THE PRIVACY AND DATA PROTECTION CONUNDRUM IN INDIA-IS IT A REAL CONCERN?

By Soumyaranjan Sahu
From University Law College, Utkal University, Bhubaneswar

INTRODUCTION:
Data is a broad concept that encompasses both personal and commercial elements of an individual. Personal information is protected by privacy laws, whereas business information is protected by proprietary laws. Data Protection refers to the set of privacy laws, policies and procedures that aim to minimize intrusion into one’s privacy caused by the collection, storage and dissemination of personal data. The progress of technology and e-commerce has not only made life simpler, but it has also resulted in a significant increase in cybercrime, data theft, abuse of private and personal information, and so on. According to cyber protection cells, India has seen a number of incidents of data theft. As a result, an effective and well-designed technique is essential to combat data theft. The idea of the right to privacy is interpreted by Indian courts under Article 19(1)(a) and Article 21 of the Indian Constitution. These rights, however, are subject to reasonable limitations set forth in Article 19(2) of the Constitution. Though there is no express legislation in India governing data protection or privacy, a few provisions in the Information Technology Act, 2000, the Information Technology (Reasonable Security Practices and Procedures and sensitive Personal data or information) Rules, 2011, and the Personal data (Protection) Bill, 2013 address data protection and privacy. In India, a codified legislation on data protection has yet to be implemented.

CONCEPT OF DATA PRIVACY:
Privacy is an emotional idea which differs from one individual to another. It starts from the expression "Privatus" which means isolated from the remainder of the world. As indicated by John Locke, privacy is natural for the thought of opportunity. According to Locke's perspectives, ",an individual who worked inside the bind of a common agreement, yet is free inside the bounds of those agreements." Privacy is a prerequisite for the enlargement and salvation of personhood. Jeffrey Reiman defined privacy as, "a acknowledgment of one's responsibility for or her physical and mental reality and an ethical right to their self-assurance." Information privacy is a new phenomena. With the development of technology and the internet, additional elements to the classic idea of the right to privacy, such as informational privacy or data privacy, have been introduced. Individuals can create both personal and non-personal information about themselves in cyberspace, deliberately or unconsciously, thanks to advances in technology. According to IITF Principle of the Unites States, Information privacy is "an individual's claim to control the terms under which personal information i.e.,information identifiable to the individual is acquired,

---


disclosed, and used".3 The core of informational privacy (also known as data privacy) is the claim of an individual to control disclosures, use, or access to information belonging to that person. The interaction between data acquisition and distribution, technology, legal and political concerns surrounding them is referred to as informational privacy or data privacy. It includes information that connects an individual to certain events, background facts, or other information. The right to privacy in information depends on whether the subject matter is "personal information" or non-personal information, because non-personal information cannot be claimed as having a right to privacy. The larger definition of informational privacy applies to both personal and group information. Informational privacy, as defined by Westin as "the right to govern how others use information about us," becomes an integral aspect of the right to privacy. As a result, informational privacy provides a framework of rights that includes both personal and public domain rights.

Indeed, the collecting of sensitive data, as well as social and individual profiling, can lead to discrimination; consequently, privacy should be defined as "the protection of life choices against any kind of public control and social stigma." Because the information flow contains not only "outbound data" (to be kept out of the hands of others), but also "inbound" information on which one may desire to exercise a "right to know," informational privacy can be considered a type of privacy. This finally emphasises data privacy, which is defined as "the right to maintain control over one's information and to select the manner in which one's own private sphere is built."

**INDIAN JURISPRUDENCE ON DATA PROTECTION AND PRIVACY:**

**ARTICLE 21:**
Article 21 of the Indian Constitution provides that, "No person shall be deprived of his life or personal liberty except according to the procedure established by law."4 However, the Indian Constitution does not explicitly acknowledge the 'right to privacy' as a basic right. This question has been brought several times before the judiciary, and the judiciary has reached different conclusions in different situations. The question of whether the right to privacy is included in Article 21 was questioned in the case of M. P. Sharma and Others v Satish Chandra, District Magistrate, Delhi and Others5. However, in this instance, the Supreme Court declined to recognise the right to privacy as a fundamental right. This issue was raised again in one of the landmark judgements in the case of K. S. Puttaswamy (Retd.) v Union of India6 the court in this case said that Privacy is a constitutionally protected right which emerges primarily from the guarantee of life and personal liberty in Article 21 of the Constitution. Elements of privacy also arise in varying contexts from the other facets of freedom and dignity recognized and guaranteed by the fundamental rights contained in Part III.”

