IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Critical Analysis Of Privacy Implications In The Digitalized India

Ms. Muskan Sharma
Teaching Assistant & Research Fellow
School of Law
The NorthCap University, Gurugram, Haryana

Abstract: The 21st century has witnessed an unprecedented surge in technological advancements globally, leading to a digital revolution across various aspects of our lives. While embracing the benefits and efficiency of the digital age, concerns regarding data privacy have become increasingly significant. The digital landscape is characterized by an intricate network of interconnected platforms, devices, and applications, all contributing to the generation and sharing of vast amounts of personal data. This article seeks to examine the implication related to privacy rights of women within the digitalized environment. It aims to explore how women's privacy is compromised in digital spaces, including issues such as impersonation or deepfake incidents, online harassment, and data breaches. Additionally, the paper will evaluate the effectiveness of existing legal frameworks and regulations designed to protect privacy rights in the digital realm, with a particular emphasis on their ability to address the unique challenges faced by women.

Key Terms - Data Privacy; Data breach; Women; Security Risk; Digital Personal Data Protection Act 2023.

I. INTRODUCTION

In our rapidly evolving digital environment, where technology permeates all aspects of daily life, the right to privacy serves as a crucial foundation protecting individual autonomy and dignity. Privacy is a fundamental human right[1] that shields individuals from unauthorized access, fostering personal autonomy in accessing their own data. It transcends mere legality, serving as a barrier against encroachments on personal autonomy. This right extends beyond physical boundaries, encompassing the freedom to make decisions regarding one's body, relationships, and identity without undue influence or coercion.

Privacy is not merely about maintaining secrecy; rather, it is about being in a state of solitude and freedom from public scrutiny or interference, as defined by the Oxford English dictionary[2]. In an era of the rapid technology innovations and digital transformation, the concept of privacy has emerged as a significant and

[1] "Privacy and Human Rights - Overview." 2024. Gilc.org. 2024, available at https://gilc.org/privacy/survey/intro.html

[2] Manzar, Osama, and Udita Chaturvedi. n.d. "UNDERSTANDING the LACK of PRIVACY in the INDIAN CULTURAL CONTEXT Opinion Piece." available at https://defindia.org/wp-content/uploads/2017/09/Understanding-the-Lack-of-Privacy-in-Indian-Cultural-Context.pdf.

multidimensional issue, particularly in a country like India. The digital revolution has fundamentally altered how people connect, communicate, and go about their daily lives, resulting in unparalleled personal data production and sharing. As India continues to embrace digital technologies in sectors such as governance, commerce, healthcare, and social interactions, consequences for privacy have gotten more complex and varied.

The development of technology has been extremely beneficial to humans. Nevertheless, many of our liberties are currently at danger due to the advancement of technology. As the technology advances and involves data that is actively gathered and utilized in the marketplace, the right to privacy is becoming increasingly important concern. Furthermore, the right to privacy is intricately linked to data protection in today's technologically advanced and interconnected world, although safeguarding it has become increasingly challenging. The shift towards digitalization has given rise to numerous criminal activities, including data fraud, cyber harassment, and the creation of deepfake videos. Additionally, the proliferation of technology has led to the existence of numerous websites, social media platforms, and dating applications where users input their personal information. This sensitive information is then exploited by hackers for data breaches. For instance, when users provide their private details to websites or log in to applications like Truecaller, WhatsApp, Instagram, or dating platforms such as Tinder and Bumble for various purposes like business or social interaction, their data is often misused.

Therefore, the Hon'ble Supreme Court (SC) in 2017 recognized "right to privacy" as a fundamental right under article 21 of the Indian Constitution of India[3]. In the words of the SC, "the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution"[4]. The "right to privacy" has interpreted in many ways. According to black law dictionary "right to privacy" means "various rights recognized as inherent in the concept of ordered liberty[5]." In other words, this right means the people has a freedom to protect right to fundamentally choose how they want to live their lives and interact with their families, other people, and their interpersonal connections and activities[6]. Therefore, right to privacy is closely related to the protection of data which in this technological and globalized world, has become very difficult to achieve. The process of going digital has led to the emergence of several criminal practices, including data fraud, cyber harassment, and so on. For instance, when user provide their private information to websites and for login in any applications like true caller, WhatsApp etc. for business and interaction, the data often be misused. There is no express legislation in India, that govern acquisition, archiving, surveillance, recording, accessing, processing, dissemination, maintenance, etc. of personal data. Further, the right to privacy is also recognized internationally as human right under Article 12 of Universal Declaration of Human Rights (UDHR), states "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks[7]." In other

