KDU Law Journal
General Sir John Kotelawala Defence University, Sri Lanka

Volume 04 Issue II
September, 2024
ISSN 2783 - 8870

Privacy Considerations in the Age of Digital Transformation in Emerging Bharat

Rumi Dhar[*]
Sonia Nath[**]

Abstract

In today's technologically advanced world, the concept of privacy has become more critical than ever before. With the digital transformation sweeping across the globe, individuals' privacy has come under intense scrutiny. This is especially true in emerging economies, where rapid technological advancements reshape the societal landscape. However, the digital revolution has also posed a significant challenge to individual privacy on digital platforms. The unauthorized access, collection, storage, and utilization of personal sensitive data have become a great concern. With the increasing reliance on digital platforms for communication, financial transactions, and other activities, individuals' risk having their sensitive information compromised. The enactment of the ***Digital Personal Data Protection Act 2023*** *aims to establish a comprehensive framework for processing and protecting personal sensitive data in India. The first section of the article discusses the various ways digital transformation has influenced privacy, and the second section discusses the existing legal provisions in India concerning data privacy. Finally, the article concludes with the need for robust data protection laws and regulations, as well as increased awareness and education on privacy rights and best practices for individuals and organizations. This paper aims to examine the aspects of data privacy in the context of digital transformation in emerging*

[*] Ph.D.(MGKVP,Varanasi), (LL.M. (Gauhati) LL.B. (Assam), Assistant Professor, Department of Law, Nagaland University, India
[**] LL.M. (Assam), B.A. LL.B. (Assam), Research Scholar, Department of Law, Nagaland University, India

Bharat, emphasizing the importance of balancing innovation with data protection.

Keywords: *Data Privacy and Protection, Digital Platform, Emerging Bharat, The Digital Personal Data Protection Act 2023*.

Introduction

The rapid advancement of technology and the digitalization of various aspects of our lives have brought about several benefits, but it has also given rise to serious privacy concerns[1]. The term ***"Emerging Bharat"*** refers to the rising economic power of India, which is experiencing a digital revolution of its own. In the age of digital transformation in emerging countries like India, it is crucial to address the potential risks and implications of these technological advancements on individuals' privacy. The notion of privacy in the digital age encompasses the right of individuals to control their personal information and to maintain a certain level of anonymity in their online activities[2]. With the widespread use of social media, online shopping, and digital communication, individuals constantly share their personal details without fully understanding the potential consequences[3]. Whether through social media posts, online purchases, or location tracking services, personal data is rapidly being generated and shared digitally.

---

[1] Godwin Oluwafemi Olaoye, "*Digital Privacy and Security in the Age of Information and Communication Technology"*, November 2023, 10.13140/RG.2.2.15449.70240, (accessed 3rd January 2024, 10:00 P.M) https://www.researchgate.net/publication/375289237_Digital_Privacy_and_Security_in_the_Age_of_Information_and_Communication_Technology

[2] Wanyi Fang, "*Socia Media Changed the Notion of Privacy*", Journal of Education, Humanities and Social Sciences, May 2023, Volume 4, DOI: 10.54097/ehss.v14i.8894, (accessed January 3rd 2024, 12:00 P.M) https://www.researchgate.net/publication/371579260_Social_Media_Changed_the_Notion_of_Privacy.

[3] Sara Quach, Park Thaichon, Kelly Martin, Scott Weaven and Robert W Palmatier, *"Digital Technologies: Tension in Privacy and Data*", Journal of the Academy of Marketing Science (2022) (Pages 1299-1323), DOI: https://doi.org/10.1007/s11747-022-00845-y, (accessed on January 3rd 2024, 10:00A.M), https://link.springer.com/article/10.1007/s11747-022-00845-y.

This has significantly blurred the lines between public and private information, raising concerns about digital data privacy and security.

In the digital age, one of the most significant privacy considerations is collecting and using personal data. With the increasing use of digital platforms and services, a growing amount of data about individuals is being collected. This data is often used for various purposes, including targeted advertising, personalized recommendations, and predictive analysis. While these personal data uses can enhance user experiences and provide valuable insights, they also raise concerns about the potential misuse or unauthorized access to this sensitive information.