**PERSONAL DATA PROTECTION BILL 2019:**
The decision in K. S. Puttaswamy (Retd.) v Union of India resulted in the creation of the

---

3 Principles for Providing and Using Personal Information (“IITF Principles”) issued by the Clinton administration’s Information Infrastructure Task.

4 The Constitution of India 1949 Article 21

5 1954 AIR 300

6 (2017) 10 SCC 1

PIF 6.242 www.supremoamicus.org
Personal Data Protection Bill\textsuperscript{7}, which is presently a draught legislation on data protection in India. On 11th December 2019, the measure was introduced in the lower house of parliament. It has yet to be enacted by Parliament, but it offers us a good picture of how data privacy legislation are progressing in India. This Bill proposes to regulate the handling of personal data of persons by government institutions and business enterprises incorporated in India and overseas. Individuals will have many rights with relation to their data, such as the ability to request corrections or access to data maintained with private businesses. The law allows for exemptions in some types of data processing, such as processing for national security, judicial procedures, and so on. It also makes it obligatory to keep a copy of data on Indian soil. Certain sensitive personal data must be kept entirely in India. Data processing is only permitted if the individual grants consent, in the event of a medical emergency, or by the state for the purpose of giving benefits to its inhabitants.

While the bill provides a framework for data protection and aims to protect data, it contains several shortcomings: The data protection act requires data trustees to collect data in a fair and appropriate manner that respects the privacy of the individual. The bill does not specifically state what is a fair and equitable way to process personal data, which could lead to principles of fairness and adequacy that may vary between data trustees and the processing of similar types of data in the same company. B. in reporting a data breach and determining whether the data breach has harmed the chief data officer, which could lead data trustees to selectively disclose data breaches, and prevents the data protection authority from being triggered in the event that a data breach involves some personal data Person concerns. The bill also does not provide definitions for some key terms. It is not clear what a “service copy” of the data entails. In addition, it does not specify what is included in the definition of "important personal data". It is important that data trustees plan in advance to only store sensitive data.

RULES THAT ARE CURRENTLY GOVERNING DATA PROCESSING AND PROTECTION IN INDIA:

The current data protection framework is laid forth in the Information Technology Act 2000 (IT Act) and the rules published under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (“IT Rules”).

INFORMATION TECHNOLOGY ACT 2000:

\begin{itemize}
  \item Pursuant to Section 43A of the IT Act, any company that owns, processes or handles information or sensitive personal data on a computer resource, that it owns, controls or operates and that is negligent in maintaining and implementing practices and appropriate security procedures, is causing damage, the loss or illicit gain of any person is responsible for paying damages and losses as compensation to the person concerned.
  \item Sec. 66A of the Act deals with identity theft and specifies that anybody who illegally or dishonestly uses another person's digital
\end{itemize}

\textsuperscript{7}By the Minister of Electronics and Information Technology
signature, password, or any other unique identification feature will be sentenced to three years in jail and fined up to Rs.100,000 (one lakh rupees).

• Section 69 of the IT Act of 2000 covers each interception and monitoring, also as decryption, for crucial reasons of work crime in India. underneath this clause, the govt. has also declared the knowledge Technology (Procedures and Safeguards for Interception, Monitoring, and cryptography of Information) Rules, 2009.

• Under section 69A of the IT Act, the govt. has notified the information Technology (Procedures and Safeguards for blocking for Access to Information) Rules, 2009, that affect web site blocking. As a results of this law, the government has barred access to many websites. The 2011 IT rules compel body corporates that store sensitive personal information of users to fulfil sure outlined standards of security so as to forestall data from theft.

• Section 72 of the IT Act states that any person who, in pursuance of any of the powers conferred by this Act, rules or regulations made thereunder, secures access to any electronic record, book, register, correspondence, information, document, or other material and discloses such electronic record, book, register, correspondence, information, document, or other material to any other person without the consent of the person concerned shall be punished with imprisonment for a term not exceeding one year.