[3] Justice K.S. Puttaswamy (Retd.) & Anr. Vs. Union of India & Ors., AIR 2017 SC 4161
[4] Ibid
[5] Yashraj Bais, Privacy and Data Protection in India: An Analysis, 4 (5) *International Journal of Law Management & Humanities*, 1793 - 1804 (2021)
[6] Ibid
[7] Article 12 of the Universal Declaration of Human Rights, 2024.

words, everyone has a liberty not to get interfered with his/her privacy, and not to be permitted to defame his/her reputation in society.

For securing the "right to privacy" under Article 17 of International Covenant on Civil and Political Rights 1966 (ICCPR), stated "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation[8]" and Article 8 of the European Convention of Huma Rights 1950 (ECHR), states that "everyone has the right to respect for his private and family life, his home and his correspondence[9]" also get adopted internationally. Although the various international conventions consensus about data privacy and data protection, still there is no universal definition of privacy.

In India, Information Technology Act of 2000 was enacted to deals with cyber fraud, cybercrime, and the webs of e-commerce, it's provisions is widely related for curbing the crimes under the cyber space, which is extensively linked with Data Protection and Privacy[10]. The Judiciary also play very crucial role in protection the personal data in digital India. When it comes to making decisions in matters involving the violation of an individual's fundamental rights as guaranteed by PART III of the Indian Constitution, the judiciary is always extremely perceptive and sensitive. Further the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules of 2021 and Digital Personal Data Protection Act of 2023 (DPDP Act) was enacted for the purpose of protect the rights of Digital Nagriks[11] and the protection of the personal data respectively. Despite of these legislative enactments for the protection of personal data and digital rights of individual, still the privacy and dignity of an individual, especially women, are at stake with the technological development. Therefore, the "right to privacy" is seriously threatened in today's digital age by individuals' growing dependence on the internet, especially social media platforms. This risk to personal information also increases as people use technology.

[8] "Freedom from Interference with Privacy, Family, Home and Correspondence or Reputation." 2023. Humanrights.gov.au. 2023. available at https://humanrights.gov.au/our-work/rights-and-freedoms/freedom-interference-privacy-family-home-and-correspondence-or.

[9] *Article 8: Respect for your private and family life | EHRC*. (2021). Equalityhumanrights.com. available at https://www.equalityhumanrights.com/human-rights/human-rights-act/article-8-respect-your-private-and-family-life#:~:text=This%20right%20means%20that%20the,permission%2C%20except%20in%20certain%20circumstances

[10] Renuga, M. (n.d.). Right to privacy in digitalized India, available at https://acadpubl.eu/hub/2018-120-5/4/339.pdf

[11] Government of India, "Government notifies Amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 for an Open, Safe & Trusted and Accountable Internet" (2021).

II. LEGAL FRAMEWORK FOR DATA PROTECTION IN INDIA

In India, the Information Technology Act (IT Act) was enacted in 2000 to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce[12]." As per the section 2(1)(o) of the IT Act define "data" as "means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer[13]". Further, section 66E of IT Act, constitutes the offence of violation of privacy, that is whosoever, intentionally captures, transmits or publishes the image of any person without the consent, shall be punishable with imprisonment which may extend to three years or with fine up to Rs. 2 Lacks or both[14]. Moreover, section 66C of IT Act, constitutes the offence of fraudulently using the password of any person, as today the computer resource of any person contains his/her private data which is expected not be observed or recorded by an anonymous individual without permission, if he does so, it shall be punishable with imprisonment with may extend to three years or fine up to Rs. 1 lacks[15].

