IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

AN ANALYSIS ON NEED OF DATA PROTECTION IN INDIA AN OVERVIEW

AUTHOR 1 - Gowri Chauhan, AUTHOR 2 – Mr. Ayush Saran

Designation of 1st Author- Student, Designation of 2nd Author- Assistant Professor

Name of Department of 1st Author- Amity Law School

Name of organization of 1st Author- Amity University, Lucknow Campus, Lucknow, India

Abstract

The world is witnessing rapid growth in technology, with the internet becoming more ubiquitous and geographical boundaries blurring the flow of information. Data has become an integral part of our daily lives and almost every aspect of the modern world is connected in some way. data Whether it's social media, banking or commerce, our daily lives are inextricably linked to data. This increased connection brings many new and difficult challenges in terms of privacy and data protection, as it is important to give individuals control over their personal data. India, one of the fastest growing economies, is at the forefront of this digital transformation and various sectors are going digital and the Digital India initiative is being launched. In response to growing concerns about personal data protection and rights, the Indian government has introduced several bills. The preamble of the Bill aims to provide a legal framework for the protection of personal data and the rights of individuals in India's rapidly evolving digital environment. The aim of this study is to analyze the effectiveness of Indian laws and the challenges of data protection laws.

Introduction

India is experiencing a digital revolution where people are increasingly using technology and online in their daily lives. There has been an increased need for cyber security and data protection measures to protect individuals and businesses from cyber attacks and data breaches. India is the second largest internet market in the world with a population of 1.3 billion and is expected to grow rapidly. Privacy and data security concerns arising from this expansion have led to calls for stronger data protection laws and regulations. There's no denying that the world we live in has changed, and it's changing fast. In recent years, globalization and international trade have increased the growth of the service sector, and modern industrial

society has relied on the storage of data and information. Data is not just energy or a source of information, it has become big business in healthcare, services and education, with both the public and private sectors collecting data using advanced data storage technologies. The problem of personal privacy has arisen due to the infinite nature of the Internet.The privacy rights we once took for granted have been completely destroyed by the new digital environment. The development of the Internet has made it possible for ordinary people to conduct all their daily activities online, but it has left questions of privacy and data protection unanswered and prone to security breaches. The data and information that individuals and organizations are concerned about before sharing their information with third parties. With concerns about digital privacy issues in various sectors around the world, government agencies are rushing to pass new laws that increase the rules for collecting, storing and processing customer-related data. All players in this space can greatly benefit from investing more resources in cyber security programs that not only prevent known attacks but also detect/prevent new attacks. It is important to strike the right balance between privacy and innovation when developing and implementing data protection laws and regulations.

Scope and Limitations

Scope:

1-This research focuses on privacy and the data protection laws in India and their effectiveness to secure the rights of privacy of individuals.
2-The research try to figure out the Indian data protection and its various legislative frameworks to identify the strengths and effects of statutes in data protection principles, enforcement mechanisms, rights for data subjects, accountability measures for data processors, cross-border data transfer provisions, and remedies for individuals in case of a data protection breach to a better understanding.

Limitations:

1-This research is limited to the provisions and a critical analysis right to privacy and data protection law in India.
2-The research is subject to the availability of relevant data and information, and any limitations in accessing such data and information could impact the findings of the research which will be based on secondary sources.
1-The study is limited to only legal provisions related to data protection laws and may not consider other factors that could impact data privacy, such as social norms, cultural values, or economic policies
2-The study is limited to the scope of the comparative analysis with the EU, and US.

Research Objectives:

The followings are the objectives of the Research-

1-Understand the legal framework for data protection and privacy in India.
2-To grab a thorough, understanding of the right to privacy, data regulation, and its relevancy in the digital era.
3-The Third objective is to provide insight into the successful enforcement of data protection law by the EU and the US and to provide suggestions to India for the better Implementation of the data protection law.

Hypothesis:

1. Despite the efforts of comprehensive data protection legislation in the form of various Data Protection Bills India still lacks adequate set laws and regulations for data protection.
2. Indian laws are not comprehensive and sufficient in terms of protection and enforcement as compared to the EU and USA Research Question
3. Whether India has any enforcement regulation in case of an invasion of the right to privacy?
4. Is India's current legal framework effective in addressing the legal problem of data breaches by international actors?