• Sec.75 of the IT Act states that the provisions of the IT Act apply to any person who commits an offence or contravention outside India if the act or behaviour constituting such crime or contravention includes a computer, computer system, or computer network situated in India.

INFORMATION TECHNOLOGY (REASONABLE SECURITY PRACTICES AND PROCEDURES AND SENSITIVE PERSONAL DATA OR INFORMATION) RULES, 2011:

Following the adoption of severe and demanding data protection legislation by the European Union, the Ministry of Communications and Information Technology established IT Rules in 2011. The Act includes provisions for three categories: corporations, governments, and Information providers.

Rule 3 of IT Rules states "sensitive personal data" includes passwords; monetary info, reminiscent of checking account or mastercard or revolving credit or alternative payment instrument details; physical, physiological, and psychological state conditions; sexual orientation; medical records and history; biometric information; any details concerning the higher than clauses as provided to a body company for service provision; and any information received below the above clauses by a body corporate for service provision.”

• As per Rule 2(1)(i) of IT Rules, Personal information is defined as "any information that pertains to a natural person and is capable of identifying such a person, either directly or indirectly, in conjunction with additional information accessible or expected to be available with a body corporate.”

Also, Except for IT rules, no statute defines personal data. Furthermore, the IT Rules impose a requirement on the Body Corporate to create a privacy policy,
which must be posted on the Body Corporate's website. The policy must address personal information and sensitive data, as well as the purpose of collection and use. The IT Rules also cover the method and procedure that the Body Corporate should follow while collecting personal information and sensitive data. It further stipulates that the Body Corporate may not keep the information for any longer than is legally needed. Before releasing information to a third party, the Body Corporate must also get the agreement of the information provider. Government entities obliged by law to gather information relating to personal information and sensitive data are exempt. The Body Corporate must use appropriate security standards, as outlined in Rule 8 of the IT Rules.

ISSUES AND CONCERNS:
In many ways, the Puttaswamy case represents a watershed moment in Indian law, emphasising the need of recognising and safeguarding informational privacy. "To make this right meaningful, it is the role of the state to put in place a data protection system that, while safeguarding individuals from threats to informational privacy coming from state and non-state actors, promotes the common good," it was held. This view of the state's responsibility is what the committee must work with when developing a data protection framework"

Although the judiciary's views on accommodating informational privacy as part of privacy are undoubtedly progressive, the researcher expresses worry that these views may open the door to a fresh floodgate of lawsuits on some pretext or another relating to the right to privacy. Aside from the basic problem that individuals have no control over information about them and that their information is used for commercial interests, there are a few other issues to consider, which are described below.

NO COMMAND OVER INFORMATION
According to the RTI request to UIDAI, the terms of UIDAI agreements with US-based biometric service providers such as L-1 Identity Solutions Operating Company Private Ltd, Morpho and Accenture Services Private Ltd were using Aadhar data. This is evident in Section 15.1 “Data and Equipment” and Sub-section 3 permitting the collection, use, transmission, storage and processing of data. The key question here is: Can people control how others use and process information about them? 'It is a constitutional right to maintain the confidentiality of information.'

ABSENCE OF THE RIGHT TO BE DELETED
Given the potential of social media and also the World Wide Web, Justice Kaul sees a desire for the "right to be forgotten." He believed that, "the right to be forgotten relates to individuals' capability to limit, de-link, remove, or amend the exposure of non-public info on the web that's deceptive, humiliating, irrelevant, or outdated." thanks to the correct to privacy, a private should have management over his personal information, which means that if he decides to get rid of his information, it must be deleted from cyberspace. However, knowledge protection laws across the world support the right to be forgotten however not the right to be deleted. Forgotten implies that the info will stay in cyberspace; the sole distinction is that it'll show at very cheap of search results pages, whereas the correct to be deleted permits the
owner of data the power to fully erase it from cyberspace.

**INADEQUATE CROSS-BORDER PROTECTION**

In Puttaswamy, an intriguing identification is formed regarding the practicableness of defensive basic rights not simply against official action, however additionally against non-public persons. in step with Justice Chandrachud, the information are often ruled by the state through the look of an appropriate data protection law, which can embody regulation of information misuse by private persons as well. thus far, the Indian court and legislative authorities have totally debated and controlled the protection of the proper to privacy among domestic jurisdiction against each state and non-state actors. However, cross-border protection of informational privacy remains uncontrolled.

