IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, April 2026
Impact Factor: 8.2

Violation of Privacy Rights under Article 21: A Study of Data Breach

Vivek Kumar
Research Scholar, Department of Law, Baba Mastnath University, Rohtak

Abstract: *This research study explores the protection and security of personal data within the broader framework of the Right to Privacy under Article 21 of the Indian Constitution, with particular emphasis on data breaches. In recent decades, the rapid expansion of the internet and advancements in technology have led to an unprecedented growth in data generation. As a result, vast amounts of individuals' personal information are being collected, stored, processed, and disseminated by various entities, including corporations, institutions, and organizations. In such a scenario, safeguarding individual privacy has become critically important, especially given the increasing risks and frequency of data breaches.*

The development of the data protection regime in India reflects a dynamic evolution, significantly influenced by international legal frameworks. This progression ultimately led to the enactment of the Digital Personal Data Protection Act, 2023, marking a crucial step toward establishing a comprehensive legal structure for data privacy and protection. Relying on an extensive review of existing literature, this study examines the salient features of the Act, identifies its structural and practical shortcomings, and proposes necessary reforms.

Furthermore, the paper critically evaluates the effectiveness of the current legal and regulatory mechanisms in addressing issues related to data breaches and in ensuring the protection of personal data. It also seeks to contribute to the evolving jurisprudence on data protection by highlighting gaps within the existing framework. By doing so, the study aims to offer constructive recommendations, promote greater public awareness, and facilitate more effective implementation and enforcement of data protection laws in India..

Keywords: Security, Surveillance, Data Breach, Privacy, Protection, etc

I. INTRODUCTION

The concept of privacy has undergone significant transformation in recent years, particularly within the constitutional framework of Article 21 of the Indian Constitution. The right to privacy, intrinsically linked with human dignity, reflects an individual's inherent desire to preserve personal autonomy and protect sensitive aspects of life from unwarranted intrusion. Privacy, however, is not a uniform concept; it is multifaceted in nature and varies across different cultural and social contexts. In the contemporary digital era, the importance of privacy has grown substantially due to rapid technological advancements and the widespread use of social media platforms.

With the increasing digitization of society, there has been a marked rise in both domestic and cross-border exchange of information among individuals, businesses, and governmental as well as non-governmental entities. Consequently, vast quantities of personal data—including financial, medical, and other sensitive information—are continuously being generated and circulated online. This digital expansion has heightened concerns regarding the lack of transparency in the processes of data collection, storage, access, and processing. The growing incidence of data breaches, involving unauthorized disclosure of sensitive personal information such as banking details, health records, and contact information, underscores the vulnerability of individual privacy in the digital landscape.

In light of these challenges, the need for a comprehensive legal framework to address data protection and privacy violations became increasingly evident. Responding to this necessity, the legislature enacted the Digital Personal Data

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 4, April 2026 Impact Factor: 8.2

Protection Act, 2023 (DPDP Act). However, given its recent introduction, it becomes essential to critically examine the effectiveness of this legislation, particularly in the context of data breaches and their implications for the right to privacy under Article 21. Such an analysis must also consider whether the Act successfully achieves its stated objective of balancing the legitimate need for processing personal data for lawful purposes with the fundamental right of individuals to safeguard their personal information.

Research Problem

In recent years, rapid digitization has led to an exponential increase in the collection, storage, processing, and exchange of data among various entities. This digital expansion has intensified concerns regarding the protection of personal information, particularly due to the lack of transparency in data handling practices. Numerous instances of data breaches and unauthorized disclosures of personal information have been reported, resulting in direct infringements of the Right to Privacy as guaranteed under Article 21 of the Indian Constitution.

In this context, it becomes imperative to undertake a comprehensive analysis of the issue of data breaches and their implications for privacy rights. Such an examination must identify the key challenges associated with data protection, including gaps in regulatory enforcement and implementation. Special attention must be given to evaluating the effectiveness of the Digital Personal Data Protection Act, 2023, while also situating it within the broader constitutional framework of the Right to Privacy, in order to assess its adequacy in addressing emerging threats to personal data security.

