International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 03 | March - 2023 Impact Factor: 7.185 ISSN: 2582-3930

DATA PROTECTION AND PRIVACY LAWS CURRENTLY IN INDIA WITH CONTRAST TO EUROPE

Aditya Narayan & Prajwal Aggarwal

ABSTRACT

Data protection is the process of safeguarding important information from corruption, compromise or loss. It covers three broad categories: traditional data protection, data security, and data privacy. Data privacy defines who has access to data, while data protection provides tools and policies to restrict access. The Personal Data Protection Bill is a controversial draft law that aims to implement similar provisions as the General Data Protection Regulation into data protection law in India. The PDP Bill has been referred to a Joint Parliamentary Committee for further debate and examination which lays down various recommendations and modifications to the report.

This paper analyses how India lacks a stand-alone data protection law. Even though the Information Technology (IT) Act of 2000 governs the use of personal data, this has been found to be insufficient for ensuring its protection. A Committee of Experts on Data Protection was established in 2017 to look into matters pertaining to data protection in the nation. The Personal Data Protection Bill, 2019 was presented in Lok Sabha in December 2019 and withdrawn from Parliament in August 2022. The Draft Digital Private Data Protection Law, 2022 was released by the Ministry of Electronics and Information Technology in November 2022 for public comment. These amendments need to be done to protect people from fraud and ensure fair and justice for the people.

RESEARCH PROBLEMS

- Lack of uniform and properly formed laws for data protection at national level in India.
- Issues related To Personal Data Protection Bill 2019.

INTRODUCTION

Data protection is the process of safeguarding important information from corruption, compromise, or loss. Data protection assures that data is not corrupted, is accessible for authorised purposes only, and follows applicable legal or regulatory requirements. Protected data should be available when needed and usable for its intended purpose. Data protection spans three broad categories, namely, traditional data protection (such as backup and restore copies), data security, and data privacy.

The importance of data protection increases as the amount of data created and stored continues to grow at unprecedented rates. There is also little tolerance for downtime that can make it impossible to access important information.

The terms data protection and data privacy are often used interchangeably, but there is an important difference between the two. Data privacy defines who has access to data, while data protection provides tools and policies to actually restrict access to the data. Compliance regulations help ensure that user's privacy requests are carried out by companies, and companies are responsible to take measures to protect private user data.

Piracy, act of illegally reproducing or disseminating copyrighted material, such as computer programs, books, music, and films. Although any form of copyright infringement can and has been referred to as piracy, this article focuses on using computers to make digital copies of works for distribution over the Internet.

LAWS AND PROVISIONS PRESENTLY IN INDIA

India presently does not have any express legislation governing data protection or privacy. However, the relevant laws in India dealing with data protection are the Information Technology Act, 2000 and the (Indian) Contract Act, 1872.

Important acts governing Data Privacy and Protection in India:

1. Information Technology Act, 2000 ('the IT Act')

2. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ('the SPDI Rules')
3. Consumer Protection Act, 2019 ('CPA')
4. Consumer Protection (E-Commerce) Rules, 2020
5. Copyright Act, 1957
6. Personal Data Protection Bill, 2019

Background of The IT Act and the SPDI Rules

The Information Technology Act, 2000 deals with the issues relating to payment of compensation (Civil) and punishment (Criminal) in case of wrongful disclosure and misuse of personal data and violation of contractual terms in respect of personal data.

Most companies, regardless of sector, are most keenly impacted by the IT Act and the SPDI Rules. The IT Act mandates that body corporates (e.g., companies, firms, sole proprietorships, and other associations of individuals engaged in commercial or professional activities) that handle sensitive personal data or information are liable to pay damages for any loss caused by their negligence in implementing and maintaining reasonable security practices and procedures.

While the IT Act does not define 'reasonable security practices and procedures,' the SPDI Rules, framed under the IT Act, specify minimum standards of data protection for sensitive personal data. The SPDI Rules are not intended to be exhaustive, but require companies to have a privacy policy, to obtain consent when collecting or transferring sensitive personal data or information, and to inform data subjects of recipients of such collected data. One of the major differences between the SPDI Rules and other more modern data regimes is that consent continues to be the primary ground for processing data.