In the context of India, where digital transformation is rapidly taking place, society needs effective regulations and policies to protect individuals' privacy rights[4]. The government and regulatory bodies must work to robustly safeguard personal information in the digital age. The objective of the paper is to explore the impact of digital transformation on privacy in emerging Bharat (India). The focus will be on how the rapid advancement in technology and the widespread adoption of digital services in the country are impacting the privacy rights of individual citizens. The article will analyze the challenges, risks and potential solutions related to privacy in this new age of connectivity and digitalization.

Research Methodology

The doctrinal methodology is adopted in writing the article titled *"Privacy Consideration in the Age of Digital Transformation in Emerging Bharat"* to explore the legal and regulatory frameworks that govern privacy rights in the country. This approach is well-suited as it allows for a detailed examination of the relevant laws

[4] Chong Wang, Nan Zhang and Cong Wang, "*Managing Privacy in the Digital Economy*", Fundamental Research, September 2021, Volume 1, Issue 5, (Pages 543-551) DOI: https://doi.org/10.1016/j.fmre.2021.08.009, (accessed January 3rd 2024, 12:00 P.M) https://www.sciencedirect.com/science/article/pii/S2667325821001552?via%3Dihub.

and policies that shape the privacy landscape in Bharat (India). By examining relevant statutes, regulations and case laws, the authors are able to provide valuable insight into the challenges and opportunities to identify gaps in existing data protection regulations and suggest ways in which the law could be strengthened to better safeguard privacy in the digital age.

Data protection laws and regulations that provide clear guidelines for collecting, using, and sharing personal data. Additionally, there is a need for increased awareness and education about privacy rights and best practices.

Data Privacy in the Digital Age and Its Importance

In today's digital age, privacy has taken on new dimensions with rapid technological advancements[5]. The proliferation of digital devices and platforms has made individuals access, share, and store personal information. This has raised important questions about what constitutes privacy in the digital age and why it is important to protect it. Data privacy is the right of individuals to control how their personal information is collected, shared, and used by others. Individuals constantly generate data through online activities, social media interactions and even through the use of smart devices, and this data contains sensitive information such as identity, financial details, location and even health records. Data privacy encompasses the right of individuals to control their personal data and to ensure that it is used in a responsible and ethical manner. Privacy is the fundamental right guaranteed to every citizen, yet its definition and scope have been continuously evolving continuously in the contemporary digital world.

Several case laws have established precedents for protecting privacy in the digital age. One such landmark case is *Carpenter v. United*

[5] Lance J Hoffman, "*Technology and Privacy Policy*", National Telecommunications and Information Administration United States Department of Commerce, (accessed 3rd January 2024, 10:00 P.M) https://www.ntia.gov/page/chapter-5-technology-and-privacy-policy#N_1_

States,[6] the Supreme Court held that law enforcement officials must obtain a warrant to access historical cell phone location data. The Court held that individuals have reasonable expectancy in the privacy of their location data, and therefore, law enforcement must meet the standard of probable cause to access such data[7]. This decision recognized the importance of protecting individuals' digital footprints from unwarranted intrusion by the government, thereby affirming the significance of privacy in the digital age.

In the case of *United States vs Jones*[8], the Supreme Court held that the government installation of a GPS tracking device on a suspect's car constituted a violation of the Fourth Amendment protection against unreasonable search and seizures. The court emphasized that the use of surveillance through GPS infringes the privacy of a person. This case highlighted the need for clear guidelines on the use of surveillance technology by government agencies and set a precedent for protecting individuals from unwarranted government intrusion.

In the case of *United States vs Miller*[9], addressed the privacy rights of financial records held by banks. The Supreme Court held that individuals do not have a reasonable expectation of privacy in their bank records, as they voluntarily disclose this information to a third party. This case establishes the "*third-party doctrine*", which allows law enforcement to access certain types of personal information without a warrant. This decision has significant implications for modern-day privacy concerns, particularly in the context of digital data collection and surveillance by tech companies and government agencies.

---

[6] Carpenter vs. United States (2018) 585 U.S

[7] Privacy Law Library, National Law University Delhi,(https://nluwebsite.s3.ap-south-1.amazonaws.com/uploads/carpenter-vs-united-states-5.pdf) accessed 5th December 2023.