Objectives of the Study

- To examine the concept and scope of the Right to Privacy as an integral part of Article 21 of the Indian Constitution in the context of the digital era.
- To analyse the nature, causes, and increasing instances of data breaches and their impact on the privacy of individuals.
- To evaluate how data breaches constitute a violation of privacy rights, particularly with respect to personal, financial, and sensitive information.
- To critically examine the legal and regulatory framework governing data protection in India, with special reference to the Digital Personal Data Protection Act, 2023.
- To assess the effectiveness of the DPDP Act, 2023 in preventing data breaches and safeguarding personal data.
- To identify the challenges and limitations in the implementation and enforcement of data protection laws in India.
- To analyse the role of transparency, accountability, and data governance mechanisms in protecting privacy rights.
- To suggest reforms and recommendations for strengthening the data protection regime and ensuring better protection of the Right to Privacy under Article 21.

Research Questions

- What is the scope and constitutional status of the Right to Privacy under Article 21 of the Indian Constitution in the digital age?
- How do data breaches affect the protection of personal and sensitive information of individuals?
- To what extent do data breaches constitute a violation of the Right to Privacy under Article 21?
- What are the major causes and forms of data breaches in the contemporary digital ecosystem?
- How effective is the existing legal framework in India in addressing issues of data protection and privacy violations?

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 4, April 2026 Impact Factor: 8.2

- What reforms and policy measures are required to strengthen the data protection regime and ensure effective protection of privacy under Article 21?

II. RESEARCH METHODOLOGY

This study undertakes an analysis of data protection and privacy laws through a doctrinal research approach, supplemented by both qualitative and quantitative methods. The research primarily relies on secondary sources, including constitutional provisions, statutory frameworks, scholarly books, journal articles, research papers, reports of various commissions and organizations, as well as credible media and newspaper sources. These materials form the foundational basis for examining issues related to data breaches and their implications for the Right to Privacy under Article 21 of the Indian Constitution.

Privacy in the Digital Data Ecosystem

Understanding the concept of privacy, along with the meaning of "data," is essential for analysing data protection within the broader framework of the Right to Privacy under Article 21 of the Indian Constitution. The term "privacy" is derived from the Latin word "Privatus" which signifies a state of being separate or withdrawn from the public sphere. Although privacy does not have a universally accepted definition, it is generally understood as the freedom from unwarranted intrusion into one's personal sphere and is often described as the right to be left alone.

Privacy is fundamentally connected to individual autonomy and human dignity, allowing a person to develop their personality and exercise choices freely. It forms the core of personal liberty by enabling individuals to make decisions without undue interference. In the contemporary context, particularly with the rise of data-driven technologies, privacy also encompasses the control over personal information, the maintenance of confidentiality, and the ability to function independently without external surveillance or intrusion.

The recognition of privacy as a fundamental human right is well established in international legal instruments. Various global conventions and treaties affirm the protection of privacy against arbitrary interference. For instance, the International Covenant on Civil and Political Rights emphasizes that no individual shall be subjected to unlawful interference with their privacy, family, home, or correspondence, nor to attacks on their honour and reputation[1]. Similarly, the European Convention on Human Rights guarantees the right to respect for private and family life, subject only to lawful and necessary restrictions in a democratic society. The Universal Declaration of Human Rights also upholds the principle that individuals are entitled to legal protection against arbitrary intrusions into their private lives.

In the context of increasing data breaches, these principles acquire heightened relevance, as unauthorized access, misuse, or disclosure of personal data directly undermines the essence of privacy and constitutes a violation of the fundamental rights guaranteed under Article 21.

The Right to Privacy has firmly established its place within Indian jurisprudence and has witnessed significant development in recent years, particularly in the context of technological advancements and data-related concerns. The Hon'ble Supreme Court, in the landmark judgment of "Justice K.S. Puttaswamy (Retd.) v. Union of India[2]", unequivocally recognized the Right to Privacy as a fundamental right. It was held to be an essential facet of the right to life and personal liberty under Article 21, as well as an intrinsic component of the freedoms guaranteed under Part III of the Constitution. This decision marked a transformative moment in India's constitutional history, especially in light of earlier rulings such as "M.P. Sharma v. Satish Chandra[3]" and "Kharak Singh v. State of U.P.[4]", which had denied the existence of a constitutionally protected right to privacy. The Puttaswamy judgment not only affirmed privacy as central to human dignity but also emphasized that other fundamental freedoms cannot be meaningfully exercised in its

[1] International Covenant on Civil and Political Rights, art. 17(1)

[2] Justice K.S. Puttaswamy and Anr. v. Union of India and Ors. (10 SCC 1, Supreme Court of India, 2017)

[3] MP Sharma v Satish Chandra, AIR 1954 SC 300

[4] Kharak Singh vs State of UP, AIR 1963 SC 1295

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 4, April 2026 Impact Factor: 8.2

absence. However, it is equally important to note that the right to privacy is not absolute and may be subject to reasonable restrictions in accordance with law.