The Government has notified the *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011*. The Rules only deals with protection of "Sensitive personal data or information of a person", which includes such personal information which consists of information relating to: -

- Passwords
- Financial information such as bank account or credit card or debit card or other payment instrument details
- Physical, physiological and mental health condition
- Sexual orientation
- Medical records and history
- Biometric information.

In this regard, the IT Act also prescribes criminal penalties that include both imprisonment of up to three years and fines for persons that disclose personal information without the consent of the person to whom the data relates, where such disclosure is in breach of a contract or results in wrongful loss or gain.[1]

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules) regulate[2]:

• Collecting, receiving, possessing, storing, dealing, handling, retaining, using, transferring, and disclosing sensitive personal data or information (SPDI) (Sections 5 to 7, Privacy Rules).

• Security practices and procedures for handling SPDI (Section 8, Privacy Rules).

• Data subjects' rights to review and update SPDI and withdraw consent for SPDI processing (Sections 5(6) and 5(7), Privacy Rules). Some practitioners interpret the Privacy Rules to apply to all personal information with additional requirements for collection and processing that involves SPDI. Under this interpretation, requirements that apply to only SPDI include:

• Obtaining the data subject's prior written consent for collection, disclosure, and transfer of SPDI.

• Ensuring the collection is necessary for or directly related to a lawful purpose.

[1]Khaitan&Company,https://www.khaitanco.com/sites/default/files/202104/Data%20Protection%20in%20India%20Overview.pdf, (last visited Mar. 21, 2023)
[2] Lexdocs, https://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf, (last visited Mar. 21, 2023)

• Disclosing SPDI to third parties only under limited circumstances.

Retaining SPDI for only as long as necessary to fulfill the organization's purpose for collecting it. The IT Act regulates personal information disclosures that:

• Breach a lawful contract.

• Are made without the data subject's consent

(Section 72A, IT Act, as amended by Section 37, IT Amendment Act.) Sectoral laws may provide additional regulations applicable to participants in the relevant sector. For more on these sectoral laws, see Sectoral Laws.

Do special rules apply for certain types of personal data, such as sensitive data

Section 43A of the Information Technology Act 2000 as amended by the Information Technology (Amendment) Act 2008 (IT Act and IT Amendment Act) and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules) apply to sensitive personal data or information (SPDI).

Indian laws do not specifically prescribe data transfer agreements so there are no forms or precedents approved by any national authority. For more on the rules governing transfers, However, the Indian government has clarified that the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules) apply only to the body corporates that collect information from natural persons. Entities that provide services relating to collection, storage, or handling SPDI under a contract with a covered body corporate within or outside of India, such as outsourcing organisations, are exempt from complying with the personal data collection and disclosure obligations set out under Privacy Rules 5 and 6 (Clarification on Privacy Rules, Press Note dated August 24, 2011). For general and country-specific resources to help organisations comply with data protection laws when transferring personal data across borders, see Cross-Border Personal Data Transfers Toolkit.

The Copyright Act, 1957

The Copyright Act, 1957 protects original literary, dramatic, musical and artistic works and cinematograph films and sound recordings from unauthorised uses. Unlike the case with patents, copyright protects the expressions and not the ideas.

Draft legislation and policies

· Personal Data Protection Bill, 2019

· Non-Personal Data Governance Framework ('the NPD Framework'), which is currently being deliberated by the Committee of Experts constituted under the Ministry of Electronics and Information ('MeitY')

· Digital Information Security in Healthcare Act, 2017 ('DISHA')

Personal Data Protection Bill, 2019

The Personal Data Protection Bill is a controversial draft law that aims to implement similar provisions as the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') into data protection law in India. The PDP Bill had, on December 12, 2019, been referred to a Joint Parliamentary Committee ("JPC") for further debate and examination. On December 16, 2021, after nearly 2 years of deliberation on the PDP Bill, the JPC has tabled its report on the PDP Bill (hereinafter referred to as the "Report"). The Report lays down various recommendations and modifications to the PDP Bill.

Dissent towards the Report

Several members of the lower house of the Parliament (Lok Sabha) have raised their voices against the recommendations provided by the Report. The main concerns regarding the recommendations of the Report and the proposed "Data Protection Bill" are that it gives sweeping powers to the Government to exempt any or all of its authorities from the provisions of the proposed legislation. The dissenting members also note that the Report does not provide any safeguards to guarantee the right of privacy of the individuals. By changing the name of the legislation and widening its scope, the recommendations of the Report have weakened the

framework for protection of privacy. There have been apprehensions that the recommendations of the Report by the JPC have alienated from the framework of the PDP Bill.