The volume of data generated has increased due to India's drive towards digitalization, widespread usage of the internet, and a wide range of applications on devices for a variety of uses[16]. It is clear that data generation has benefited people and improved their efficiency while also contributing to the advancement of society. Unfortunately, data generated is not safeguarded and is frequently exploited, infringing on an individual's right to privacy. As discussed the issue of right to privacy was discussed in Puttaswamy case[17], that challenged the validity of the "Aadhaar Card Scheme" required the people to submit their biometric data for the identity card which would be mandatory for access to government services and benefits. It was contended that this scheme violates the right of the people under article 12 of the COI. This case entertained by 9 judge bench on July 2017. The SC decide the case while taking reference of various cases like M.P. Sharma v. Satish Chandra[18] , and Kharak Singh v. State of Uttar Pradesh[19], and held that the Constitution guaranteed the right to privacy as an intrinsic part of the right to life and personal liberty under Article 21.

In India, there is implied legislation which govern the technological threat to data like Information Technological Act of 2000 (Amended in 2008), Indian Contract Act of 1872 and Indian Constitution. Under section 43A of IT Act, stated "where a body corporate, possessing, dealing or handling any sensitive personal

[12] "Home | Ministry of Law & Justice | GoI." 2024. Lawmin.gov.in. 2024. available at https://lawmin.gov.in/

[13] The Information Technology Act, 2000 (Act 21 of 2000), s. 2(1)(0).

[14] Rai, N. (n.d.). Right to Privacy and Data Protection in the Digital Age - Preservation, Control and Implementation of Laws in India. *IJLJ*, *11*(1). Retrieved February 5, 2024, from https://ir.nbu.ac.in/bitstream/123456789/4009/1/IJLJ%20-%20Vol.%2011%20No.%201%20%28Part%20III%29%20Article%20No%209.pdf *(Privacy and Data Protection in India: An Analysis - International Journal of Law Management & Humanities, 2021).*

[15] Boruah, J., & Das, B. (2021, March 16). *RIGHT TO PRIVACY AND DATA PROTECTION UNDER INDIAN LEGAL REGIME*. Ssrn.com. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3827766

[16] Supra note 14

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

[18] M. P. Sharma and Others vs Satish Chandra (1954) 1 SCR 1077

[19] *Kharak Singh vs the State of U. P. & Others AIR 1963 SC 1295*

data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected" and section 72A of IT Act states "Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both" of the IT Act was inserted in 2008 for the protection of data, states that there is liability of the body corporate if there is any infringement of data.

Recently, the Indian Parliament has passed the Digital Personal Data Protection Act of 2023 (DPDP Act), marking the first cross-sectoral law on personal data protection in India after over a decade of deliberations[20]. The Act will significantly change the existing data protection regime and replace the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. Since 2018, the Indian Government has been working on a standalone data protection legislation, with four drafts introduced in Parliament. The final draft is a pillar for the enactment of the DPDP Act. The DPDP Act governs personal data, digital personal data, and data processors, similar to GDPR but narrower and does not include entities outside India monitoring Data Principals' behaviour[21]. It imposes narrowly defined obligations for processing digital personal data, establishes purpose limitation obligations, and creates rights for individuals whose data are collected and used. It also establishes a supervisory authority, the Data Protection Board, that investigates complaints and issues fines, but lacks the power to issue guidance or regulations.

The DPDP Act extends the scope of personal data processing to all entities, regardless of size or private status. It borrows from the European Union's General Data Protection Regulation (GDPR) approach and has significant extraterritorial application if the processing of digital personal data is related to any activity related to the offering of goods or services to Data Principles within India[22]. Section 3(c) includes a household exemption when data processing occurs for solely personal or domestic purposes[23].

With the advancement of technology, it is very easier to infringe the "Right to privacy" or access someone data and share with third party, this may cause cybercrime or fraud like identity fraud, steal credit card or other financial record etc. The DPDP Act lacks effective protection for people's privacy and information rights, fundamental rights from the Constitution. It also fails to protect women's privacy due to inability to

[20] Carnegie India, "*Understanding India's New Data Protection Law*", available at: https://carnegieindia.org/2023/10/03/understanding-india-s-new-data-protection-law-pub-90624#:~:text=Introduction,(DPDP)%20Act%2C%202023.&text=The%20new%20law%20is%20the,half%20a%20decade%20of%20deliberations

[21] Robyn Annetts, & Matthew R. Cin., "*Unpacking India's Digital Personal Data Protection Act*", Ropes & Grey, (December 8, 2023), available at: https://www.lexology.com/library/detail.aspx?g=505cf55a-8bd8-4202-9938-bb999a746faa

[22] Digital Personal Data Protection Act 2023 (Act no. 22 of 2023), s. 3(b) states, "Subject to the provisions of this Act, it shall-also applies to processing of digital personal data outside the territory of India, if such processing is in connection with any activity related to offering of goods or services to Data Principals within the territory of India".

