THE RIGHT TO CONFIDENTIALITY AND DATA PROTECTION IN THE DIGITAL AGE: CONSERVING, CONTROLLING, AND ENFORCING LAWS IN INDIA

Drishya Asrani*

ABSTRACT

The progress of technology and the dynamism of the legal environment provide insight into contemporary privacy and data protection challenges. Privacy should not conflict with the interests of others. As a consequence of technological advancement, privacy has become a universal issue, with a particular emphasis on data protection. Individual liberty is stressed in data protection, and it is jeopardized by the stranger's interference. The stranger's actions in any way connected to the individual's activities must end. The constitution may validate the basic legal requirement of each new occurrence. India's constitution prioritizes rights above obligations. It sees the emphasis on data protection as a right-based approach. As a developing nation, India will need time for the new area of law to become functional or implemented. The data protection problem is largely concerned with the following areas: the right to privacy, the right to information, information technology, the Indian Penal Code, national security, intellectual property, corporate affairs, consumers, and so on. The purpose of this study is to investigate the existing legislative position of privacy and data protection in India as a matter of right. The legality of privacy and data protection has gotten a lot of attention lately. As a consequence, it is important to assign a certain legal position. The effectiveness of the present legislative framework must be assessed in order to give enhanced protection against privacy issues. It evaluates the nature of an individual's rights as a consequence of data protection violations under other laws. The purpose of presenting this subject is to connect the notion of India to other countries. The human species has significantly profited from technical advances. However, technological improvements are gradually undermining many of our rights. With the advent of the digital age and the incorporation of often collected and sold data in the new economy, the right to privacy is becoming more crucial. Other criminal behaviours, such as identity theft, stalking, and online victimization, have arisen as a consequence of technology improvements. Personal information provided by people in social media, marketing, communication surveillance corporations, government and private

*BBA LLB, SECOND YEAR, NMIMS, NAVI MUMBAI.

stakeholders, and other sites may often be misused. In India, there is no specific rule controlling data collection, preservation, monitoring, intercepting, obtaining, analysing, using, and storing. The present study seeks to address issues about privacy and data analysis in the digital world. This research analyses privacy issues by examining conditions under which data gained by people may be misused and, in some instances, used against the person who provided it. The paper also investigates the efficacy of the Information Technology Act, as well as other existing privacy regulations, and the degree to which they provide data protection protections. Because data is gathered equally in the public and private sectors, the application of legislation to each sector will be investigated and contrasted. Recently, the Ministry of Electronics and Information Technology hired specialists headed by former Supreme Court Judge B.N. Sri Krishna to draft data protection laws. The Personal Data Protection Bill of 2018 was prepared as a draft. However, it was unable to be submitted, thus on December 11, 2019, the Personal Data Protection Bill 2019 was introduced in the Lok Sabha. The present study seeks to analyse the Bill and evaluate how far it may promote the right to privacy and data protection. It will also compare the draft Bills of 2018 and 2019. Overall, the essay aims to examine data privacy laws in India, identify shortcomings, and recommend revisions to guarantee the proper execution of present and future legislation.

Keywords: Data Protection, Constitution, Privacy, Information Technology, Indian Penal Code, Intellectual Property.

INTRODUCTION

Technological advancements are the driving force behind the expansion of any civilization. It has helped the human race bring about change and advancement in society as a whole by interfering in areas such as health, communication, and banking. The twenty-first century has seen a spike in the digital revolution, and India is not an exception. India has the biggest number of internet users. Given this, the Indian government developed and recently implemented the "Digital India" program. The "Digital India" movement resulted in the processing of personal data via the use of multiple electronic gadgets and applications, which has offered many advantages while threatening human rights, notably the right to privacy. The public and commercial sectors are continuously collecting personal data, and because of the widespread use of the internet, people are constantly uploading all of their personal information in a variety of apps, forms, and other electronic devices. For example, when people fill out forms or applications for government or private services; data entry for online marketing; online

shopping; social media posts; upload curriculum vitae to various job sites; purchase sim cards or phone connections; children using electronic devices for online gaming, and so on. All of these activities need us to submit our most important personal information, such as our full name, address, contact information, location, and friends. All of the information that a person has submitted with his or her consent for specific purposes is easily accessible to marketers and organized criminals, who may then use this data and information. This not only violates an individual's right to privacy via various technical means, but it also necessitates data protection laws. Rights, an inherent and inalienable characteristic of human society, have been reduced to a visible and actionable document in both international and national settings. 1 Some rights are clearly referenced in such writings, while others are presented using an interpretative technique because of their basic link to such rights. Among them, the right to privacy is one of the most basic and widely acknowledged personal rights. It enables people to spy on others. The Universal Declaration of Human Rights, the International Covenants of Civil and Political Rights, and the Child's Rights Convention all reference the right to privacy. 2. The right to privacy is the most essential feature of human life. 3 In India, this right is seen as an intrinsic component of the right to life, liberty, and free speech. Every individual has the right to a 'personal sphere' free of unwarranted state or other agency involvement or surveillance. Despite universal recognition of the need to safeguard privacy, international human rights protection mechanisms have yet to adequately define the scope of this right. The lack of clarity in describing the nature of this right has impeded its implementation and enforceability. 5 Because the right to privacy is a qualified right, its interpretation raises concerns regarding how the private sphere is structured and what constitutes public interest. As Prakash Shah, "International Human Rights, A Perspective From India," Fordham International Law Journal, Vol. 21, Issue 1, Article 3 (1997): 24–38. According to Article 12, "No one will be subjected to arbitrary interference with his private, family, home, or communications, nor to assaults on his honour and character. Everyone has the right to the protection of the law against such interference or attacks. A subject of public interest, the right of a human being is infringed upon via the means of communication. The privacy of communications concludes that people may communicate information and ideas in a place that

Modern technology has permeated every aspect of human existence, and it has become a daily occurrence, either through voluntary disclosure or involuntary acquisition of knowledge. In the mid-twentieth century, a right to non-interference in one's personal life was recorded, and it

has grown in importance with the commercialization of technology. Modern computer systems' monitoring capabilities have sparked.