Future of the Bill

The ultimate outcome of the right to privacy is dependent on the discussions and modifications made in the PDP Bill, based on the recommendations by the JPC. Since this proposed legislation will be India's first comprehensive data protection law, the Government may propose to modify the PDP Bill and protect the right to privacy of the individuals, while balancing national security and interests of India which necessitates infringement in certain cases within the contours of law already laid down by the Supreme Court of India.

National Intellectual Property Rights Policy, 2016

The National IPR Policy is a vision document that encompasses and brings to a single platform all IPRs. It views IPRs holistically, taking into account all inter-linkages and thus aims to create and exploit synergies between all forms of intellectual property (IP), concerned statutes and agencies. It sets in place an institutional mechanism for implementation, monitoring and review. It aims to incorporate and adapt global best practices to the Indian scenario.

Landmark Cases in India

In the case Justice K.S. Puttaswamy (Retd.) And Another Versus Union Of India And Others[3] a nine-judge bench of the Supreme Court of India held unanimously that the right to privacy was a constitutionally protected right in India, as well as being incidental to other freedoms guaranteed by the Indian Constitution. The case, brought by retired High Court Judge Puttaswamy, challenged the Government's proposed scheme for a uniform biometrics-based identity card which would be mandatory for access to government services and benefits. The Government argued that the Constitution did not grant specific protection for the right to privacy. The Court reasoned that privacy is an incident of fundamental freedom or liberty guaranteed under Article 21 which provides that: "No person shall be deprived of his life or personal liberty except according to procedure established by law".

[3]Justice K.S. Puttaswamy (Retd.) And Another v. Union Of India And Others Writ Petition (Civil) No. 494 Of 2012

NEW AMENDMENTS OF THE BILL OF 2022

PDP Rules 2022[4]

The current legal framework for privacy enshrined in the Information Technology Rules, 2011 (IT Rules, 2011) is wholly inadequate to combat such harms to data principals, especially since the right to informational privacy has been upheld as a fundamental right by the Supreme Court (K.S. Puttaswamy vs Union of India [2017]). It is inadequate on four levels; first, the extant framework is premised on privacy being a statutory right rather than a fundamental right and does not apply to processing of personal data by the government; second, it has a limited understanding of the kinds of data to be protected; third, it places scant obligations on the data fiduciaries which, moreover, can be overridden by contract and fourth, there are only minimal consequences for the data fiduciaries for the breach of these obligations.

The following important sections have been substituted and inserted by the IT Amendment Act, 2008:

1. Section 43A[5] – Compensation for failure to protect data.

3. Section 66A[6] – Punishment for sending offensive messages through communication service, etc. (This provision had been struck down by the Hon'ble Supreme Court as unconstitutional on 24th March 2015 in Shreya Singhal vs. Union of India)

4. Section 66B[7] – Punishment for dishonestly receiving stolen computer resource or communication device.

5. Section 66C[8] – Punishment for identity theft.

6. Section 66D[9] – Punishment for cheating by personation by using computer resource.

[4]TheHindu,https://www.thehindu.com/sci-tech/technology/a-first-look-at-the-new-data-protection-bill/article66162209.ece, (last visited Mar. 21, 2023)
[5] Sec 43A, The Information Technology Act 2000, Act No. 21 Of 2000
[6] Sec 66A, The Information Technology Act 2000, Act No. 21 Of 2000
[7] Sec 66B, The Information Technology Act 2000, Act No. 21 Of 2000
[8] Sec 66C, The Information Technology Act 2000, Act No. 21 Of 2000
[9] Sec 66D, The Information Technology Act 2000, Act No. 21 Of 2000

7. Section 66E[10] – Punishment for violation for privacy.

8. Section 66F[11] – Punishment for cyber terrorism.

9. Section 67[12] – Punishment for publishing or transmitting obscene material in electronic form.

10. Section 67A[13] – Punishment for publishing or transmitting of material containing sexually explicit act, etc, in electronic form.

11. Section 67B[14] – Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc, in electronic form.

12. Section 67C[15] – Preservation and Retention of information by intermediaries.

13. Section 69[16] – Powers to issue directions for interception or monitoring or decryption of any information through any computer resource.