[8] United States vs Jones (2012) 565 U.S. 400.

[9] United States vs Miller (1976) 425 U.S 435

Similarly, in the case of *Smith vs Maryland*[10], the court held that when individuals voluntarily provide information to a third party, they can't claim for infringement of privacy[11]. In this case, the court ruled that the installation of a pen register device on a suspect's phone did not constitute a violation of the Fourth Amendment. The Court reasoned that individuals had no legitimate expectation of privacy in the numbers dialed from their phones, as this information was already shared with the telephone company. This judgement has a significant impact on privacy in the digital age, where vast amounts of personal information are shared with third-party service providers on a daily basis.

These judgments demonstrate the need for a nuanced understanding of privacy expectations, particularly in the context of technology and surveillance practices. As new technologies continue to emerge and reshape the way in which information is collected and shared, it is imperative for legal frameworks to adopt and provide adequate safeguards for individuals' privacy rights.

In India, the right to privacy is considered a fundamental right under Article 21[12] of the Constitution, which guarantees the right to life and personal liberty. The Supreme Court of India has recognized the importance of privacy in several landmark cases, including the recent judgment in *Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others*[13], in which a nine-judge bench unanimously held that privacy is a fundamental right protected under the Constitution of India. The judgment emphasized protecting personal autonomy and the right to control one's personal information in the digital age. The court recognized the need for robust data protection laws and strict

[10] Smith vs Maryland (1979) 442 U.S. 735

[11] Privacy Law Library, National Law University, Delhi, (https://nluwebsite.s3.ap-south-1.amazonaws.com/uploads/carpenter-vs-united-states-5.pdf) accessed 15th December 2023.

[12] "Article 21 of the Indian Constitution- Protection of life and personal liberty- No person shall be deprived of his life and personal liberty except according to procedure established by law".

[13] Justice K S Puttaswamy (Retd) & Anr. Vs Union of India & Ors. (2017) 10 SCC 1, AIR 2017 SC 4161.

regulations to safeguard individuals' privacy rights. This decision has set a significant precedent for protecting privacy in the digital sphere.

Another notable case is the European Court of Justice's ruling in *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems*[14] *(the Schrems II case),* invalidating the EU-U.S[15]. Privacy Shield agreement due to concerns over U.S. government surveillance activities. This decision highlighted the need for robust legal safeguards to protect individuals' personal data from indiscriminate access by foreign governments. The judgment underscored the significance of privacy rights in the context of international data transfers, particularly in the digital age where data easily flows across borders[16].

Another important Indian case highlighting privacy's significance in the digital age is the Aadhaar judgment. In *Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors*[17]. (2018), the Supreme Court upheld the constitutional validity of the Aadhaar Act, while imposing several key restrictions to protect the privacy rights of individuals. The court ruled that Aadhaar, India's biometric identification system, could not be made mandatory for certain services and that strict measures must be adopted to protect the security confidentiality of Aadhaar data[18].

In the digital age, it is essential to recognize the importance of privacy for several reasons. Firstly, privacy is an integral part of

[14] Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems C-311/18.

[15] Dillon Swensen*, "Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems: Where Do We Go From Here*?", Maryland Journal of International Law, 2022, Volume 36, Issue 1, (accessed 5th January 2024, 3:00 P.M) https://digitalcommons.law.umaryland.edu/mjil/vol36/iss1/6

[16] The Definitive Guide to Schrems II, (Data Guidance 22 November 2022) (https://www.dataguidance.com/resource/definitive-guide-schrems-ii#Schrems%20II%20Case), accessed on 15th December 2023.

[17] Justice K S Puttaswamy (Retd) & Anr. Vs Union of India & Ors. (2019) 1 SCC 1

[18] Privacy Law Library, National Law University, Delhi, (https://nluwebsite.s3.ap-south-1.amazonaws.com/uploads/justice-ks-puttaswamy-and-ors-vs-union-of-india-uoi-and-ors-5.pdf), accessed 15th December 2023.

individual dignity and autonomy[19]. Additionally, privacy is crucial for safeguarding individuals from potential harms such as identity theft, fraud, and cyberstalking[20]. Moreover, in a democratic society, privacy also plays a vital role in fostering freedom of expression and association, as individuals are less likely to freely express themselves or associate with others if they fear their personal information will be misused.