[23] Digital Personal Data Protection Act 2023 (Act no. 22 of 2023), s. 3(c)

safeguard personal data, potentially increasing cybercrimes like cyber pornography and deepfake videos. Therefore, strict regulation is needed to address these threats.

III. ISSUE AND CHALLENGES RELATED TO DATA PRIVACY IN DIGITALIZED INDIA

The Digital Personal Data Protection Act of 2023, was recently passed to allow for the processing of digital personal data in a manner that acknowledges both the need to process such data for legitimate purposes and for matters related or incidental thereto, as well as the right of individuals to protect their personal data[24]. In this Act, the personal data share by the consent of the person but while obtaining consent, a company does not have to disclose who all the data will be shared with and for what purposes[25]. Further, government has a broad power to exempt itself demand information from companies, and retain data for an unlimited period can result in mass surveillance[26]. In another words, the DPDP Act of 2023's section 2(t) specifies "personal data" as "any data about an individual who is identifiable by or in relation to such data," which the government can retain for an unrestricted period of time, regardless of whether the original purpose for which it was obtained has been fulfilled. A data protection law must safeguard and balance peoples' right to privacy and their right to information, which are fundamental rights flowing from the Constitution. Unfortunately, this Act fails on both counts[27].

Additionally, millions of Indian personal records were accessed and made available on the dark web in 2022 using the True Caller programme. An investigative study published in the Economic Times claims that vast amounts of personal data, including the phone numbers and email addresses of Truecaller subscribers, are for sale on dark web and private internet forums[28]. While the personal data of the 140 million users of the mobile app may be acquired for up to 25,000 Euros (about Rs. 19.45 lakh), the personal data of Indian users, who make up 60–70% of the user base, can be purchased for roughly 2,000 Euros (roughly Rs. 1.55 lakh).[29] So, the personal data is becoming the basic income source to earn their livelihood for those who illegally share data with third party other than authorized person. Moreover, many business cooperation's are alleged to have been conducted in India wherein a person data is exported by oversees companies[30].

As per the report on 31 October 2023, there is a massive data breach that involves over 80 crore Indian citizens was surfaced by an American cybersecurity agency called "Resecurity". It claimed that data of around 81.5 crore Indian citizens was being sold on the dark web by a person with an alias 'pwn0001'[31]. In other words, the crucial data information such as Aadhar and passport details along with names, phone numbers and address set on sale on the dark web. There are many instances where the personal data security is at stake in this

---

[24] *Supra note 12.*

[25] Sarvesh Mathi. (2023, August 4). *Fifteen major concerns with India's Data Protection Bill, 2023*. MediaNama. https://www.medianama.com/2023/08/223-major-concerns-india-data-protection-bill-2023/

[26] Digital Personal Data Protection Act 2023 (Act no. 22 of 2023)

[27] Bhardwaj, A. (2023, February 20). *The problems with the Data Protection Bill*. The Hindu. https://www.thehindu.com/opinion/op-ed/the-problems-with-the-data-protection-bill/article66531928.ece.

[28] Shweta Ganjoo. (2019, May 22). *Truecaller data breach: Personal data of millions of Indians available on dark web, company denies breach*. India Today; available at https://www.indiatoday.in/technology/news/story/personal-data-of-millions-of-truecaller-users-available-on-dark-web-1531969-2019-05-22

[29] Ibid

[30] Boruah, J., & Das, B. (2021, March 16). Right to privacy and data protection under Indian legal regime, *Ssrn.com*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3827766

[31] Sharma (2023, November 1), What we know and don't know about the alleges Aadhar data leak, *India Today*. Available at https://www.indiatoday.in/india/story/aadhaar-data-leak-what-we-know-and-dont-know-about-breach-2456474-zzzzzzzzzzzzzzzzzzzzzzzzz2023-11-01

digital world. Therefore, there is need to enact strict laws to govern such type of instances or crime by using digital platform or harm the privacy of the individual.