HISTORICAL CONTEXT OF PRIVACY RIGHTS IN INDIA

The Evolution Of Privacy Rights

The concept of privacy in India has deep historical roots, influenced by cultural, social, and legal factors. Traditionally, Indian society valued the notion of personal space and autonomy, albeit within the context of communal living. However, the legal recognition of privacy has evolved over time, particularly in response to changing societal and technological dynamics. In the mid-twentieth century, the Indian judiciary began to grapple with issues related to privacy.

In the landmark case of Justice K.S. Puttaswamy (Retd.) v. Union of India in 2017, the Supreme Court of India unanimously declared that the right to privacy is inextricably linked to the right to life and personal liberty under Article 21 of the Indian Constitution. This decision recognized privacy in its broadest sense, encompassing personal autonomy, informational privacy, and the protection of personal data.

The Impact Of Technological Advancements

The proliferation of smartphones, widespread internet access, and the digitalization of services have led to massive data generation and collection. Government initiatives like Digital India have further accelerated this trend by promoting digital literacy and expanding internet connectivity across the country.

The rise of social media platforms, e-commerce, and digital payments has created vast amounts of personal data, which is often stored and processed by private corporations. The use of big data analytics, artificial intelligence, and machine learning has further complicated privacy [1]issues, as these technologies rely on large datasets to function effectively. These advances necessitate robust legal and technological measures to protect privacy and ensure that individuals maintain

[1]Article 12: "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."

DIGITAL AGE AND PRIVACY IN INDIA

Definition of "Digital Age"

The digital age, also known as the information age, refers to the current era characterized by the rapid development and adoption of digital technologies. In India, the digital age is marked by the widespread use of the internet, mobile devices, and digital services. India's internet user base has grown exponentially, with over 600 million internet users as of 2021, making India one of the world's largest online markets.

Digital Footprints and Data Collection

In the digital age, individuals leave behind a digital footprint—a trail of data generated through their online activities. This digital footprint includes a wide range of personal information, such as browsing history, search queries, social media interactions, and location data. Companies and governments collect and analyse this data for various purposes, including targeted advertising, service personalization, and monitoring.

In India, the digital footprint is rapidly expanding due to increased internet penetration, the popularity of social media platforms, and the government's push towards digitalization. The use of digital payment systems, e-commerce platforms, and online services generates vast amounts of personal data, often without explicit user consent. This data is valuable for businesses, which use it to understand consumer behaviour and tailor their offerings. However,

Data Collection Types and Uses

In India, the kinds of data acquired in the digital era are varied and comprehensive, including:

Social networking networks, e-commerce sites, and government databases gather Personal Identifiable Information (PII), which includes names, addresses, phone numbers, and other identifying information.

Companies utilize behavioural data, including website visits, search queries, and social media interactions, to analyse user behaviour, tailor services, and target adverts.

Biometric data, like as fingerprints and iris scans, is used for identity verification and access to services via the Aadhaar system. However, it also raises privacy and security issues.

Mobile applications and service providers capture location data, which may be used for navigation, marketing, and tracking purposes.

Personal and behavioural data are used by businesses to improve customer experiences, develop new products and services, and drive targeted marketing campaigns, while governments use data to improve service delivery, implement public policies, and conduct surveillance for national security purposes. However, while data can bring significant benefits, it also poses risks to privacy, particularly when data is collected without adequate safeguards.

Concept of Data Protection

Section 2 (o) of the Information Technology Act, 2008 defines "data" as "a representation of information, knowledge, facts, concepts, or instructions which are being prepared or have been prepared in a formalized manner and are intended to be processed." Data protection is becoming more critical globally, and all countries are gradually adopting data protection principles and enacting regulations that govern the use and misuse of personal information.

protection" is derived from the German term "Datenschutz". The data protection concept is more or less connected with the individual's privacy. 13 It is typically reserved for a set of norms that serve a wider range of interests than simply privacy protection. It is not privacy only which has been taken into consideration for data protection. There are a variety of other, partly overlapping concepts that have been invoked too, particularly those of "freedom", "liberty" and "autonomy". In the concern, the first and foremost condition that comes to mind for the individual that data protection is a right or not. 16 An emerging issue in this area is the extent to which such laws should protect organizations and groups. This data protection concept is mostly accepted about the individual's information protection. The scope of data protection is also the protection of information laws to "data subjects" defined narrowly as "living individuals". Thus in the matter of the corporate body, such as a limited company, has no right of access to any information

Computer printouts, magnetic or optical storage devices, punched cards, and punched tapes) or saved internally in the computer's memory." "Data Protection Efforts in India: Are the Blind Leading the Blind?"," The Indian Journal of Law and Technology, Vol. 4 (2008)[2]. Bygrave,