Situation in India

Data security breaches are an ongoing problem in India. The largest data breach, according to the WEF World Economic Forum's Global Risk Report 2019, occurred in India called the "Aadhaar leak case" In order to meet the rising demand for digital services and to secure data protection, the country's cyber security workforce will require an extra 1 million qualified personnel by 2025, according to a report by the Internet and Mobile Association of India (IAMAI) (IAMAI, 2020). The rise in cyber attacks and data breaches nationwide also emphasizes the importance of data protection. Over 4 lakh cyber events were reported in India in 2019, a 37% increase from the previous year (CERT-In, 2019). The world's greatest data breach, known as the Aadhaar leak case, happened in India that same year and exposed the personal information of over 1.1 billion Indian people as a result of a security hole in the country's biometric identity system, the Aadhaar system (Jain, 2018).Data protection laws in India are now governed by the out-of-date Information Technology (IT) Act 2000, which is insufficient to deal with the complexity of the modern digital environment.The Personal Data Protection Bill 2019 is a data protection law that the Indian government has been developing in order to give Indian residents complete data protection has failed to convert into an act and the new proposed Digital Personal Data Protection Bill, 2022 is still pending. The government has also started a number of initiatives and programs to support data security and privacy in India. The Digital India initiative was launched in 2017 by the Ministry of Electronics and Information Technology (MeitY) with the aim of transforming India into an economic and knowledge-based society. The project focuses on various data protection and security-related measures, including creating a secure

digital infrastructure, increasing public awareness of cyber security, and encouraging internet research and development. In addition, the Indian government has established various agencies to oversee data protection. Most prominent is the Data Security Council of India (DSCI), a self-regulatory organization that works to create and promote best practices in data privacy and security. DSCI works with governments and other stakeholders to develop data protection policies and laws, and provides data protection advice and certification worldwide, including in countries such as the EU. The United States is reforming its laws to meet the challenges presented by new technologies. However, India lags behind in establishing comprehensive data protection laws to protect privacy and individual rights in the digital age. India has made several attempts to create separate data protection laws, but these initiatives have not been incorporated into law or failed to protect personal information. India's proposed new legislative framework, the Personal Digital Data Protection Bill, 2022, brings significant changes compared to the past. However, there is a problem with the law that data protection is limited to certain formats, making it difficult to implement.

[1]Privacy and Data Protection in India: An Analysis

The article discussed the nature of threats by public officials on behalf of "statutory bodies" or "public officials". Privacy is essential to a peaceful life and to dignity and freedom, essential to human rights. With the rise of digitization and increased use of social media and the Internet, data protection and privacy has become a national issue. Data protection and privacy are inextricably linked and of utmost importance to the legal profession..

[2]Privacy and Data Protection in India: A Critical Assessment

This article discusses the conflict between privacy rights and data protection in India and argues that the current Information Technology (Amendment) Act, 2008 is inadequate for data protection. The authors intend to start a discussion on this topic by stating the need for a specific law on data protection and privacy. It will be used for research to look at the Information and Communications Technology Amendment Act 2008.

---

[1]Yashraj Bais, Privacy and Data Protection in India: An Analysis, International Journal of law and Management and Humanities, Volume 4 issue 5, 2021

[2] Shiv Shankar Singh, Privacy and Data Protection in India: A Critical Assessment, JSTOR, Volume 53 no. 4, 2011

India's Digital Personal Data Protection Act, 2022: How practical is consent?.

This study describes the concept of consent in relation to digital personal data protection laws, highlights key issues related to consent in law and demonstrates the potential for understanding the concept of consent in different national laws for research purposes.

THE ORIGINS AND DEVELOPMENT OF PRIVACY AND DATA PROTECTION

The Constitution of India is the supreme law of the land and has supreme authority. What cannot be denied is that our Constitution is a dynamic and adaptive document that can be shaped in response to changing social and environmental conditions. Among many fundamental rights, the right to privacy is a fundamental right that falls within the ambit of protection under Article 21. Article 21 states that "no one shall be deprived of his life or liberty.".It is universally acknowledged hat the right to privacy is intricately linked with an individual's life and liberty, making it an inherent part of the fundamental rights guaranteed by Article 21.[3]

The discourse on the existence of a fundamental right to privacy in the Indian context can be traced back to a series of judgments by the Supreme Court of India, starting from **M.P. Sharma vs Satish Chandra [4]to K.S. Puttaswamy v. Union of India**.[5]