India has greatly benefited from the digital revolution, enhancing connectivity, accessibility, and convenience. However, it has also raised concerns about privacy rights protection. As we transition towards the technological era, new ethical and juridical difficulties arise, such as access to information, privacy, free information movement, and the safety of intellectual property owners' economic interests. The nation is experiencing unprecedented levels of creativity and innovation due to the widespread use of cell phones, internet connectivity, and digital services. However, concerns about individual privacy rights have become more prevalent. The growing use of facial recognition and mass surveillance technologies presents another threat to digital rights, violating both dignity and privacy. These systems often inaccurately identify people, leading to wrongful incarceration and arrests, violating human rights. The major challenge of technology in this era is the growing amount of personal data linked to technology, such as Aadhar and bank details, which can put individuals and businesses at serious risk.

The foremost concerns related to privacy in recent times are discussed below:

a. Data breach and Security risk

A data breach refers to unauthorized access, disclosure, or acquisition of sensitive information, leading to potential misuse or exploitation. Common types of data breaches include hacking, phishing attacks, insider threats, and physical theft of devices containing sensitive data. Data breaches can have severe consequences, including financial losses, reputational damage, legal repercussions, and loss of customer trust. The impact varies based on the type and scale of the breach, highlighting the need for robust cybersecurity measures.

According to Cambridge dictionary, "data breach" is defines as "an occasion where private information can be seen by people who should not be able to see it[32]". The protection of personal data and information's of an individual is crucial for safeguarding the right to privacy. The 'right to privacy' refers to the specific right of an individual to control the collection, use and disclosure of personal information[33]. Personal information could be in the form of personal interests, habits and activities, family records, educational records, communications (including mail and telephone) records, medical records and financial records, credit card details, to name a few[34].

Data breaches are a growing concern in India due to the rapid development of technology. In January 2024, cybersecurity firm CloudSEK revealed a massive security breach exposing personal information of 750 million people, including names, mobile numbers, addresses, and Aadhaar information[35]. The breach covered 85% of the Indian population and hackers demanded $3,000 for the entire dataset. During the Covid-19 period, the Indian government investigated potential data breaches in the Indian Council of Medical Research (ICMR) Covid-testing database. A threat actor accessed personal details of over 8 crore Indians who underwent Covid

[32]Cambridge Dictionary, "data breach. @Cambridge Words" (March 20, 2024), available at **https://dictionary.cambridge.org/dictionary/english/data-breach**

[33] Supra Note 63

[34] Ibid

[3535] Chakravarti, A., "*Data of 750 million telecom users in India being sold on dark web, cyber experts claim*", India Today; (January 31, 2024), available at https://www.indiatoday.in/technology/news/story/data-of-750-million-telecom-users-in-india-being-sold-on-dark-web-cyber-experts-claim-2495752-2024-01-31

tests, including names, addresses, and phone numbers[36]. The breach was first noticed by American cyber security firm on October 9, 2023. The head of the National Health Authority, RS Sharma, stated that India is putting people at risk from data collection and overreach due to the push for greater digitisation of health data without adequate protection[37]. Personal data leaks, such as the Aadhar database, are also responsible for security threats to individuals and companies, as they can lead to financial loss, reputation loss, and identity theft. In 2022, the southern state of Karnataka in India had the highest number of registered offences related to online identity theft, with over 3.7 thousand cases registered with authorities[38]. This category of crime came under the purview of Section 66C of the IT Act. Another example is a hacker attack on Air India's passenger service system provider, SITA, resulting in the theft of 4.5 million passengers' personal data in February 2021[39]. The hackers obtained sensitive information to access passengers' GST invoices and reveal it in the public domain, causing Air India to face reputational loss. Therefore, data protection remains a major challenge to protecting privacy in digitalization.