[2] Section 72A, The Information Technology Act, 2000

L.A., "Data Protection Law: Approaching Its Rationale, Logic, and Limits," Kluwer Law[3] International, The Hague, London, and New York, 2002. 15. Westin, A.F., "Privacy and Freedom," Atheneum, New York (1970); Miller, A., "The Assault on Privacy: Computers, Data Banks, and Dossiers," University of Michigan Press, Ann Arbor (1971). Westin's key book, Privacy and Freedom, is a prime example. Indeed, as discussed further below, "privacy" in this context has tended to be regarded primarily as a type of autonomy - that is, one's capacity to regulate the flow of information about themselves. 16 In the matter of The Central Public Information Officer, Supreme Court of India v. Subhash Chandra Agarwal and Others. It has been asserted that "the right to access public information and processing of this information by the state agencies and governments, in democracies, is an accountability measure empowering citizens to be aware of the actions taken by such state "actors". This transparency value must be balanced against the legal interests protected by law, such as other basic rights, notably the right to privacy. Certain conflicts may arise in certain circumstances of access to information and personal data protection, owing to the fact that neither right may be exercised completely in all cases. All affected parties' rights must be respected, and no one right must take precedence over others unless in clearly stated situations. There are two types of information seen as exceptions to access; the first usually refers to those matters limited only to the State in the protection of the general public good, such as national security, international relations, confidentiality in cabinet meetings, etc. The second class of information with the state or its agencies is personal data of individual citizens, investigative processes, or confidential inf Individuals' personal data is safeguarded by the rules of access to secret data and privacy rights." About itself, since the organisation is not a data subject, and information about it is not considered personal data.

As a consequence, the authoritative relevance of data protection issues is questioned. The state, non-state actor, or individual who will protect it as a matter of legality. The two most important aspects of data protection for non-state actors are: first, a narrower definition based on the argument that legislation should apply to organisations, particularly smaller businesses, because information about the organisation may indirectly reveal information about the organisation's owners and controllers. Second, in a broader sense, organizations have legitimate rights to information about them held by others, just as individuals have. 18

[3] Rule 3, The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal data or Information) Rules, 2011

Several countries have data protection directives. The European Union's data protection regulations are complicated. 19 According to EU rules, personal data may only be gathered legitimately in limited situations and for a good cause. Furthermore, persons or organizations who collect and manage your personal information must protect it from misuse and preserve certain data owners' rights as outlined in EU law. The absence of comprehensive privacy legislation in the United Nations is a major concern for EU nations, making establishing whether the United States offers an adequate level of protection difficult. While the government is working hard to establish privacy laws covering different categories of data, the enormous number of proposals in Congress dealing with privacy concerns indicates that the United States may continue to pursue a piecemeal approach to privacy legislation.

CONSTITUTIONAL STATUS

The Indian constitution contains provisions such as "freedom of speech and expression" 22 and "right to life and personal liberty." Article 19 (1) (a) of the Indian Constitution; Article 21 of the Indian Constitution. Bharati Law Review, October–December 2016 59

These restrictions have an impact on the right to privacy, a fundamental right. There are several examples 24 that show the right to privacy as a fundamental right. The conceptual basis of this approach is also linked to the new dimension of 'Data Protection'. The link between privacy and data protection is interdependent. The right to data protection is closely related to a person's 'information' 25.

The analysis of constitutional provisions to understand the relationship between privacy and explicitly stated rights, as well as the interpretation offered by the country's highest court. 26 It examines the problem of data protection under several laws. 27 Finally, it provides a reason for addressing data protection via a rights-based lens.

Sir John Simmons defines human rights as "rights possessed by all human beings [at all times and in all places], simply by virtue of their humanity... [They] will have the properties of universality, independence [from social or legal recognition], naturalness, inalienability, non-forfeitability, and

In a case, The CPIO, Supreme Court of India v. Subhash Chandra Agarwal and Others. The Information Technology Act of 2008 defined "information" as "any material in any form, including records, documents, memos, e-mails, opinions, advice, press releases, circulars,

orders, logbooks, contracts, reports, papers, samples, models, data material held in any electronic form, and information relating to any private body which can be accessed by a public authority under any other l 26 It has been decided that in the case of Ram Jethmalani & Ors v. Union of India, (2011) 8 SCC 1. "The right to privacy is an essential component of the right to life, a valued constitutional principle, and it is critical that human beings are granted zones of freedom that are free of public observation unless they engage in illegal behaviour. Disclosing people's bank account information without first establishing prima facie grounds to accuse them of wrongdoing would violate their right to privacy. The State cannot compel citizens to reveal, or reveal details of the imprescriptibly. Only in this way can an explanation of human rights communicate the core notion of rights that may always be claimed by every human being." 28 As a consequence, the concept of defending human rights includes data protection. The universality and independence of data protection are significant considerations for individuals. These data protection safeguards also confer a right to privacy.

The most important and revealing conclusion is that privacy and data protection are inextricably linked. different links or shadows symbolize various sites associated with different [4]regimes. Privacy, like seclusion, solitude, and isolation, is a concept related to these terms, but it is not synonymous with them; it goes far beyond the purely descriptive aspects of privacy, such as withdrawal from the company, curiosity, and the influence of others, to imply the right to exclusive control over access to individual realms. The court's role in fostering this developmental right is also being emphasized as a matter of right.

Individual rights may be obtained naturally, therefore the right to privacy must also be earned organically. Herbert Hart, a jurist, authored a key paper titled "Are There Any Natural Rights?" that distinguishes between 'universal rights' and special rights'. Special rights derive from special transactions [or] particular connections' such as pledges, contracts, or participation in a political society, while general rights belong to 'all individuals capable of choice...in the absence of those exceptional circumstances which give birth to special rights'. This study also discusses whether data protection is a general or specific right.