From the *Carpenter v. United States judgements*[21]*, Schrems II case*[22], *Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors*[23] it becomes evident that courts are increasingly recognizing the significance of privacy in the digital age and are taking steps to ensure its protection.

Impact of Digital Transformation on Privacy:

The digital revolution has created countless opportunities for innovation and efficiency, but it has also raised serious concerns about privacy and data security. The impact of digital transformation on privacy is the erosion of anonymity. In the digital age, it is becoming increasingly difficult to remain anonymous online, as our digital footprint continues to expand with each click, like, and share. This loss of anonymity has serious implications for individuals who value their privacy, as it can lead to targeted advertising, surveillance, and potential misuse of personal sensitive data.

Moreover, if we look at the impact of digital technology on privacy within the framework of Emerging Bharat, increasing reliance on biometric identification technologies, such as Aadhaar, has further

[19] Dorota Mokrosinska, "*Privacy and Autonomy: On Some Misconceptions Concerning the Political Dimensions of Privacy"*, Law and Philosophy, April 2018, Volume 37 No. 2 (Pages 117-143), (accessed February 6th, 2024, 3;00 P.M), https://www.jstor.org/stable/44980918

[20] Dr. Mark Van Rijmenam, "*Privacy in the Age of AI: Risks, Challenges and Solutions*", The Digital Speaker February 17, 2023, (accessed 5th January 2024, 10:00 P.M) https://www.thedigitalspeaker.com/privacy-age-ai-risks-challenges-solutions/#:~:text=Privacy%20is%20crucial%20for%20a,for%20personal%20dignity%20and%20respect.

[21] 585 U.S (2018).

[22] *Supra note* 14.

[23] Justice K S Puttaswamy (Retd) & Anr. Vs Union of India & Ors. (2019) 1 SCC 1

amplified privacy concerns in India. While biometric authentication offers a convenient and secure way to verify individual's identities, it also raises a question about the potential misuse of biometric data and the erosion of individual's privacy rights. The Supreme Court of India, in its landmark judgement on Aadhaar, held that the government cannot compel individuals to link their Aadhaar number to various services and has highlighted the importance of striking a balance between security and privacy in the digital age. The effects of digital transformation on privacy are:

In today's technologically advanced world, the concept of privacy has become more critical than ever before. With the digital transformation sweeping across the globe, individual privacy in the digital sphere has been intensely scrutinized. The impact of digital transformation on privacy has increased concern in the legal community. The proliferation of digital technologies has led to a major shift in how personal information is collected, processed, stored, and handled. With the advent of social media, online transactions, and the Internet of Things, individuals are constantly sharing their personal information in the digital realm.. The implications of digital transformation on privacy are:

One noteworthy impact of digital transformation on privacy is companies and governments' increased collection and use of personal data. In the *2018 Cambridge Analytica scandal*[24], in which it was revealed that the political consulting firm had collected personal data from millions of Facebook users without their consent. This case highlighted the substantial privacy risks associated with companies' large-scale collection and use of personal data for targeted advertising and political campaigning. The scandal ultimately led to increased scrutiny of data privacy practices and has increased the understanding of the necessity for stronger legal

[24] Katie Harbath and Collier Fernekes, "*History of Cambridge Analytica Controversy*", (Bipartisan Policy Centre, 16 March 2023), (https://bipartisanpolicy.org/blog/cambridge-analytica-controversy/), accessed 10th December 2023.

protections for personal information.

Another significant impact of digital transformation on privacy is the potential for data breaches and cybersecurity threats to personal information. As per the report of the Hindu on 7th November 2023, 815 million Indian citizens' personal data, including Aadhar numbers and passport details, were sold on the dark web[25]. The rapid exchange of personal information in the digital sphere has made it difficult for individuals to track how their personal data is used.

The emergence of the Internet of Things (IoT) devices has further blurred the line between the physical and digital worlds, creating new opportunities for surveillance and data collection. Smart devices such as connected cameras and voice assistance can potentially record and analyze private conversations or movements, raising concerns about the erosion of privacy boundaries.

A significant aspect of digital transformation is the rise of cybersecurity threats and data breaches. The increased reliance on digital technologies has made personal data vulnerable to unauthorized access and misuse.