b. Cross border transaction and jurisdictional issue

The digital economy presents numerous economic opportunities, with cross-border data flows playing a crucial role in global trade. The global nature of the digital environment allows users to access websites and content from anywhere, subject to copyright restrictions. Global e-commerce allows buyers to purchase goods and services from sellers in other countries, involving billions of daily transactions[40]. As per the World Bank report, global internet traffic was about 3 zettabytes in 2020, equal to 1 GB per person per day, and is projected to double in the future[41]. Cross-border data flows are essential for international trade, enabling efficient transactions in goods and digital services. Electronic payment systems, internet-based advertising, and cloud computing are now essential in all sectors of business[42]. Data transfer is fundamental in international trade transactions, but this raises issues for governments regarding data privacy, consumer protection, public safety, and national security.

The Asia-Pacific Economic Cooperation (APEC) adopted the APEC Cross-Border Privacy Rules (CBPR) in 2011 to balance data flow across borders and protect personal information[43]. Under the CBPR, companies located in signatory countries can become an independent third party, called an Accountability Agent, that evaluates and certifies the companies' privacy policies and practices. Currently, nine countries are part of this cooperation, such as Australia, Canada, Japan, Korea, Mexico, Philippines, Singapore, Chinese Taipei, and

---

[36] Reuters. "*India's health data faces rising risk of breaches, cyberattacks*" The Economic Times (July 24, 2023), available at https://economictimes.indiatimes.com/news/india/india-health-data-faces-rising-risk-of-breaches-cyberattacks/articleshow/102065523.cms?from=mdr

[37] Ibid

[38] India: number of online identity theft offences registered by leading state 2022 | Statista. (2022). Statista; Statista, available at https://www.statista.com/statistics/1097526/india-number-of-online-identity-theft-offences-registered-by-leading-state/

[39] Editorial, "*Air India sued over data breach, flyer seeks Rs 30 lakh in damages*", The Economic Times, (July 7, 2021), available at https://economictimes.indiatimes.com/news/india/air-india-sued-over-data-breach-flyer-seeks-rs-30-lakh-in-damages/articleshow/84197878.cms?from=mdr

[40] Digital Regulation Platform. (2020). Digitalregulation.org, available at https://digitalregulation.org/cross-border-collaboration-in-the-digital-environment-2/

[41] Bhawna Sharma, Dhawal Gupta & Ajay Singh Chauhan, "Data Protection Standards for Cross Border Data Transfers in India: Suggestive Approaches and Way Forward" *Live Law*, (May 25, 2023).

[42] Ibid

[43] APEC, "What is the Cross-Border Privacy Rules System", (2024), available at: https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system#:~:text=Currently%2C%20nine%20economies%20participate%20in,visit%20www.cbprs.org

the United States. India has not joined APEC despite a 20-year pending membership request[44]. The European Union's General Data Protection Regulations (GDPR) is one of the most comprehensive frameworks for cross-border data transfers, applying to all businesses that process the personal data of EU citizens, regardless of where the business is located. The GDPR requires businesses to obtain explicit consent from individuals before collecting their personal data and to provide clear information about how that data will be used.

The DPDP Act permits cross-border data transfers, with government restrictions on certain countries. This blacklisting approach means that personal data is freely transferable unless the transfer is proposed to a country blacklisted by the Central Government[45]. However, the Act may prescribe additional compliance or limit data types, and any parallel law providing higher protection or restriction on data transfer outside India would prevail over the DPDP Act's provisions[46]. Privacy in the digital age is a complex and multifaceted issue, and taking proactive steps to address emerging technologies and their privacy implications is critical. Balancing innovation, security, and privacy in India is a major challenge.