[4] Rule 4, The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal data or Information) Rules, 2011

Right to Privacy and Data Protection.

The 'Right to Privacy' permits a person to separate himself from others. It often enables users to select whether or not to share personal information with others. It simply refers to a person's right to express themselves to certain persons. It does, in reality, enable us to pick which components are available to others, as well as manage the degree, manner, and timing of their usage. The right prohibits others from making any public statements about the person without his or her consent. If someone does this, he is violating the individual's rights and may be held liable in a civil case for damages. The right to privacy is a fundamental right recognized by international treaties such as the Universal Declaration of Human Rights (1948), the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, the United Nations Convention on the Protection of Children, and the International Covenant on Civil and Political Rights.

Unlike the International Instruments, the right to privacy in India is not a separate right. It is, in fact, enshrined in Article 216 of the Indian Constitution and recognized as a right via a series of Supreme Court decisions, starting with R. Rajagopal v. State of Tamil Nadu[5] also known as "Auto Shankar's Case." In this case, Auto Shankar, who was imprisoned for many murders at the time, authored an autobiography in which he chronicled his interactions with various IAS, IPS, and other police personnel. Some were complicit in his actions. In this case, the editor of the Tamil magazine "Nakkheeran" filed a writ petition to prevent government officials from interfering with the publishers' right to publish the autobiography. The Supreme Court held in the case that government employees do not have the right to privacy when it comes to public responsibilities, even if the disclosure is based on erroneous information. Thus, it was decided that the State or its officials have According to Article 12, "No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks on his honour and reputation." Everyone has the legal right to be safeguarded from such interference or assaults.

According to Article 14[6], "no migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home correspondence, or

[5] (1994) 6 SCC 632

[6] Article 14: "No migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home correspondence or to other communications, or to unlawful attacks on his or her honour and reputation. Each migrant worker and member of his or her family shall have the right to the protection of the law against such interference or attacks."

other communications, or to unlawful attacks on his or her honour and reputation." Every migrant worker and member of his or her family will be entitled to legal protection against such interference or assaults.

of Article 16[7]: "No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation."

of Article 17.1[8]: "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."

Article 21: "No person shall be deprived of his life or personal liberty except in accordance with the procedure established by law." There is no legal authority to impose prior restrictions on the distribution of defamatory information. Officials may only take action if the publication is shown to be false.[9]

Thus, the right to privacy is closely tied to Article 21 of the Indian Constitution, which guarantees the right to life and personal liberty. However, in India, the right to privacy is not guaranteed. It is subject to a number of restrictions, including a legal procedure that must be just, fair, and reasonable; if it is in the interest of India's sovereignty and integrity; if there is a significant countervailing interest that is superior; in the interest of the state; not available to individuals who voluntarily enter into controversy; and if it is against the interests of private citizens.

Moving on to data protection. Let us first define what we mean by 'data'. Section 2(1)(o) of the Information Technology Act 2000 defines "data." It describes the actual technique of data collection, which may be stated as follows:

It asserts that data is—

a representation of data, knowledge, facts, or concepts.

[7] Article 16.1: “No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.”
[8] Article 17.1: “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.”
[9] Article 21: “No person shall be deprived of his life or personal liberty except according to the procedure established by law.”

instructions; which are now being prepared.

were created in a standardized manner using a computer system or Computer networks.

It further specifies that such data may be provided in a number of forms, such as computer printouts, magnetic or optical storage media, punched cards, or punched tapes, as well as stored internally in the computer's memory.

The amount of data generated has expanded due to India's digital push, widespread usage of the internet, and the proliferation of applications on devices for a variety of purposes. There is little question that data generation has helped people by enhancing productivity and social advancement. However, the produced data is not secure and is often misused, infringing on an individual's right to privacy. This issue was recently raised before the Supreme Court in the case of K.S.Puttaswamy (Retd.) v. Union of India.8 In 2012, retired High Court Judge Puttaswamy challenged the constitutional validity of the UPA Government's "Aadhaar Card Scheme," which required people to submit biometric data for an identity card that would allow them to access government services and benefits. It was claimed that the Aadhar Card Scheme violated people. It was brought before a Bench of three judges, who issued an order requiring that a Bench of appropriate size investigate the subject as well as the legality of the Court's orders in Madhya Pradesh. Sharma v. Satish Chandra, District Magistrate, Delhi9; Kharak Singh v. State of Uttar Pradesh10. This case was first considered by a five-judge panel but was then referred to a nine-judge bench on July 18, 2017. The Supreme Court unanimously determined that the right to privacy is an intrinsic component of the right to life and personal liberty guaranteed by Article 21 of the Constitution. Thus, the right to privacy may result in two interrelated protections: against the world at large (the ability to select what personal information is published into public space) and against the state (a necessary consequence of democratic ideals, limited governance, and State power restriction). The nine-judge bench in Justice K.S. Puttaswamy (Retd) v. Union of India11 decided whether the "Aadhar Card Scheme," which was introduced by the UPA Government of India to collect and compile demographic and biometric data of Indian residents for various purposes, violates the "right to privacy."

During a discussion of the right to information and privacy in today's world, the Hon'bleMr. Justice D.Y. Chandrachud expressed his views on "informational privacy." He stated that in this information age, a person's right to privacy is jeopardized not only by the state but also by

some non-state actors. Thus, he suggests that, prior to such an application, the Union Government assesses and establishes a robust data protection framework that strikes a balance between individual rights and reasonable governmental interests. He went on to say that in order to achieve such a balance, the Union Government must take into account the legitimate interests of the states while establishing such a strategy, which might include national security, crime prevention and investigation, and so on. In this case, all nine judges unanimously said that the 'right to privacy' is protected by Article 21 of the Indian Constitution and that the 'Aadhaar Card Scheme', which lacks a strong data protection system, violates people's rights. Although this right is protected by Article 21, it must meet three criteria: (i) legality, (ii) the need for a legitimate aim, and (iii) proportionality.