Artificial Intelligence (AI) and Machine Learning (ML) systems rely on vast amounts of data to train their algorithms and make decisions. This data includes sensitive information such as personal details, financial records, health data and more. As these systems become more advanced and pervasive, the risk of data breaches and privacy violations also increases. Moreover, there is a lack of transparency and control over how personal data is used by AI and ML systems. The lack of transparency can erode trust and lead to concern about privacy breaches.

[25] Nabeel Ahmed, *"How the personal data of 815 million Indians got breached- Explained"*, The Hindu, (7th November 2023), (accessed 20th December 2023, 6:00 A.M), https://www.thehindu.com/sci-tech/technology/how-the-personal-data-of-815-million-indians-got-breached-explained/article67505760.ece,

Emergence of big data analytics and artificial intelligence has raised concerns about the potential for profiling of personal data. The digital transformation has significantly impacted privacy rights in India. The rapid exchange of personal sensitive data in the digital realm has raised concerns about consent, cybersecurity threats, and potential profiling. The *Cambridge Analytica scandal*[26], *Equifax Data Breach*[27], *Aadhaar Data Breach*[28], *SBI Data Breach*[29], *Cowin Data Leak*[30] in India, and data breaches worldwide are important reminders of the potential consequences of inadequate privacy safeguards in this digital era.

Legal and Regulatory Framework:

As technology continues to evolve at an unprecedented pace, digital India, i.e. the digital transformation of India, becomes a priority for government and industry. The rapidly expanding digital landscape has created new economic development and innovation opportunities. However, the widespread adoption of digital technologies has also raised the importance of privacy in the digital age and challenges that need to be addressed.

In response to these and other privacy concerns raised by digital transformation, lawmakers worldwide have sought to strengthen

[26] Katie Harbath, Collier Fernekes, "*History of Cambridge Analytic Controversy*", Bipartisan Policy Centre, May 16, 2023, (accessed February 12, 2024, 3:00P.M) https://bipartisanpolicy.org/blog/cambridge-analytica-controversy/#:~:text=Cambridge%20Analytica%20claimed%20to%20be,fully%20shut%20down%20in%202015.

[27] Equifax Data Breach, Electronic Privacy Information Centre, (accessed February 12, 2024, 10:00 P.M), https://archive.epic.org/privacy/data-breach/equifax/

[28] Nabeel Ahmed, "*How the Personal Data of 815 million Indians got Breached Explained*", The Hindu November 07, 2023, (accessed 20th December 2023, 6:00 A.M), https://www.thehindu.com/sci-tech/technology/how-the-personal-data-of-815-million-indians-got-breached-explained/article67505760.ece

[29] Bidisha Saha*, "Over 12,000 SBI employee data leaked on Telegram channels",* India Today July 11, 2023 (accessed January 5th 2024, 3:00 P.M) https://www.indiatoday.in/india/story/telegram-channels-leak-data-of-12-thousand-sbi-employees-ignored-some-red-flag-2405024-2023-07-11

[30] John Xavier, *"Explained What does the alleged CWIN data leak reveal?",* The Hindu, June 18, 2023, (accessed 5th February 2024, 4:00 P.M) https://www.thehindu.com/sci-tech/technology/explained-what-does-the-alleged-cowin-data-leak-reveal/article66980831.ece.

data privacy laws and regulations. The *European Union's General Data Protection Regulation (GDPR)*[31] was enacted in 2018. The EU GDPR has benchmarked other countries' data protection regulations. In response to these concerns, the Indian government enacted the *Information Technology Act of 2000*[32] and the *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011*[33] *(IT Rule 2011),* which regulate electronic data collection, processing, and storage. Furthermore, the legislature enacted the *Digital Personal Data Protection Act 2023*[34] to strengthen data privacy governance in India.

The impact of digital transformation on privacy raises intricate legal and ethical considerations that demand a judicious approach to regulation and governance. The Indian legal landscape has evolved significantly to address these challenges, recognizing the right to privacy as a fundamental right and enacting the Digital Personal Data Protection Act 2023.

