's profile. The result is full acceptance of all conditions without the user being aware of them. In this case, she/he is not aware of exactly what will happen to her/his personal data in the created user's profile.

In other cases, the user's data are stored after one visit only and automatically transferred to the center without the owner's knowledge and consent. Indicative is the fact that only 54% of social network users think that they are informed about the conditions for collecting personal data and their next use when they join a social networking site or register for an online service.

In some cases, the media may not provide information about the Privacy Policy or require too much personal information when the [31] principle of limited personal data is violated). principle of limited personal data is violated).

Another problem is the location of stored personal data somewhere in the global network. It may be possible to maintain multiple copies when looking for an acceptable position. This is contrary to the GDPR principle for minimizing stored and processed personal data. An example in this direction is the conclusion of the National Consumer Agency in Germany for violation of legislation on data protection by Facebook with the disseminated information that the advertisements are fully free of charge. The stated reason is that social network receives significant amounts by collecting personal data and their storage in various locations in the global network.

The "right to be forgotten/erased[32] provision in the event of a refusal of continued usage is negatively impacted by the issue. The user is unable to confirm that every copy of their personal information has been removed from all network nodes. In one instance, an Austrian law student asked for all the data that a social networking site (SNS) had on file on the user's profile. He was sent 1224 pages of information in response, some of which he thought had been deleted, including his old articles, messages, and photographs. It appears that in addition to keeping deleted and superfluous information, the website has gathered a lot more personal data than the

[30] *Ibid.*
[31] The General Data Protection Regulation of 2018.
[32] *Ibid.*

user had anticipated. It appears that in addition to keeping deleted and superfluous information, the website has gathered a lot more personal data than the user had anticipated.

KEY CONCERNS

Informed Consent: Numerous users unintentionally consent to data gathering in return for digital services.

Digital Divide: Often, marginalized groups face greater risks of privacy violations.

Finding a Balance Between Security and Privacy: Governments advocate for monitoring to fight crime and terrorism, frequently sacrificing personal rights in the process.

SOLUTIONS

- **Data Encryption**

  Applications such as Signal and WhatsApp use end-to-end encryption to guarantee secure conversations by encoding messages in a manner that only the sender and intended receiver can interpret. This stops unauthorized entry by hackers, companies, or even governments.

- **Technology Focused on Privacy**

  Brave and similar privacy-focused browsers block trackers and advertisements that collect user data. Virtual Private Networks (VPNs) hide a user's whereabouts and online actions by encrypting internet data. Instruments such as Tor enable anonymous browsing by spreading the traffic across multiple servers.

- **Modifications to Regulations**

  Enhanced legal frameworks ensure better enforcement of privacy protections. This entails enhancing the transparency of data collection processes, implementing routine audits for firms managing sensitive information, and imposing stricter penalties for data violations. International cooperation on privacy laws can also aid in standardizing protections globally.

- **Public Knowledge**

  People can adopt safer online practices and comprehend the value of digital privacy with the aid of educational efforts. These programs could involve training sessions on

identifying phishing efforts, utilizing privacy technologies, and comprehending data rights under regulations such as the CCPA[33] and GDPR.[34]

- **Business Accountability**

  To protect user privacy, businesses are essential. By including privacy considerations in product development, they ought to embrace privacy-by-design principles. This entails minimizing data acquisition, giving consumers control over their information, and establishing explicit data regulations. Trust must be upheld by ethical actions, such as not selling customer data without permission.

RECOMMENDATIONS

- **Policy Development:** To handle the issues brought about by cutting-edge technologies like artificial intelligence (AI), the Internet of Things (IoT), and quantum computing, governments should create thorough legal frameworks. Clear rules for data collection, use, and retention should be part of these policies, along with strong enforcement measures.
- **Global Cooperation:** To minimize jurisdictional disparities, international treaties, and accords should seek to standardize privacy rules across national boundaries. Cooperation among nations is necessary to create a worldwide data protection framework that covers cross-border data transfers, reciprocal legal aid, and coordinated enforcement tactics.
- **Technological Innovation:** Research and development of privacy-preserving technologies like homomorphic encryption, differential privacy, and secure multi-party computation require more funding. Collaboration and data analysis are made possible by these technologies without sacrificing personal privacy. The use of such technologies should be encouraged, and research projects should be funded by public and private entities.
- **Accountability Mechanisms:** It is necessary to set up independent regulatory organizations to keep an eye on and audit government and corporate data activities. These organizations must be able to enforce sanctions for noncompliance, carry out routine examinations, and guarantee openness in data handling procedures.

[33] The California Consumer Privacy Act of 2020.
[34] The General Data Protection Regulation of 2018.

Strengthening whistleblower protections is another way to promote the reporting of privacy issues.

- **Empower People:** It is necessary to create resources and educational initiatives that empower people to take charge of their digital footprint. Access to tools like workshops and online manuals, easily navigable privacy settings, and concise explanations of data usage are all part of this. Governments and nonprofit organizations should work together to assist underserved communities to successfully protect their privacy and to advance digital literacy.

CONCLUSION

To protect privacy in the digital age[35], a thorough and cooperative strategy that tackles the various issues raised by modern technology is needed. While international collaboration guarantees consistency in privacy norms across borders, policy development must offer explicit legal frameworks to regulate data collection and usage. Technology innovation provides the means to strike a balance between data utility and privacy protection but to ensure adherence to regulations and preserve openness, these developments need to be backed by accountability systems. The first line of defense against privacy invasions is informed citizens, therefore arming people with information and resources is equally important. We can create a digital ecosystem that embraces the benefits presented by technological advancement while protecting individual privacy by putting these suggestions into practice against privacy invasions in informed citizens, therefore arming people with information and resources is equally important. We can create a digital ecosystem that embraces the benefits presented by technological advancement while protecting individual privacy by putting these suggestions into practice.

[35] OHCHR and privacy in the digital age.