DATA PROTECTION AND LAWS IN INDIA

With the expansion of the internet and data generation in a variety of methods, India is facing difficulties relating to a wide range of cybercrime. Credit/debit card theft, identity theft, money laundering, invasion of privacy, fraud, and so forth. There is presently no formal law in India addressing data protection and the right to privacy. However, we cannot argue that there is no law protecting people from it. There are a few pieces of legislation that address private and national security concerns while simultaneously dealing with data privacy problems to some extent.

The "right to privacy" is protected by Article 21 of the Constitution, which is paired with reasonable constraints on the right to free speech and expression provided by Article 19(1)(a). However, it should be highlighted that India currently lacks explicit regulations for controlling data protection. In the absence of clear data protection regulation, we rely on the Information Technology Act of 2000 and the Indian Contract Act of 1872.

Section 43A of the Information Technology Act of 2000 provides compensation for failure to safeguard data. The main goal of this provision is to protect personal information and privacy. It grants any employee of a corporation the right to compensation if they possess, deal with, or handle sensitive data or information stored in computers or other such means and has violated the rights of those whose data and information they hold by being negligent or failing to maintain reasonable security practices and procedures. According to Explanation (ii) of Section 43A, "reasonable security practices and procedures" are those that were designed to protect such data and information from unauthorized access, damage, use, modification, disclosure, or

impairment as part of an enforceable agreement between the parties or as specified in current laws. In the absence of a written agreement, it should adhere to the Central Government's security rules and procedures.

Explanation (iii) of Section 43A defines "sensitive personal data or information" as any personal information specified by the Central Government in consultation with such professional bodies or associations as it considers necessary. What exactly do the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 describe as "sensitive personal data or information"? It proves that sensitive personal data or information of a person, which means things like password motion regarding bank accounts, credit cards, or debit cards; health condition, which includes physical, physiological, and mental health; sexual orientation of a person; biometric information; medical records; or any details provided to a body corporate.12However, it also provides that any information is freely available and is accessible in public documents.

According to the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, any corporation that collects, receives, possesses, stores, deals with, or handles information from an information provider must provide a privacy policy for handling or dealing in personal information, including sensitive personal data or information. A body corporate's policy should also ensure that the information and data given by people are available for review under a valid contract. Such policies should be made available on the business website. The policy must be unambiguous, expressing its processes and standards in a style that is easily accessible to those who will supply their information. It should also consist of the type of personal and sensitive data that are collected; the purpose of collection and usage of such information; disclosure of information, including sensitive personal data or information as provided in Rule 6; and reasonable security practices and procedures as provided under Rule 8.13 Rule 6 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 provides The Information In addition to the aforementioned rules, telecommunications firms have taken efforts. Telecommunications companies also collect a vast quantity of data via phone calls, SIM card transactions, conversations, phone taps, and other methods. The Indian Telegraph Act of 1885 oversees the telecommunications business in all of these areas, enabling the government to confiscate licensed telegraphs and intercept messages in the case of a national emergency to ensure public safety and the preservation of India's sovereignty and

integrity. TRAI also supervises telecom and internet services (TSPs) in India, requiring all of them to follow the license's terms and conditions, such as subscriber information security and communication privacy. In Karmanya Singh Sareen v. Union Of India[10], a lawsuit regarding WhatsApp users' 'right to privacy' came into question. People use WhatsApp to interact with loved ones, and many prefer it over other applications because of its privacy regulations. On February 19, 2014, Facebook announced that it had purchased WhatsApp. WhatsApp changed its privacy policy on August 26, 2016, allowing it to share user account information, such as phone numbers and contact information, with Facebook, a more public platform than WhatsApp. The amended privacy policy will take effect after September 25th, 2016. Karmanya Singh and Shreya Sethi challenged the amended privacy policy in a writ petition filed in the Delhi High Court. In their petition, they claimed that when WhatsApp was originally founded in 2010, they specified a privacy policy that provided complete safety against the sharing of any user information, as well as extensive security and privacy protection for its users. However, the new privacy policy violates its users' personal rights. However, the Delhi High Court gave the petitioners limited relief, saying that non-existing members' information, data, and details as of September 25, 201,6 would be erased and not shared. As a consequence, users were given the choice of continuing to use the app or not. The petitioners, dissatisfied with the Delhi High Court's decision, filed a Special Leave Petition before the Supreme Court on December 17, 2016.16 The key issues highlighted in this Special Leave Petition are:

Does the alteration of WhatsApp's privacy policy after September 25th, 2016 violate its users' 'right to privacy'?

Do online messaging services that enable users to exchange messages via text, audio, video, and phone/video calls qualify as "telecommunication" services? Is it possible for the proper telecoms authorities to regulate this?

Can WhatsApp allow users to 'not share' data with Facebook?

(d) Many users in our country are unable to read and understand the App's privacy policy. Thus, asking for consent from individuals who are unable to read or grasp the terms is deceptive, dishonest, and unlawful.

The case is now pending before the Honourable Supreme Court.