The Digital Personal Data Protection Act 2023[35]

The Digital Personal Data Protection Act of 2023 stands as a landmark legislation aimed at safeguarding the digital privacy of individuals in the rapidly evolving landscape of the digital age. The provisions of this act are designed to address the growing concerns surrounding the collection, storage, and use of personal data in the digital realm. They are expected to have a profound impact on the way businesses and

[31] Regulation (EU) 2016/679 (General Data Protection Regulation) OJL 119, https://gdpr-info.eu/

[32] The Information Technology Act 2000 (Act No. 21 of 2000), Gazette Notification dated 9th June 2000, https://www.indiacode.nic.in/bitstream/123456789/1999/1/A2000-21%20%281%29.pdf

[33] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Gazette Notification dated 11th April 2011, https://www.meity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf

[34] Digital Personal Data Protection Act 2023 (Act no 22 of 2023), Gazette Notification dated 11th August 2023, https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

[35] *Supra note* 34.

organizations handle sensitive information.

Section 6[36] and *section 4 (1) (a)*[37] of the Digital Personal Data Protection Act require explicit consent from individuals to collect and process their personal data. This means that organizations will no longer be able to arbitrarily gather data without the knowledge and consent of the individuals involved. These provisions of the act are crucial in protecting the privacy of individuals and preventing the misuse of personal information for commercial or other purposes.

Furthermore, *Section 4(1)*[38] of the act establishes clear guidelines for collecting, processing and storing personal data. *Section 11*[39], the right to access information about personal data; the data principal has the right to request information about their personal data being processed and with whom their data has been shared. *Section*

[36] Section 6 of the Digital Personal Data Protection Act-"(1) The consent given by the Data Principal shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose". *Supra note* 34.

[37] Section 4-(1)(a)" A person may process the personal data of a Data Principal only in accordance with the provisions of this Act and for a lawful purpose, -(a) for which the Data Principal has given her consent", *Supra note* 34.

[38] "Section 4- Grounds for processing of personal data- (1) A person may process the personal data of a Data Principal only in accordance with the provisions of this Act and for a lawful purpose, -
(a) for which the Data Principal has given her consent; or
(b) for certain legitimate uses." *Supra note* 34.

[39] Section 11 – Right to access information about personal data- (1) The Data Principal shall have the right to obtain from the Data Fiduciary to whom she has previously given consent, including consent as referred to in clause (a) of section 7 (hereinafter referred to as the said Data Fiduciary) for processing of personal data, upon making to it a request in such manner as may be prescribed,-
(a) a summary of personal data which is being processed by such Data Fiduciary and the processing activities undertaken by that Data Fiduciary with respect to such personal data;
(b) the identities of all other Data Fiduciary and Data Processor with whom the personal data has been shared by such Data Fiduciary, along with a descriptive of the personal data so shared; and
(c) any other information related to the personal data of such Data Principal and in processing, as may be prescribed.
(2) Nothing contained in clause (b) or clause (c) of subsection (1) shall apply in respect of the sharing of any personal data by the said Data Fiduciary with any other Data Fiduciary authorized by law to obtain such personal data, where such sharing is pursuant to a request made in writing by such other Data Fiduciary for the purpose of preventing or detection or investigation of offences or cyber incidents, or for prosecution or punishment of offences. *Supra note* 34.

12[40], the right to correction and erasure of personal data. The data principal can request that the fiduciary correct, complete, update and erase personal data when it is no longer required. *Section 13*[41], the right of grievance redressal, data principals have the right to register their grievances with a data fiduciary; and *Section 14*[42], the right to nominate, the data principal has the right to nominate any other individual to exercise their right. This ensures that individuals have greater control over how their information is used. The act aims to empower individuals and give them greater control over their digital identities by establishing these rights.

[40] Section 12- Right to Correction and erasure of personal data- (1) Data Principal shall have the right to correction, completion, updating and erasure of her personal data for the processing of which she has previously given consent, including consent as referred to in clause (a) of section 7, in accordance with any requirement or procedure under any law for the time being in force.
(2) A Data Fiduciary shall, upon receiving a request for correction, completion or updating from a data Principal-
(a) correct the inaccurate or misleading personal data;
(b) complete the incomplete personal data; and
(c) update the personal data.
(3) A Data Principal shall make a request in such manner as may be prescribed to the Data Fiduciary for erasure of her personal data, and upon receipt of such a request, the Data Fiduciary shall erase her personal data unless retention of the same is necessary for the specific purpose or for compliance with any law for the time being in force. *Supra note* 34.