In the series of Landmark cases on the right to Privacy in India **M.P. Sharma vs Satish Chandra**, is remarked as the first case in which the right to privacy has been discussed the issue of whether privacy is a fundamental right was first raised before the esteemed Supreme Court of India. The case involved a search and seizure carried out by the authorities in pursuit of disputed documents of the Dalmia Group of Delhi, based on a First Information Report (FIR) and warrants issued under the statutory provisions of the Code of Criminal Procedure, 1973. The Group challenged the validity of the search and seizure through a writ petition, contending that it was arbitrary and violated their Right to Privacy and Fundamental Rights as guaranteed under Article 19(1)(f) [6]and Article 20(3)[7] of the Constitution, pertaining to protection against

---

[3] Nivedita Baraily, An Analysis of Data Protection and Privacy Law in India

[4] (1954) S.C.R. 1077

[5] Justice K. S. Puttaswamy (Retired.) and another. v Union of India and others, (2017) 1 SCC 10

[6] Article 19, of the Constitution of India

"Right to freedom"

self-incrimination. The matter was referred to an Eight-Judge Constitutional Bench of the Supreme Court, which thoroughly examined and deliberated on the issue. In the end, the Supreme Court ruled that the Constitution does not regard searches and seizures carried out in accordance with established legal procedure, such as a FIR and subsequent decisions of the District Magistrate, as a violation of personal privacy or fundamental rights. According to the court, the Indian constitution does not recognize the right to privacy as a fundamental right in India because the language of the Indian constitution is inconsistent with the Fourth Amendment of the US Constitution. The court found that the current case's search and seizure weren't illegal or unconstitutional.

In **Kharak Singh v. State of U.P,** The petition before the Supreme Court challenges the constitutionality of Chapter 22 (Regulations 236 and 237) of the Uttar Pradesh Police Regulations and the powers conferred on police officials by its various provisions, claiming that they violate citizens' rights guaranteed by Articles 19(1)(d) and 21 of the Constitution. The Court referred the **J Frankfurter's remark in Wolf v. Colorado**.[8] The knock on the door, whether day or night, as a prelude to a search, without legal authority but solely on the authority of the police, did not require the approach to recent history must be condemned as inconsistent with the concept of human rights embodied in the history and constitutional documents of English-speaking nations. We have no trouble in stating that if a state knowingly sanctioned such police intrusion into privacy, it would violate the Fourteenth Amendment guarantee." The Court took notice. "It is clear that the knock at the door, or the man being roused from his sleep, does not impede or prejudice his locomotion in any way," and so does not violate Article 19 (1)(d).37 Clause (b) of Regulation 236, in our opinion, is clearly in violation of Article 21, and because there is no "Law" to justify it, it must be declared unconstitutional. However, the majority of judges participating in the decision noted that the right to privacy is not a right guaranteed by the constitution.

In his opinion, **Justice Subha Rao** favored inferring the right to privacy from the phrase "personal liberty" in Art. 21. In addition, ‘the right to personal freedom means not only the right to be free from restrictions on one's movement, but also the right to be free from violations of one's privacy’, writes SUBBA RAO, J. Although our constitution does not directly declare the right to privacy as a Fundamental Right, it is a fundamental component of personal liberty. Every democratic country values family life

---

[7] Article 20 of the Indian Constitution.

[8] Power for Government to take possession of licensed telegraphs and to order interception of messages

In the series of landmark cases **R. Rajagopal v. State of Tamil Nadu**[9], also known as the "Auto Shanker Case," the Supreme Court of India has unequivocally established that the right to privacy, or the right to be left alone, is protected under Article 21 of the Constitution. This fundamental right extends to safeguarding an individual's privacy in various aspects, such as their personal life, family, education, marriage, procreation, and motherhood. Furthermore, in the case of State of **Maharashtra v. Madhulkar Narain[10],** it has been conclusively held that the right to privacy is applicable to all individuals, including those who may be considered of "easy virtue," and that no one can infringe upon their privacy.

Gobind v. State of M.P. [11]recognized the right to privacy as implicit in the concept of individual autonomy and liberty, but not an absolute right and subject to restrictions based on compelling public interest. The Court noted that the contours of the right to privacy would have to develop through a case-by-case process. The Court also acknowledged that the right to privacy contained multiple aspects, such as spatial privacy, informational privacy, decisional autonomy, and full development of personality.