In order to understand data protection within the framework of privacy, it is necessary to examine the meaning of the term "data." Data broadly refers to collected facts, observations, or measurements that serve as a source of information and may exist in various forms. These may include statistical or informational records such as demographic data, literacy rates, or employment figures. In the legal context, particularly under frameworks such as the General Data Protection Regulation (GDPR) of the European Union, "personal data" refers to any information that can directly or indirectly identify an individual. This includes identifiers such as name, location, or any characteristics relating to an individual's physical, mental, economic, cultural, or social identity. Accordingly, details such as phone numbers, bank account information, credit card details, health records, educational background, and marital status fall within the ambit of personal data.

Data protection, in the context of the Right to Privacy, is primarily concerned with ensuring that individuals retain control and autonomy over their personal information. It mandates that such data should not be collected, used, or disclosed without the informed consent of the individual. However, with the rapid advancement of digital technologies, instances of data breaches have become increasingly common. The ease with which data can now be collected, stored, processed, and transmitted has heightened the risk of unauthorized access and misuse. Recent reports, including those by the Data Security Council of India, indicate a sharp rise in data breaches, reflecting the growing vulnerability of personal data in the digital ecosystem. These concerns are further amplified by the expanding digital footprint of individuals and the increasing reliance on digital services, particularly in light of the Government's vision of transforming India into a trillion-dollar digital economy.

In the present digital landscape, the establishment of a robust and secure data protection framework has become essential for ensuring the privacy and safety of individuals, particularly in light of increasing instances of data breaches. It is noteworthy that many developed nations have already instituted comprehensive data protection regimes, thereby providing a greater degree of security and confidence to their citizens. Although developing countries like India face distinct structural and technological challenges, the urgency of safeguarding personal data cannot be overlooked.

The effective exercise of individual liberty is intrinsically dependent upon the assurance of privacy. When personal information remains vulnerable to misuse or unauthorized access, the meaningful enjoyment of fundamental freedoms is significantly undermined. Recognized as a fundamental right under Article 21 and as an essential component of human dignity, privacy occupies a central position in the constitutional framework. In the contemporary era, where vast amounts of personal data are continuously processed, the risk to privacy is not confined to state surveillance alone but also extends to private entities and institutions that handle such data.

Therefore, there exists an urgent and compelling need to strengthen legal and regulatory mechanisms to ensure the protection of personal information. A well-structured data protection regime is indispensable for mitigating the risks of data breaches and for upholding the constitutional guarantee of the Right to Privacy, thereby reinforcing the dignity, autonomy, and security of individuals.

Legal Framework for Data Protection in India

With the increasing incidence of data breaches and the inadequacy of existing legal safeguards, the necessity for a comprehensive legislative framework to protect personal data became evident. However, it would be incorrect to suggest that no legal provisions existed earlier. In fact, the foundation of data protection and privacy regulation in India can be traced to the Information Technology Act[5], 2000, along with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. These measures represented the initial legislative attempts to establish a structured framework for the protection of personal data and the preservation of individual privacy.The Information Technology Act, 2000 provides a statutory definition of "data" under Section 2,

[5]The Information Technology Act, 2000 (Act 21 of 2000)

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 4, April 2026 Impact Factor: 8.2

wherein data is described as any representation of information, knowledge, facts, concepts, or instructions that are prepared in a formalized manner and are intended to be processed, are being processed, or have already been processed in a computer system or network. Such data may exist in various forms, including digital storage formats, printouts, or other electronic media, thereby reflecting the broad scope of information covered within the digital ecosystem.