[41] Section 13- Right of grievances redressal- (1) Data Principal shall have the right to have readily available means of grievance redressal provided by a Data Fiduciary or Consent Manager in respect of any act or omission of such Data Fiduciary or Consent Manager regarding the performance of its obligations in relation to the personal data of such Data Principal or the exercise of her rights under the provisions of this Act and the rules made thereunder.
(2) The Data Fiduciary or Consent Manager shall respond to any grievances referred to in sub-section(1) within such period as may be prescribed from the date of its receipt for all or any class of Data Fiduciaries.
(3) The Data Principal shall exhaust the opportunity of redressing her grievance under this section before approaching the Board. *Supra note* 34.

[42] Section 14- Right to nominate- (1) A Data Principal shall have the right to nominate, in such manner as may be prescribed, any other individual, who shall, in the event of death or incapacity of the Data Principal, exercise the right of the Data Principal in accordance with the provisions of this Act and the rules made thereunder. (2) For the purposes of this section, the expression “incapacity” means inability to exercise the right of the Data Principal under the provisions of this Act or the rules made thereunder due to unsoundness of mind or infirmity of body. *Supra note* 34.

Obligations of the data fiduciary *Section 8 (4)*[43] and *(5)*[44] of the act require that the data fiduciary must ensure the security and integrity of personal data. To ensure security, the data fiduciary must implement security measures to protect against data breaches and unauthorized access and maintain detailed records of data processing activities.Lastly, the act introduces strict penalties for non-compliance, including hefty fines and potential legal action. By imposing these consequences, the act seeks to encourage businesses and organizations to take data protection seriously and prioritize the privacy rights of individuals. These measures ensure compliance with the act but also serve as a deterrent against negligence or misconduct in handling personal data. Overall, the Digital Personal Data Protection Act 2023 represents a significant step forward in strengthening the rights of individuals in the digital space and promoting responsible data practices. However, it comes with several limitations that need continuous review and refinement. Firstly, the Act grants the government substantial leeway to exempt any of its agencies from the provisions of the Act. This raises concerns about the potential for misuse, especially regarding surveillance and privacy. Secondly, limited scope of applicability, the Act primarily applies to digital data and does not comprehensively address non-digital data. In an era where data is increasingly integrated across digital and physical platforms, this limitation could leave a significant gap in data protection. Thirdly, the Act mandates data breach notifications, but it does not specify stringent timelines or the exact nature of information that must be disclosed to affect individuals. This lack of specificity can hinder effective response and remediation efforts.

[43] Section 8(4) - A data Fiduciary shall implement appropriate technical and organizational measures to ensure effective observance of the provisions of this Act and the rules made thereunder. *Supra note* 36.

[44] Section (6) - A Data Fiduciary shall protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguard to prevent personal data breach. *Supra note* 34.

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011[45]

The regulatory framework on data privacy in India was initially governed by the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. These rules were introduced under the Information Technology Act of 2000 and have been a cornerstone of India's approach to data privacy. The rules seek to regulate the collection, use, and disclosure of sensitive personal data or information and mandate certain security measures for its protection. Additionally, they outline requirements for obtaining consent from individuals to collect and use their personal data and establish a framework for transferring such data outside India.

Transfer of information under *Rule 7*[46] of IT Rule 2011 is particularly significant in the age of globalization, where data is often transferred across international borders. The rule requires organizations to ensure that the personal data they transfer is subject to the same level of protection as it would be in their home jurisdiction and to obtain the necessary consent from individuals for such transfers. This provision upholds individuals' privacy rights even in an increasingly interconnected world.

[45] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Gazette Notification dated 11th April 2011, https://www.meity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf

[46] Rule 7- Transfer of Information- A body corporate or any person on its behalf may transfer sensitive personal data or information including any information, to any other body corporate or a person in India, or located in any other country, that ensures the same level of data protection that is adhered to by the body corporate as provided for under these Rules. The transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer. *Supra note* 45.