Subsequently, many judgments of the Apex Court have relied on Gobind case and recognized the right to privacy as a fundamental right under the Indian Constitution.

Finally, in the case of **K.S. Puttaswamy v. Union of India**[12], (ADDHAR CASE) a nine-judge constitutional bench of the Supreme Court of India in 2017 invoked the concept of "Liberty" as enshrined in the Preamble and Article 21 of the Constitution to establish that the Right to Privacy is a fundamental right. This right encompasses the protection of data, including unauthorized access or use of an individual's data without their explicit consent, which constitutes a grave violation of the Right to Privacy. Individuals have the option to approach the Supreme Court of India directly under Article 32 [13]or the High Court of their

---

[9] (1994) 6 SCC 632

[10] (1991) AIR 207

[11] 1975) 2 SCC 148

[12] Supra 25

[13] **Article 32**. Of the Constitution of India

respective state under Article 226 [14]to seek redressal for such infringements. overruled the M.P Sharma and Kharak Singh case and declared the Right to privacy as the fundamental right under Article 21 of the Constitution of India.

Need for Data Protection India

India, the second largest country in the world, has undergone a technological revolution with the widespread adoption of online services such as social media and e-commerce platforms. The move to digitization has had significant economic benefits, including improved efficiency and productivity. But people and organizations have become more vulnerable to new threats from cybercriminals. New challenges present security and privacy risks. Recent findings (KPMG 2020) show that data breaches are on the rise in banking, healthcare, public and private organizations in India. whereas, the introduction of Digital India and the India Stack, the percentage of smart phones in rural India increased from 9 to 25 percent by 2018, the number of Indians using social media increased from 142 to 326 million by the same year, and the average monthly data usage increased by 129 percent between 2015 and 2018 (assumed a compound annual growth rate). [15]Sensitive data, such as bank records or personal identity information, may be lost as a result of these breaches. Due to the fact that these occurrences are being discovered more frequently than ever, Identity theft and other forms of fraud have disturbed many people's personal lives in the past few years alone, causing significant harm to both parties. Additionally, company losses are significant, running to crores per year. Additionally, journal articles on the subject emphasize how cyber threats pose genuine risks to all Indians, including both small businesses and individual citizens.

It is important to take the necessary steps to protect your information systems from unauthorized access if you want to protect your sensitive data from malicious actors who seek to exploit your network vulnerabilities using malware, such as ransomware, for public sector organizations. Awareness programs aimed at improving IT hygiene practices among employees should be developed, and private organizations should invest heavily in protecting their own infrastructure from cyber security incidents. Professionally the l opinion indicates that data Protective measures are very much needed in India if we want to protect ourselves as individuals and society. This is because technology is constantly evolving and security threats are becoming more powerful.

---

[14] **Article 226**. (1) Subs. by the Constitution (Forty-second Amendment) Act

[15] *Kantar. "Internet Adoption in India: ICUBE 2020." June 2021. Accessed [insert date of access]. Available at: https://images.assettype.com/afaqs/2021-06/b9a3220f-ae2f-43db-a0b4-36a372b243c4/KANTAR_ICUBE_2020_Report_C1.pdf*

Sensitive personal data or Information Rule 2011

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) were promulgated on April 13, 2011, under Section 87(2)[16] in conjunction with Section 43-A of the IT Act. These regulations pertain to the handling of sensitive personal data or information and are applicable to both body corporates and individuals situated in India. The rules govern the collection, receipt, possession, storage, processing, handling, storage, use, transfer and disclosure of SPDI and the security practices and procedures for its handling. Data subjects have the right to review and update their SPDI and withdraw consent for its processing.

Intermediary Guidelines, 2011

The Indian government established the Information Technology (Intermediaries Guidelines) Rules, 2011[17], as a framework for regulating online intermediaries. The rules attempt to strike a balance between the need for freedom of speech and expression and the need to protect against harmful and illegal online content. The guideline made the Intermediaries must exercise due diligence when performing their duties, as stated in Rule 3[18] of the guidelines. According to the guidelines, According to the guidelines, moderators must

---

[16] Power of Central Government to make rules.