Further, Section 43A of the Act lays down provisions for compensation in cases involving failure to protect data. It stipulates that where a body corporate, engaged in handling sensitive personal data or information through a computer resource under its control, is negligent in implementing and maintaining reasonable security practices and procedures, and such negligence results in wrongful loss or wrongful gain to any person, the entity shall be held liable to pay compensation to the affected individual. This provision represents an important step towards accountability in cases of data breaches and unauthorized disclosure of personal information.The Explanation to Section 43A clarifies that "reasonable security practices and procedures" refer to measures designed to prevent unauthorized access, misuse, modification, disclosure, or damage to data. Such practices may be determined through agreements between parties, existing laws, or, in the absence of these, may be prescribed by the Central Government in consultation with relevant professional bodies. Additionally, the term "sensitive personal data" encompasses categories of personal information as may be notified by the Government, reflecting the evolving nature of data protection concerns.However, the Act also contains provisions that may limit the scope of privacy. Notably, Section 69 empowers the Central and State Governments to undertake surveillance measures, including the interception, monitoring, or decryption of data, on specified grounds such as national security, public order, sovereignty and integrity of India, or maintaining friendly relations with foreign states. While such powers are intended to serve legitimate state interests, they raise important concerns regarding potential encroachments on the Right to Privacy, particularly in the context of increasing risks of data breaches and misuse of personal information.

The Digital Personal Data Protection Act, 2023 (DPDP Act) was enacted by the Indian Parliament in August 2023, marking a significant milestone as India's first comprehensive legislation dedicated to the protection of personal data. The enactment of this law followed extensive deliberations and multiple revisions of earlier legislative proposals, particularly the Personal Data Protection Bill, 2019. The 2019 Bill envisaged the establishment of a Data Protection Authority (DPA) as a central regulatory body to oversee data protection across sectors. It laid down foundational principles aimed at preventing misuse of personal data by mandating informed consent, ensuring accuracy and security of data, and restricting its use to specified purposes.Additionally, the 2019 Bill recognized several rights of individuals, including the right to access, correct, erase, and port their data, along with the requirement for data to be deleted once its intended purpose was fulfilled. It also imposed obligations on entities to implement grievance redressal mechanisms, adopt "privacy by design" principles, and maintain transparency and robust security standards. The concept of "consent managers" was introduced as intermediaries to facilitate and manage user consent. However, the Bill also provided certain exemptions, particularly for state functions, public order, employment-related processing, health emergencies, and prevention of unlawful activities, thereby allowing specific entities to bypass consent requirements under defined circumstances.

The framework of the 2019 Bill was largely influenced by the recommendations of the Justice B.N. Srikrishna Committee, constituted in 2017 by the Ministry of Electronics and Information Technology, whose draft in 2018 formed the basis of India's evolving data protection regime. Despite its progressive features, the 2019 Bill faced several criticisms and limitations, which necessitated further refinements. These developments ultimately culminated in the enactment of the DPDP Act, 2023, based on the revised 2022 draft, reflecting a more streamlined and distinct legislative approach.

The DPDP Act defines "data" broadly as any representation of information, facts, concepts, opinions, or instructions capable of being processed by human or automated means. The Act emphasizes consent as the primary basis for processing personal data, subject to certain specified exceptions. It grants individuals significant rights, including the ability to access, correct, update, and erase their personal data, as well as the option to nominate a representative to exercise these rights. Special safeguards have also been incorporated for the processing of children's data.Furthermore,

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 4, April 2026 Impact Factor: 8.2

the Act imposes clear obligations on data fiduciaries, including adherence to purpose limitation, provision of notice regarding data collection and processing, implementation of appropriate security measures, and establishment of effective grievance redressal mechanisms. The Data Protection Board of India has been constituted to adjudicate complaints, address grievances, and impose penalties for non-compliance.

Overall, the DPDP Act represents a transformative shift in India's approach to data protection. It seeks to regulate the manner in which personal data is collected, processed, stored, and utilized, with the overarching objective of enhancing privacy and data security. The legislation aligns with global data protection standards and reflects a conscious effort to strengthen the protection of personal data in the digital age, thereby reinforcing the constitutional guarantee of the Right to Privacy under Article 21.

Shortcomings of the Digital Personal Data Protection Act, 2023

Although the Digital Personal Data Protection Act, 2023 represents a significant advancement in the domain of data privacy and security, it is not devoid of certain limitations. Some of the key shortcomings of the Act may be outlined as follows:

Firstly, the Act provides broad exemptions to certain entities and activities, particularly those related to the sovereignty and integrity of India, state security, friendly relations with foreign states, public order, and prevention of offences. Such exemptions allow security and investigative agencies to function beyond the purview of the Act, thereby raising concerns regarding potential encroachments on privacy.