[10] 233 (2016) DLT 436

Data protection and the right to privacy in the banking sector are governed by laws such as the Credit Information Companies Regulations 2006, RBI circulars including KYC circulars, Master Circulars on Credit Cards, Master Circulars on Customer Services, and the Code of Banks' Commitment to Customers. In the field of medicine and health care, regulations such as the Clinical Establishments (Central Government) Rules 2012 and the Indian Medical Council (Professional Conduct, Etiquette, and Ethics) Regulation 2002 address data protection and the right to privacy. Data protection regulations should apply to both the public and private sectors. Personal information is also maintained by government entities.

THE PERSONAL DATA PROTECTION BILL, INDIA

Although legislation exists in India to safeguard data, the complexity, dynamism, and all-encompassing scope of the digital revolution needs a far more comprehensive regulatory system to meet the current issues. Thus, in August 2017, the Ministry of Electronics and Information Technology established a ten-member Committee, chaired by Supreme Court Judge B.N. Sri Krishna (Retd), to create and codify data privacy legislation in India. After a year of deliberation and public consultations, the Committee has released a draft bill titled "The Personal Data Protection Bill, 2018." The Bill contains provisions governing the processing and collection of individuals' personal data and information by government and private entities incorporated in India and abroad. Along with it, the Bill includes rules for protecting children's personal data, such as age verification, parental consent, and so on. The law also covers the hiring of Data Protection Officers to perform functions such as ensuring compliance with the Act, monitoring data processing activities, and resolving grievances for data principals. It also enables data to be sent across national borders. It can only be done if certain requirements are satisfied. The Bill also has many exemptions if data protection is not available. It also outlines the establishment and powers of the Central Government's Data Protection Authority of India (DPAI). It specifies the following consequences:

The Act prohibits obtaining, transferring, or selling sensitive personal data.

Re-identify and process de-identified personal information.

The legislation creates distinct procedures for dealing with transgressions committed by corporations, and national or state governments. The Personal Data Protection Bill of 2019, with a few revisions, was introduced in Parliament on December 11, 2019. A Joint Parliamentary Committee has been appointed to evaluate the Bill and report on its findings.

The purpose of the Bill 2019 is to protect people's personal information and establish a Data Protection Authority. However, it varies from the Draft Bill of 2018 for the following reasons:

The Bill 2019 retains the meaning of "personal data" as established in the Draft Bill 2018.

Unlike the Draft Bill of 2018, the 2019 Bill eliminates 'passwords' from the scope of sensitive personal data. It also authorized the Central Government (in consultation with the Data Protection Authority) to classify any personal data as sensitive personal data. The Data Protection Authority was granted this authority under the Draft Bill 2018.

The Draft Bill 2018 specifies that the data principal has the right to request confirmation that their data has been processed, as well as to seek correction, transfer, or restriction on the continuing publishing of their data. The Bill of 2019 added one more right to the individual's rights: the right to erase personal data.

According to the Draft Bill 2018, personal data can be processed without the individual's consent on certain grounds, including functions of Parliament or State legislatures, wherein the individual will benefit from such steps by the state and for any reasonable purposes specified by the authority to detect fraud, recover debt, etc., however, the Bill 2019 removes the provision on functions of Parliament or State legislatures for non-con

According to the 2019 Bill, a social media intermediary' is someone who helps people connect and share information online. As a consequence, we suggest that social media intermediaries are critical data fiduciaries who must provide a voluntary user verification option to all users in India. There is no mention of this in the 2018 Draft Bill.

Although we know that government agencies collect data, they are exempt from the requirements of the Draft Bill 2018. However, the Bill 2019 includes them in the regulations while exempting them for certain reasonable reasons, such as defending the nation's integrity or banning encouragement to do any cognizance offence.

Small businesses were also exempt from the provisions of the Draft Bill 2018. The exemption is kept in Bill 2019, although there is a section stating that if the Authority considers its yearly turnover to exceed the statutory level, may be subject to the restrictions.

According to the Draft Bill 2018, one serving copy of all personal data transmitted outside the country would be kept in India. The Bill 2019 removes the obligation to store all personal data and instead requires that only sensitive personal data be kept.

Bill 2019 has changed the composition of the Data Protection Authority of India's selection committee.

According to the Draft Bill 2018, actions such as collecting, exposing, transferring, or selling personal data in violation of the Act, as well as re-identifying and processing de-identified personal data without consent, are punishable by imprisonment. However, according to Bill 2019, only the re-identification and processing of de-identified personal information without authority is punishable by imprisonment.

The Draft Bill 2018 has no provisions for utilizing non-personal data gathered by the government to develop digital economy, growth, and security policies.

The 2019 Bill enables the government to obtain non-personal and anonymised personal data from data fiduciaries in order to better service targeting and evidence-based policy development.

COMPARATIVE PERSPECTIVE: GDPR AND OTHER INTERNATIONAL FRAMEWORKS

The European Union's General Data Protection Regulation (GDPR) is widely regarded as one of the world's most comprehensive and toughest data protection legislation. It establishes a strong foundation for safeguarding personal data while stressing individual rights, openness, and responsibility. The GDPR establishes high requirements for data protection and imposes hefty fines for noncompliance, impacting data protection practices throughout the globe.

In contrast, India's proposed Personal Data Protection Bill aims to accord with global norms while also addressing the country's specific issues and demands. The Bill embraces numerous GDPR principles, such as the right to access, correct, and delete personal data, as well as the necessity for express permission for data processing. However, it incorporates measures unique to India, such as data localization requirements and exemptions for government entities.

Other nations, such as the United States, use a more fragmented approach to data protection, combining federal and state legislation. The California Consumer Privacy Act (CCPA) is one

of the most significant state-level privacy legislation, providing safeguards comparable to the GDPR but tailored to the unique setting of California. Developing nations such as Brazil and South Africa have also enacted extensive data protection legislation, reflecting a worldwide trend toward better privacy safeguards.