[17] Ministry of Electronics and Information Technology, Information Technology (Intermediary Guidelines) Rules, 2011, Gazette of India (Apr. 11, 2011)

[18] (1) Due diligence by an intermediary: An intermediary, including social media intermediary and

significant social media intermediary, shall observe the following due diligence while discharging itsduties, namely:—

(a) the intermediary shall prominently publish on its website, mobile based application or both,

as the case may be, the rules and regulations, privacy policy and user agreement for access

or usage of its computer resource by any person;

(b) the rules and regulations, privacy policy or user agreement of the intermediary shall inform

the user of its computer resource not to host, display, upload, modify, publish, transmit,

store, update or share any information that,—

(i) belongs to another person and to which the user does not have any right;

(ii) is defamatory, obscene, pornographic, paedophilic, invasive of another's privacy, including bodily privacy, insulting or harassing on the basis of gender, libellous, racially or ethnically offensive, about or encouraging money laundering or gambling, or otherwise goes against the law;

remove or disable access to content deemed offensive, offensive or defamatory within 36 hours of receiving a complaint or notification from a user. This provision helps limit the online

distribution of illegal material. The guidelines have also played a significant role The guidelines have played an important role in influencing the data protection environment in India. These guidelines have helped create a culture of responsibility and accountability among online mediators by forcing mediators to follow certain standards.

Intermediary Guidelines and Digital Media Ethics, 2021

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 were published on 25 February 2021 by the Ministry of Electronics and Information Technology of the Government of India. In accordance with the Information Technology Act of 2000, these rules (henceforth "New IT rules") have replaced the Information Technology (Intermediaries Guidelines) Rules of 2011. These standards apply to creators and publishers of digital media content, as well as intermediaries. Under this law, each intermediary must designate an Agency, and its name and contact information must be clearly displayed on the intermediary's website, application, or both (if applicable).

EFFORTS TAKEN TOWARD SEPARATE LEGISLATION

India has made several efforts to enact robust data protection legislation through various Data Protection Bills. The first such bill was the Personal Data Protection Bill, of 2006, which was introduced by Vijay J

(iii) is harmful to child;

(iv) infringes any patent, trademark, copyright or other proprietary rights;

(v) violates any law for the time being in force;

(vi) deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates any information which is patently false or misleading in nature but may reasonably be perceived as a fact;

(vii) impersonates another person;

(viii) threatens the unity, integrity, defence, security or sovereignty of India, friendly

relations with foreign States, or public order, or causes incitement to the commission of any cognisable offense or prevents investigation of any offence or is insulting other nation;

(ix) contains software virus or any other computer code, file or program designed to interrupt, destroy or limit the functionality of any computer resource;

(x) is patently false and untrue, and is written or published in any form, with the intent tomislead or harass a person, entity or agency for financial gain or to cause any injuryto any person;

Darda [19]in the Rajya Sabha. The draft consisted of a total of 14 points and aimed to replace and compensate individuals whose personal data was used by organizations for direct marketing or other financial gain without their consent. The bill was to apply to both private and public data collection organizations.

Key Features of the 2006 Bill:

- The bill mandated the obtaining of consent from individuals before processing their personal data[20]
- The bill prohibited the public and government organizations from disclosing personal data to other organizations for direct marketing or economic gain.[21]
- The bill established provisions for individuals to seek compensation from public and government agencies in cases of unauthorized alteration, disclosure, or transmission of their data.[22]
- The bill empowered the government to appoint a Data Collector for adjudicating complaints related to data disclosure, with a maximum term of three years.[23]
- The Bill encompassed provisions for both civil and criminal penalties in the event of contravention, attempted contravention, or abetment of contravention. And the punishment was three years imprisonment, along with a fine of up to ten lakh rupee[24]

Key Features of the Personal Data Protection Bill, 2018

---

[19] Vijay Jawaharlal Darda, Member of the Parliament of India

[20] Clause 3 of The Personal Data Protection Bill, 2006

[21] Clause 4 of The Personal Data Protection Bill, 2006

[22] Clause 5 of The Personal Data Protection Bill, 2006

[23] Clause 6 of The Personal Data Protection Bill, 2006

[24] Clause 10 of The Personal Data Protection Bill, 2006

The Bill Application covered Indian companies, Indian citizens, or bodies of persons incorporated, and the Companies not present within Indian territory but processing personal data, under its ambit[25].