Rule 8(1)[47], Reasonable Security Practices and Procedures of IT Rule 2011, focuses on data protection and privacy. The rule requires organizations to implement appropriate security measures to protect personal data from unauthorized access, disclosure, alteration, or destruction. This includes implementing access controls, encryption, and secure data storage practices. The IT Rules 2011 concerning privacy are an important step towards establishing a legal framework for safeguarding individuals' privacy rights in the digital age. By implementing these provisions, proactive measures ensure the privacy and security of information in the digital age.

Addressing Privacy Concerns in the Age of Digital Transformation

The emergence of new technologies such as IoT (Internet of Things), artificial intelligence (AI), machine learning, and big data analytics has further complicated the privacy landscape. These technologies have the potential to analyze and interpret vast amounts of personal data, raising concerns about the potential misuse or unauthorized access to such information. The current legal framework for protecting privacy is a topic of considerable debate with both strengths and weaknesses.

Strengths of Existing Legal Frameworks:

(a) Constitutional recognition of the right to privacy as a fundamental right by the Supreme Court of India, particularly through the landmark judgement of *Justice K S Puttawamy*

[47] Rule 8(1) Reasonable Security Practices and Procedures-A body corporate or a person on its behalf shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business. In the event of an information security breach, the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandate under the law, that they have implemented security control measures as per their documented information security programme and information security policies. *Supra note* 45.

(Retd). V Union of India (2017). This provides a strong legal foundation for privacy protection.

(b) The Act puts forth various provisions and guidelines to ensure that an individual's privacy is safeguarded and that their personal information is not misused or exploited by unauthorized parties.

Weaknesses of the Existing Legal Framework:

(a) Delay implementation of data protection legislation leaves a significant gap in the legal framework as technology is developing at an unprecedented rate making comprehensive data protection uncertain.

(b) The Act does not adequately address emerging technologies and data practices such as artificial intelligence and data analytics, which pose new challenges to data privacy.

(c) The Act does not specifically address issues such as data localization and cross-border data sharing, which are key concerns in the digital age.

In India, where digital literacy levels are still evolving, there is a pressing need for measures to educate and empower individuals to understand the implications of sharing their personal data online and to make informed choices about their privacy.

The Potential Solutions to Address Privacy Considerations in the Age of Digital Transformation are as Follows:

(a) Implementing EU GDPR-like principles for cross-border data transfer.

(b) Strengthening data protection laws to keep pace with technological advancements and changing privacy concerns.

(c) Implementing such measures creates a legal framework that ensures the privacy rights of individuals are respected and protected in the age of digital transformation.

(d) By developing privacy-enhancing technologies. These technologies are designed to give individuals greater control over their personal information while using digital platforms and services.

(e) By increasing public awareness and education about privacy rights and best practices for personal information online.

(f) Efforts should be made to promote digital literacy so that individuals can better understand their rights and take proactive measures to protect their privacy when interacting with digital technologies.

Conclusion

"Privacy is not an option, and it shouldn't be the price we accept for just getting on the Internet."

- Gary Kovacs-[48]

In conclusion, as Bharat (India) undergoes a significant digital transformation, addressing the privacy considerations accompanying this process is essential. Prioritizing the protection of personal sensitive data, ensuring transparency and consent, and implementing strong regulations and policies, India can harness the benefits of digital transformation while safeguarding the rights to privacy of its citizens. It is crucial for all stakeholders, including businesses, organizations, government, and individuals, to work together to create a safe and secure digital environment that respects and protects privacy in digital transformation.

The phase of digital transformation presents complex challenges for privacy protection. By establishing comprehensive data protection laws and regulations, developing privacy-enhancing technologies, increasing public awareness and education, and promoting collaboration, it is possible to address privacy considerations in the age of digital transformation. These solutions can help create a legal and technological framework that enables individuals to have

[48] https://www.us-ignite.org/wp-content/uploads/2021/06/USIgnite-Civic-Trust-Guide_Sec3_Privacy.pdf

greater control over their personal information and ensures privacy protection in the digital age. India's regulatory framework on data privacy is undergoing significant development. Introducing the Digital Personal Data Protection Act 2023 represents a step towards modernizing and strengthening the country's data protection laws. However, there is still a need for robust enforcement mechanisms and continued vigilance to ensure that individuals' privacy rights are adequately safeguarded in the digital age.