CHALLENGES OF PRIVACY IN THE DIGITAL AGE

Government surveillance

Government monitoring poses a serious threat to privacy in the digital era, especially in India. Surveillance tactics, which are justified in terms of national security and law enforcement, often violate individuals' private rights. The Indian government uses a variety of surveillance methods, including telecommunications monitoring, internet traffic interception, and social media inspection. Government measures to enhance surveillance capabilities include the Central Monitoring System (CMS) and the National Intelligence Grid (NATGRID).

While monitoring is critical for national security and terrorist prevention, a lack of supervision and openness raises worries about possible abuse of power. The lack of a clear legal framework for surveillance operations exacerbates these issues. The Supreme Court's recommendations in the Puttaswamy case underline the need for proportionality, necessity, and judicial monitoring for surveillance, but putting these ideas into practice remains difficult.

Corporate Data Practices

Corporate data practices, especially those of internet behemoths like Facebook, Google, and Amazon, present substantial privacy risks. These corporations acquire massive quantities of personal information, sometimes without the user's express agreement, and utilize it for targeted advertising, service customisation, and other commercial objectives. The commercialization of personal data has created worries about data misuse and privacy violations.

In India, the expansion of digital services and e-commerce platforms has resulted in widespread data collecting by private enterprises. The absence of rigorous data protection legislation has enabled businesses to engage in opaque data practices, which often result in illicit data sharing and breaches. The proposed Personal Data Protection Bill seeks to solve these difficulties by

establishing requirements on data processors and granting data subjects rights, but its adoption and enforcement are still pending.

Cybersecurity Threats

Cybersecurity dangers such as hacking, data breaches, and cyberattacks pose substantial hazards to digital privacy. India's increasing dependence on digital infrastructure and online services has made it a prime target for hackers. High-profile data breaches, like those involving Zomato, Big Basket, and Aadhaar, have exposed millions of people's personal information, underlining the digital ecosystem's vulnerabilities.

The Indian government has made attempts to improve cybersecurity, including the National Cyber Security Policy (2013) and the formation of the Indian Computer Emergency Response Team (CERT-In). However, the changing nature of cyber attacks needs ongoing advancements in cybersecurity measures, such as stronger encryption procedures, safe data storage, and quick reaction systems.

TECHNOLOGY SOLUTIONS FOR PRIVACY PROTECTION IN INDIA

Encryption and Anonymization Techniques

Encryption is an important technique for safeguarding digital privacy since it ensures that data, even if intercepted, cannot be viewed without the appropriate decryption key. In India, using end-to-end encryption in messaging applications such as WhatsApp and Signal has considerably improved communication privacy. However, the government's desire for backdoor access to encrypted communications for monitoring reasons has stirred discussion over the right balance of privacy and security.

Anonymization methods, which remove personally identifying information from datasets, are critical for safeguarding individual privacy while still enabling data to be utilized for analysis and study. These strategies are especially useful in industries such as healthcare and financial services, where sensitive data must be secured.

Privacy Enhancing Technologies (PETs)

Privacy-enhancing technologies (PETs) are meant to reduce data gathering while maintaining user anonymity. Some examples of PETs are:

Differential Privacy is a technology that introduces statistical noise to datasets, enabling businesses to gather and analyze data while maintaining individual privacy. Companies such as Apple employ differential privacy to secure consumer data.

Federated Learning trains machine learning models over numerous decentralized devices, minimizing privacy hazards. Google has looked at federated learning to improve privacy in AI applications.

Zero-Knowledge Proofs: These cryptographic approaches enable one party to confirm the correctness of a statement without exposing any underlying knowledge. Zero-knowledge proofs are used for a variety of purposes, including secure transactions and identity verification.

Blockchain and Decentralized Systems

Blockchain technology provides interesting possibilities for increasing privacy via decentralization. Blockchain technology can be used in India's finance, healthcare, and supply chain management sectors to ensure secure and transparent transactions without the need for centralized data control. Blockchain's immutability and transparency can improve trust and accountability while lowering the risk of data manipulation and fraud.

The Indian government's use of blockchain to secure land records is an example of how this technology can be used for public good. However, implementing blockchain solutions necessitates addressing issues such as scalability, interoperability, and regulatory compliance.

BALANCING PRIVACY WITH OTHER RIGHTS AND INTERESTS IN INDIA

National Security and Law Enforcement

Balancing privacy and national security is a complicated topic in India. The government claims that monitoring and data collecting are essential for countering terrorism, reducing crime, and upholding law and order. However, there are worries about a lack of monitoring and the possible abuse of surveillance authorities. The Supreme Court's instructions on the use of Aadhaar and the need for a Data Protection Authority seek to strike a balance, but stronger measures are required to guarantee that monitoring activities are reasonable and subject to judicial oversight.

Business Interests and Innovations

Businesses in India depend on data to innovate and improve their services. Data-driven insights empower businesses to create new products, improve consumer experiences, and fuel economic development. However, there must be a balance between using data for corporate objectives and respecting individuals' privacy. The proposed Personal Data Protection Bill tries to remedy this by placing requirements on data processors, promoting openness, and offering rights to data subjects. The problem comes in developing a legislative climate that supports innovation while respecting privacy.

Freedom of Expression and Information

Privacy must also be balanced with the right to freedom of speech and access to information. In India, ensuring that people may express themselves freely without fear of unwarranted monitoring is vital for democracy. At the same time, privacy laws are important to avoid the exploitation of personal data for harassment, manipulation, or suppression of opposition. Striking a balance between these rights involves sophisticated rules that protect both privacy and freedom of speech.