•The Bill provided important definitions such as consent, Data, Data fiduciary, Data principal, Data processor, Personal Data, Sensitive Personal Data, Transgender status[26]

- The Bill specified the obligations of data protection with special mention of collection limitation, lawful processing, data storage limitations, and accountability for the data Fiduciary[27]

- The bill separately provided the grounds for the Processing of Personal data and sensitive personal data and mentioned the sensitive personal data of children[28]

- The bill recognizes the right to correction, right to access, and right to be forgotten of the data principle[29]

- The Bill provided the exemption in certain cases for data processing.[30]

- The Bill provided the formation of a Data Protection Authority for the supervision and monitoring of data fiduciaries and to impose penalties and award compensations.

- The Bill regulated cross-border data storage and also provided Penalties for various contraventions of the law.

---

[25] Section 2 of Personal Data Protection Bill, 2018

[26] Section 12 of Personal Data Protection Bill, 2018

[27] Section 3- Processing of personal data 2018

[28] Section4- Section 112 of Personal Data Protection Bill, 20188

[29] Chapter VI of Personal Data Protection Bill, 2018

[30] Chapter X of Personal Data Protection Bill, 2018

The bill failed to convert into the act, so the parliament directed the committee to revise the provision of the bill and draft new data protection law, in 2019, the committee came up with a revised data protection bill named, the personal data protection bill, 2019[31]

Key Feature of the Data Protection Bill, 2019

1. **Applicability**: The Bill deals with the processing of personal data by an entity operating in India or by another entity handling personal data in connection with a business carried on in India, for the purpose of collecting, using, distributing or displaying personal data in India..
2. **Definition of Personal Data and sensitive personal data-** Personal data is a name, identification number, location data, internet identifier or any other material related to the physical, physical, genetic, mental, economic, cultural or social nature of an individual or more natural persons.

3. **Grounds for Processing Personal Data**: The draft law establishes several grounds for the processing of personal data, including obtaining the consent of the individual, when the processing is necessary for the performance of a contract or to comply with a legal obligation.

4. **Rights of Data Subjects**: The bill provides individuals with several rights with respect to their personal data, including the right to obtain confirmation of The Bill gives individuals a number of rights over their personal data, including the right to confirm whether their personal data is being processed, the right to access their personal data and the right to correct inaccurate personal data. Right to be forgotten, right to data portability, right to oppose the processing of personal data.

5. **Data Protection Authority:** The bill establishes a data protection authority responsible for enforcing the provisions of the bill, conducting investigations and imposing penalties for non-compliance..

6. **Cross-Border Transfer of Personal Data:**The draft law provides for the cross-border transfer of personal data, subject to certain conditions and safeguards, including obtaining the consent of the individual and the consent of the data protection authority.

7. **Penalties:** The bill imposes significant penalties for non-compliance with the provisions of the bill,

Digital Personal Data Protection Bill 2022

In the Fifth instance of data protection Law, MEITY released the draft of an amended bill known as the Digital Personal Data Protection Bill, 2022, the bill consisted of a total of 6 chapters and 30 sections which

[31] Upasana Sharma & Aniket Singhania, The Personal Data Protection Bill, 2019: An Overview, Mondaq (Jan. 13, 2020),

is less in number in comparison with the personal data protection bill 2021. The Bill is still pending as a draft and has not been presented before the parliament.

Key Features of the Bill

1. **Territorial application**- The Bill deals with the processing of digital personal data, including data collected online, within the geographical boundaries of India. The scope extends to the processing of personal data outside India if the processing is for the purpose of providing goods or services to natural persons in India. The term "personal data" is defined as information relating to an identifiable individual, while "processing" refers to the collection, storage, use and sharing.

2. **Consent-** Under the bill, personal information can only be used as a legal basis if you have your consent. Before requesting permission, you must provide us with a notice that contains information about the personal data you want to collect and what that data will be used for. It is important to note that consent can be withdrawn at any time. However, consent is not always required. This may include processing to comply with a legal obligation, to provide you with a government service or benefit, to manage a medical emergency, to apply for employment, to carry out other activities in the public interest, such as protecting national security, preventing fraud. , or data. holding Information security. If you are under 18, you must obtain permission from your legal guardian.