**ABSENCE OF ETHICAL APPROVAL**

Another threat to informational privacy noted by judges is the lack of informed consent. Most privacy rules in today's era of 'click-wrap' contracts are exceedingly complicated and couched in legalese. In actuality, very few people read the permission for posted on the internet. The absolute nature of acceptance or denial, as well as the necessary character of most digital services, provide important challenges to the conventional definition of "informed consent," inasmuch as whether those who are uninformed of usage and ramifications may offer agreement to use of the same. The judges expressed their worry about the regulation of informational privacy, believing that consent should be extended not just for data collection but also for the objectives for which it was acquired and to the degree it was released.

The primary threat comes from totalitarian regimes. Service providers do not pay adequate attention to ensuring high levels of privacy and security for various internet platforms. Existing legislative measures in certain nations are quite effective in protecting residents' privacy in the age of big data. However, appropriate application of the 'Rule of Law' is uncommon.

The study made a number of recommendations on the topic of personal privacy in the age of big data.

- It is proposed that the state establish a set of clear norms on data collection, monitoring, storage, and ownership for authorities, technology corporations, and other players involved in the gathering of user data.

- It is important to have a robust privacy policy and security measures in place to safeguard individuals from potential cybersecurity risks and abuse of power by the government and private parties. The privacy legislation should be written in such a manner that it protects all types of personal data, such as passwords, financial information, health issues, medical history, and biometric information, as well as a necessity to get individuals' consent before collecting any personal information. If an app requires the user's personal information, that data must be deleted as soon as the app is finished.

- To address the issue of privacy, a multi-stakeholder strategy is required. In the age of big data, many stakeholders must adhere to certain common and some independent best practises while collecting, storing, analysing, and processing personal data and information.
• It is advocated that a regulatory authority such as TRAI (Telecom Regulatory Authority of India) control how data is utilised and gathered, as well as the availability of data in the public domain by both state and non-state actors.

• It is proposed that public consultations be held on ways to strengthen people’s privacy and data protection protections.

• If necessary, get judicial authorisation for access to any information held in any data centre.

• Provide appropriate physical and digital protections for various data centres.

• Stop all ongoing mass surveillance and desist from bulk data collection on civilians in the grounds of national security or public order.

• Obtain prior authorisation in scenarios of national security or counter-terrorism.

• It is advised that while collecting data from users, users provide informed consent for the storage and use of data.

• It is advised that the end user be educated and that the language used to construct the policy, user agreements, and terms and conditions be simplified as much as feasible. End-user agreements must be more concise and explicit. The exclusions should be indicated to show which data will and will not be shared. The user must be explicitly informed about where and how his or her data will be used (purpose), and the data acquired must be confined to the indicated use.

CONCLUSION:
Good government in the digital era is unachievable without the efficient deployment of digital services and the active participation of citizens. At the same time, governments must ensure that citizens are safeguarded from damage when utilising various digital services and preserve the human rights framework. A unified digital platform may collect many sorts of data that aid in the proper, seamless, rapid, and effective coordination of government operations. The importance of establishing a single digital platform for governance cannot be overstated, particularly in emerging nations where mobile networks are quickly expanding.

With the exponential expansion in the way individuals consume and create data all around the world, data is becoming increasingly valuable. With data fueling growth, it will be critical to secure people’s data. The existing Indian legal framework on informational privacy and data protection is insufficient to handle the growing concerns about data gathering, leakage, and connection. There is undoubtedly a need for comprehensive legislation that addresses informational privacy and associated challenges. Once the Data Protection Bill of 2019 is passed, we may assume that informational privacy will be strictly monitored in the future. As technology advances at an unfathomable rate, more study into issues concerning the preservation and regulation of informational privacy is unquestionably necessary.

SELECT BIBLIOGRAPHY:
2. PRIVACY IN INDIA IN THE AGE OF BIG DATA by Buddhadeb Halder
4. The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act)
5. Information Technology (Reasonable Security Practices And Procedures And Sensitive Personal Data Or Information) Rules, 2011:

*****