CASE STUDIES

Aadhaar and Privacy Concerns

The Aadhaar initiative, which intends to provide a unique identifying number to each Indian citizen, has prompted serious privacy issues. The risks include mass surveillance, data breaches, and biometric data exploitation. The Supreme Court's verdict in the Puttaswamy case supported Aadhaar's legitimacy while imposing strong privacy limits, including tricking its obligatory usage and guaranteeing data protection. Despite these efforts, concerns concerning Aadhaar's rollout and data management remain, emphasizing the need for offering supervision and improvements in data security standards.

Pegasus Spyware Incident

In 2021, it was discovered that the Israeli business NSO Group produced Pegasus spyware, which was used to target activists, journalists, and politicians in India. This event exposed the weaknesses in digital communications, as well as the possibility of government exploitation of surveillance technologies. The Pegasus malware may infect cellphones and harvest a variety

of data, including texts, emails, and location information, without the user's awareness. The incident sparked widespread demands for tougher legislation and monitoring to preserve privacy and avoid the abuse of surveillance capabilities.

Data Breach Incidents in Indian Companies

Several high-profile data breaches have happened in India, revealing the personal information of millions of people. For example, the Zomato data breach in 2017 compromised the data of 17 million users, while the Big Basket hack in 2020 exposed the data of more than 20 million consumers. These instances highlight the need for effective cybersecurity safeguards and tougher data protection legislation. They also emphasize the significance of openness and responsibility in corporate data practices, as well as the necessity for consumers to understand their privacy rights and take precautions to secure their personal information.

COMPARATIVE ANALYSIS OF PRIVACY LAWS.

India vs. EU Approaches

GDPR, the General Data Protection Regulation of the European Union, establishes a high standard for data protection by stressing individual rights, openness, and responsibility. It establishes severe fines for noncompliance and compels organizations to adopt strict data protection procedures. The GDPR's principles, including data minimization, purpose restriction, and the right to be forgotten, establish a solid foundation for safeguarding personal data.

India's proposed Personal Data Protection Bill aims to line with global norms while also addressing India's unique requirements and concerns. The Bill embraces many GDPR concepts, but it also includes measures specific to India, such as data localization requirements and exemptions for government institutions. While the Bill is an important step toward complete data security, its efficacy will be determined by how it is implemented and enforced.

Lessons From Other Countries

Countries such as Brazil and South Africa have extensive data protection legislation that might serve as good lessons for India. The GDPR, like Brazil's General Data Protection Law (LGPD) and South Africa's Protection of Personal Information Act (POPIA), emphasizes the protection

of personal data and individual rights. These laws provide frameworks for resolving privacy problems in varied and quickly evolving economies.

The United States has a more fragmented approach to data protection, with a combination of federal and state legislation. The California Consumer Privacy Act (CCPA) is a prominent example, offering privacy safeguards comparable to the GDPR but tailored to the unique setting of California. India's approach may benefit from researching these various frameworks and implementing best practices to handle its own privacy concerns.

THE FUTURE OF PRIVACY IN THE DIGITAL ERA IN INDIA

Potential Legal Reforms

To improve privacy protection in the digital era, India needs significant legislative changes. The passage of the Personal Data Protection Bill is an important start, but further measures are needed to address rising privacy concerns. This includes:

Establishing strong surveillance oversight procedures, such as judicial scrutiny and openness, may avoid abuse and safeguard individual rights. Strengthening cybersecurity measures and establishing best practices among companies and government organizations may prevent data breaches and cyberattacks. Promoting Digital Literacy involves raising public understanding of privacy rights and digital security practices, empowering people to safeguard their personal information.

The Role of Civil Society and Industry

Civil society groups play an important role in promoting privacy rights and keeping the government and companies responsible. Their efforts to raise awareness, conduct research, and provide legal help are critical to strengthening privacy rights. The industry is also responsible for implementing best practices for data security and transparency, ensuring that privacy is emphasized in corporate operations and technology advances.

Global Cooperation and Standards

Privacy is a worldwide concern, and international collaboration is required to manage cross-border data flows and cyber threats. India may benefit from taking part in global conferences and harmonizing its data protection legislation with international norms. Collaboration with

other nations and international organizations may help India secure its citizens' privacy while also promoting economic development and innovation.

CONCLUSION

With data digitalization and processing in almost every field, it is difficult to keep one's personal information from slipping into the wrong hands. As a result, present rules governing personal data protection must be revised and new laws enacted as quickly as feasible. Enacting legislation will not suffice unless adequate mechanisms are in place to defend persons' rights. As a consequence, in addition to the Data Protection Authority, which is specified in both the 2019 Bill, special courts must be established to deal with data protection and other intellectual property rights concerns. Data protection and the right to privacy are intricately intertwined, and although the right to privacy is a significant individual right with reasonable limitations, it is nonetheless safeguarded by Article 21's concept of the right to life and human dignity. As a consequence, constitutional modifications are required to create the right to privacy as a separate article safeguarding individual rights. Incorporating a comprehensive policy that includes the EU's General Data Protection Information Technology principles is critical to ensuring that several Indian cyber security agencies, such as the National Technical Research Organization, the National Intelligence Grid, and the National Information Board, carry out their duties properly. Aside from that, it is vital that we, as people, exercise great care while interacting in the digital world, especially where personal information is involved, in order to avoid being victims of various forms of cyber threats, scams, and personal data theft.