3. **Rights And Duties of Data Principal-** The person whose data is being processed, called the "data principal," has certain rights when it comes to data processing. These include the right to know how their data is being used, the right to ask for corrections or deletions of their personal data, the right to choose someone else to use their rights if they die or become unable to, and the right to seek redress for a problem. But data leaders also have responsibilities that they have to keep up with. These include not filing false or pointless complaints, giving fake information, hiding information, or pretending to be someone else in certain situations. If these responsibilities aren't met, you could be fined up to Rs 10,000

4. **Obligation of Data Fiduciaries**- According to data protection laws, the controller, who is responsible for determining the purposes and methods of data processing, must be able to carry out certain procedures. These steps include making reasonable efforts to ensure the accuracy and integrity of data, implementing appropriate safeguards to prevent data breaches and notifying the Data Protection Commission of India if necessary. In addition, data controllers must stop retaining personal data when the purpose is fulfilled and storage is no longer necessary for legal or commercial purposes, subject to storage limitation requirements. It is important to note that this provision does not apply to government agencies involved in data processing.

5. **Transfer of personal data outside India**: -The Government of India will issue a notification to the countries where personal data will be transferred by the data controller. These transactions are subject to certain terms and conditions..

6. **Exemptions** – The bill provides for exemptions that do not apply to the rights of data subjects or the responsibilities of data banking, but to data security. This exemption also applies in cases of prevention and criminal investigation, including the enforcement of legal rights or claims. The Government also has the power to exempt certain acts from the provisions of the Bill by notification. These activities may include processing by government authorities for national security and public welfare purposes, including for research, reporting or statistical purposes.

7. **Data Protection Board of India** – The Indian government has announced its intention to establish a Data Protection Board of India, which will be responsible for monitoring data protection laws and imposing penalties for violations. The board also has the power to instruct data controllers on what to do in the event of a data breach and hear complaints from those affected. The government decides who the board members are, how they are elected, what their position and title are, and how they are fired.

8. **Penalties**- The Bill's timetable outlines the consequences for a range of offenses, including a maximum penalty of Rs 150 crore for non-compliance with child-related obligations and a maximum penalty of Rs 250 crore for failing to implement security measures to prevent data breaches and can exceed upto 500 crores. The Board will conduct an investigation before imposing penalties. This information is presented in a formal academic tone.

A critical analysis of the Digital Personal Data Protection Act 2022

The Digital Personal Data Protection Bill, 2022 is a comprehensive data protection framework that governs personal data in India and is the fifth data protection law where earlier laws have not become law. DPDPB, 2022 has the power to establish rules and regulations for national and international institutions related to the collection of data and is based on seven principles: The objectives of the Digital Personal Data Protection Act 2022 are considered to protect the personal data of individuals by establishing: Sample their rights, responsibilities and leaders who will follow them..

Scope and Applicability:The Digital Data Protection Bill 2022 mandates that all entities processing personal data relating to Indian citizens, irrespective of their location, must comply with its provisions. The bill's definition of "personal data" includes data that can be used to identify an individual, such as name, address, telephone number, email, biometric data, financial information and other sensitive personal information. This law is designed to regulate the processing of personal data by organizations and to ensure that the necessary steps are taken to protect the privacy of individuals. Expanding the scope of the Bill to include organizations outside India that process personal data relating to Indian persons is an important step towards strengthening the protection of Indian persons..

Right to be Forgotten- A major focus is the Digital Data Protection Bill 2022. The bill includes provisions requiring companies to delete personal data that is no longer relevant to the purposes for which it was collected. The introduction of the right to be forgotten in the Digital Data Protection Act 2022 is an important step towards protecting people's privacy in the digital world. The right to erasure is an important aspect of data protection and privacy because it gives people control over their personal data. This right is considered fundamental because natural persons can request the deletion of their data from various sources. By exercising this right, individuals can protect their personal information and prevent misuse..

The establishment of a Data Protection Authority/ Board This is an important step to ensure the protection of your personal data. This body is responsible for overseeing the application and compliance with data protection laws and regulations. The creation of these rights is necessary to respect the person's right to privacy and not to misuse their personal data. Data protection authorities/commissioners play an important role in protecting sensitive information such as medical records, financial data and other personal information. This initiative is an important step to create a safe digital environment for people and businesses.