Secondly, the Act excludes data processing undertaken for archival, statistical, or research purposes, provided that such data is not used to make decisions specific to an identifiable individual. While this exception may be justified in certain contexts, it nonetheless creates scope for misuse if not adequately regulated.

Thirdly, the government is empowered to relax key obligations such as accuracy, completeness, data retention, and notice requirements for specific categories of data fiduciaries, including startups. This relaxation, though aimed at promoting innovation, may dilute the effectiveness of data protection safeguards.

Another significant concern arises from the provision enabling the government to exempt certain data fiduciaries or classes thereof from the application of the Act for a specified duration, extending up to five years. The absence of clearly defined criteria governing such exemptions, including the grounds, categories of entities, and duration, grants wide discretionary powers to the government, which may undermine accountability and transparency.

Further, under Section 7(b), the Act permits the processing of personal data without explicit consent in cases where an individual has previously availed benefits or services from the State. This provision facilitates the creation of extensive governmental databases and may potentially bypass purpose limitation principles, as it allows continued use of personal data beyond its original intent.

Lastly, a major challenge lies in the effective implementation of the Act at the ground level. There exists a considerable lack of public awareness regarding data protection rights and obligations, which may hinder its practical enforcement. This concern is substantiated by recent studies indicating low levels of consumer awareness about data privacy laws in India.

In light of these limitations, while the Act is a progressive step, its efficacy in safeguarding the Right to Privacy, particularly in the context of data breaches, will largely depend on its implementation, oversight mechanisms, and future refinements.

Policy Recommendations for Enhancing Data Protection Laws

Although the DPDP Act, 2023 is a well-intentioned and carefully drafted legislation, it exhibits certain limitations that necessitate reform. In light of these shortcomings, the following recommendations may be considered to strengthen and refine India's data protection regime:

The 2019 Personal Data Protection Bill had proposed the establishment of a "Data Protection Authority (DPA)" with broader regulatory powers compared to the current "Data Protection Board (DPB)" under the DPDP Act. The DPB's

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 4, April 2026 Impact Factor: 8.2

role is largely limited to imposing penalties and issuing directions in cases of non-compliance, with insufficient authority to make regulations or proactively enforce data protection measures. There is a pressing need to review and enhance the powers of the DPB to ensure more effective implementation and enforcement of the law.

The DPDP Act confers "wide discretionary powers to the Government", exemplified by Section 9(4), which grants Data Fiduciaries considerable exemptions in the processing of children's data. The Act does not specify the criteria or basis for such exemptions, creating the potential for misuse of governmental authority. Clear guidelines and limitations should be prescribed to prevent undue exercise of discretionary powers.

A "contradiction exists between Sections 38(1) and 38(2)". While Section 38(1) emphasizes that the Act should be interpreted to remain compatible with other laws, Section 38(2) establishes that the provisions of the DPDP Act will prevail over any conflicting laws. This inconsistency complicates the interpretation and enforcement of the law and could impact certain industries. There is a need to harmonize sectoral regulations to reduce ambiguity and facilitate compliance.

Several provisions of the Act rely heavily on "rule-making powers of the Central Government". Given India's relatively nascent experience in data protection compared to developed nations, it is crucial that the Government adopts best practices from international frameworks while formulating rules and regulations, to ensure effective enforcement and alignment with global standards of data security and privacy.

III. CONCLUSION & SUGGESTIONS

Data protection and privacy are closely interconnected, functioning as two complementary aspects of the same principle, particularly in the context of the digital age. The enactment of the Digital Personal Data Protection Act (DPDP), 2023 represents a landmark development in India's data security landscape. The Act introduces several significant reforms aimed at safeguarding the personal data of individuals more effectively. Key provisions, including those related to informed consent, protection of children's data, and restrictions on legitimate data use, impose clear responsibilities on businesses and organizations, holding them accountable for breaches or violations of the law.

While the DPDP Act constitutes a major advancement in India's data privacy framework, it is not without limitations. Certain provisions may pose challenges to practical implementation, particularly given the current lack of widespread public awareness about the Act and its implications. Despite these challenges, the legislation marks an important step forward and has the potential to usher in a new era of enhanced data security, reinforcing the protection of individual privacy in India's increasingly digital society.