IV. **Conclusion and Suggestion**

The right to privacy has become a fundamental right in India due to various court interpretations. However, globalization has led to significant technological advancements that have directly affected our privacy, such as cybercrimes, data theft, and misuse of data. In India, users currently disclose their personal data to third parties, including government agencies and private companies, which increases the risk of data theft or misuse. There are several laws, such as the IT Act, Criminal Law, and Intellectual Property Law, that deal with data protection, but these laws may be considered a "Breach of Privacy" if it is unlawfully disclosed or used by a third party. The strict data protection laws are required to safeguard private information. The Supreme Court confirmed privacy's legitimacy as an inherent Fundamental Right under Article 21 of the Constitution. However, just having this opinion is insufficient; everyone has rights and should be aware of their alternatives, including the ability to file a complaint with the Higher Authority if their rights are violated. Only when a person is well-known for their rights can they grow or lead a dignified life. Data privacy must now be taken into account, while personal privacy was once the sole factor to be considered. Legal officials should establish laws, rules, or regulations that guarantee the security of the data gathered. Only those with the necessary authority and for the benefit of the public welfare should be able to access the database where the information is kept. Strict security measures should be implemented to make it hard for even specialists to access data. Additionally, each regulation must include provisions about penalties, such as financial penalties and imprisonment, that are severe enough to make someone who is not authorized reconsider handling personal data.

---

[44] Ibid

[45] Digital Personal Data Protection Act, 2023-Key Highlights, (2023, September 11). Azb. available at https://www.azbpartners.com/bank/digital-personal-data-protection-act-2023-key-highlights/

[46] Digital Personal Data Protection Act 2023 (Act no. 22 of 2023), s. 16 (2) states "Nothing contained in this section shall restrict the applicability of any law for the time being in force in India that provides for a higher degree of protection for or restriction on transfer of personal data by a Data Fiduciary outside India in relation to any personal data or Data Fiduciary or class thereof

A few experts have proposed switching to smart cards, which would be an optional replacement for the collection of biometric data. Smart cards that require pins will require the conscious cooperation of citizens during the identification process and cannot be used to identify any specific person once they are disposed of. Implementing smart cards would eliminate or at least reduce the danger created by terrorists and criminals. Foreign governments may use the biometric database to identify Indians. As the world moves into the world of modernization and globalisation, there is bound to be a drastic change in the technology and lifestyle of the people in society. India, as a developing country, needs to strengthen its technology to move towards modernization and the digital era. The recent enactment of the DPDP Act marks a significant step towards safeguarding personal data in the digital realm. However, this legislative framework has certain untouched issues, like jurisdictional issues, that undermine the protection of data, ultimately leading to privacy breaches and harm to the dignity of women in the digital age. The collaborative efforts between government bodies, civil society organizations, and technology companies are essential to create a more secure and respectful digital environment for all individuals, upholding the fundamental right to privacy and preserving the dignity of women in India's digital age.

REFERENCES

- Privacy and Human Rights - Overview. 2024. Gilc.org. 2024, available at https://gilc.org/privacy/survey/intro.html
- Robyn Annetts, & Matthew R. Cin., "*Unpacking India's Digital Personal Data Protection Act*", Ropes & Grey, (December 8, 2023), available at: https://www.lexology.com/library/detail.aspx?g=505cf55a-8bd8-4202-9938-bb999a746faa
- Rai, N. (n.d.). Right to Privacy and Data Protection in the Digital Age - Preservation, Control and Implementation of Laws in India. *IJLJ*, *11*(1). Retrieved February 5, 2024, from https://ir.nbu.ac.in/bitstream/123456789/4009/1/IJLJ%20-%20Vol.%2011%20No.%201%20%28Part%20III%29%20Article%20No%209.pdf *(Privacy and Data Protection in India: An Analysis - International Journal of Law Management & Humanities, 2021).*
- Boruah, J., & Das, B. (2021, March 16). *RIGHT TO PRIVACY AND DATA PROTECTION UNDER INDIAN LEGAL REGIME*. Ssrn.com. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3827766
- Manzar, Osama, and Udita Chaturvedi. n.d. "UNDERSTANDING the LACK of PRIVACY in the INDIAN CULTURAL CONTEXT Opinion Piece." available at https://defindia.org/wp-content/uploads/2017/09/Understanding-the-Lack-of-Privacy-in-Indian-Cultural-Context.pdf.
- Yashraj Bais, Privacy and Data Protection in India: An Analysis, 4 (5) *International Journal of Law Management & Humanities*, 1793 - 1804 (2021)
- Bhawna Sharma, Dhawal Gupta & Ajay Singh Chauhan, "Data Protection Standards for Cross Border Data Transfers in India: Suggestive Approaches and Way Forward" *Live Law*, (May 25, 2023).