CONCLUSION

With the rapid advancement of technology, data protection has become an important part of privacy in India. As more people use the Internet and digital devices, more and more personal or sensitive data is available. Data protection is a very important issue in India today. Throughout the analysis it was found that loneliness is important for human well-being and it is very important. This allows people to control their lives and prevent others from interfering with them. This means that they can express their opinion without being prosecuted or punished.According to Article 21 of the Constitution of India, the right to privacy is a fundamental right that ensures that no one is deprived of his liberty and life. India is a digital society and a knowledge economy. The Aadhaar card scheme has been instrumental in improving identity verification in India. Each citizen is assigned a unique identification number linked to their biographical information. The project includes the MyGov platform, which allows citizens to access government services and provides a secure and confidential communication channel. The Supreme Court of India acknowledged the right to privacy as a fundamental right under the Constitution in Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others. The court noted that the right to privacy encompasses the right to manage one's own personal information. India has acknowledged the significance of data protection and put in place various laws and regulations to ensure the safety of individuals' personal data.

The Personal Data Protection Act 2018 and its updated version, the Personal Data Protection Act 2019, set out a data governance framework to protect people's privacy. It defines important terms such as consent, data privacy, subject, data processing, personal data, sensitive personal data and genetic control and introduces rules for consent, data privacy relationships and implementation. The bill outlines the requirements for data protection, including limits on data collection, lawful processing, storage restrictions

and responsibility for data integrity. A special legal framework is established for the processing of sensitive data and personal data, including children, and to understand the rights of data subjects to access, correct, delete, etc. Some cases of data processing are not billable. A data protection authority will be established to monitor the activities of data controllers, regulate cross-border data transfers and impose fines and penalties. However, both bills failed to become law.

SUGGESTIONS

The proposals were made after reviewing the Personal Data Protection Act 2018 and 2019 and the Digital Data Protection Act 2022.Overall, the Digital Data Protection Act 2022 represents a major step forward in the collection and management of data in collection Processing of personal data in the digital world. In this way, it is intended to give individuals more control over their personal data and to make companies responsible for the management and use of data. With respect to the current bill, the number of topics subject to fines has increased, as has the scope of media rights. Enforcement will require some tweaking, but the ultimate goal is to create a safer digital environment for everyone.Protecting sensitive personal data is important in today's world. This type of data includes information such as DNA samples, medical records and credit card information. However, the current DPDP bill does not recognize the importance of sensitive personal data.

References

1. Yashraj Bais, Privacy and Data Protection in India: An Analysis, International Journal of law and Management and Humanities, Volume 4 issue 5, 2021
2. Shiv Shankar Singh, Privacy and Data Protection in India: A Critical Assessment, JSTOR, Volume 53 no. 4, 2011
3. M. R Konvitz, Privacy and the Law: a Philosophical Prelude. Law and Contemporary Problems Vol 31, No. 2. (1966) p. 272
4. World Bank and CGAP. Data Protection and Privacy for Alternative Data. GPFI-FCPL Sub-Group Discussion Paper - Draft - May 4 2018.
5. Nikhil Pahwa, The Problem with India’s Proposed Intermediary Liability Rules, Quartz India (Dec. 28, 2018),
6. Upasana Sharma & Aniket Singhania, The Personal Data Protection Bill, 2019: An Overview, Mondaq (Jan. 13, 2020),
7. National Institution for Transforming India. (2020). Data Empowerment and Protection Architecture (DEPA): A Policy Framework for Empowering Residents with Control over their Personal Data. New Delhi: NITI Aayog.

8. Vijay Pal Dalmia and Rajat Jain, Compliances by an Intermediary Under Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 - social media - India, Mondaq (May 9, 2022),

9. Shanaz, Asifullah Samim and Mohammad Edris Abdurahim Zai, Navigating Data Protection in India: Key Laws and Regulations for Protecting Personal Information, Trinity Law Review, Volume-3, Issue-2, 2023

Bibliography

- 1. The Constitution of India
- 2. Information Technology Act 2000
- 3. Personal Data Protection Bill 2006
- 4. Personal Data Protection Bill 2018
- 5. Personal Data Protection Bill 2019
- 6. Personal Data Protection Bill 2021
- 7. Digital Personal Data Protection Bill 2022
- 8. SPDI Rules 2011
- 9. Intermediary Guidelines 2011
- 10. Intermediary Guidelines and Digital Ethics Rule 2021