14. Section 69A[17] – Power to issue directions for blocking for public access of any information through any computer resource.

15. Section 69B[18] – Power to authorise to monitor and collect traffic data or information through any computer resource for cyber security.

16. Section 72A[19] – Punishment for disclosure of information in breach of lawful contract.

17. Section 79[20] – Exemption from liability of intermediary in certain cases.

[10] Sec 66E, The Information Technology Act 2000, Act No. 21 Of 2000
[11] Sec 66F, The Information Technology Act 2000, Act No. 21 Of 2000
[12] Sec 67, The Information Technology Act 2000, Act No. 21 Of 2000
[13] Sec 67A, The Information Technology Act 2000, Act No. 21 Of 2000
[14] Sec 67B, The Information Technology Act 2000, Act No. 21 Of 2000
[15] Sec 67C, The Information Technology Act 2000, Act No. 21 Of 2000
[16] Sec 69, The Information Technology Act 2000, Act No. 21 Of 2000
[17] Sec 69A, The Information Technology Act 2000, Act No. 21 Of 2000
[18] Sec 69B, The Information Technology Act 2000, Act No. 21 Of 2000
[19] Sec 72A, The Information Technology Act 2000, Act No. 21 Of 2000
[20] Sec 79, The Information Technology Act 2000, Act No. 21 Of 2000

18. Section 84A[21] – Modes or methods for encryption.

19. Section 84B[22] –Punishment for abetment of offences.

20. Section 84C[23] –Punishment for attempt to commit offences.

Draft Digital Personal Data Protection Bill, 2022[24]

Information that can be used to identify or contact a specific individual is known as personal data. Personal data is processed by both businesses and governmental organisations in order to supply goods and services. Processing personal data enables comprehension of user preferences, which may be helpful for customization, targeted advertising, and suggestion development. Law enforcement may benefit from the processing of personal data. Unchecked processing may have detrimental effects on people's privacy, which has been acknowledged as a fundamental right. Individuals may suffer harm from it including financial loss, reputational damage, and profiling.

India currently lacks a stand-alone data protection law. The Information Technology (IT) Act of 2000 governs the use of personal data. This framework has been found to be insufficient for ensuring the protection of personal data. 1 A Committee of Experts on Data Protection, headed by Justice B. N. Srikrishna, was established by the national government in 2017 to look into matters pertaining to data protection in the nation. In July 2018, the Committee turned in its report. The Personal Data Protection Bill, 2019 was presented in Lok Sabha in December 2019 based on the Committee's recommendations. A Joint Parliamentary Committee was given the bill, and it delivered its report in December 2021. The Measure was withdrawn from Parliament in August 2022. The Draft Digital Personal Data Protection Law, 2022 was released by the Ministry of Electronics and Information Technology in November 2022 for public comment.

Key Features

[21] Sec 84A, The Information Technology Act 2000, Act No. 21 Of 2000
[22] Sec 84B, The Information Technology Act 2000, Act No. 21 Of 2000
[23] Sec 84C, The Information Technology Act 2000, Act No. 21 Of 2000
[24] PRS Legislative Research, https://prsindia.org/billtrack/draft-the-digital-personal-data-protection-bill-2022, (last visited Mar. 21, 2023)

Application: The Bill would be applicable to the handling of digital personal data that is processed in India and that is either (i) obtained online or (ii) gathered offline and converted to digital form. If processing is done to create profiles of people in India for the purpose of selling them products or services, it will also apply to processing done outside of India. Any information on a person who may be identified from or in connection with that information is referred to as personal data. An automated action or series of operations carried out on digitally stored personal data is referred to as processing. It comprises collecting, keeping, utilizing, and sharing.

Consent: Only a legitimate purpose for which a person has provided consent may personal data be handled. Before requesting consent, a notification must be given. Information about the personal data to be gathered and the processing goal should be included in the notice. The ability to revoke consent is always available. When processing is required for one of the following reasons: I carrying out a legal obligation, (ii) providing a service or benefit on behalf of the State, (iii) responding to a medical emergency, (iv) pursuing employment opportunities, or (v) certain public interest purposes like information security, fraud prevention, or national security, consent will be deemed to have been given. The legal guardian must give consent on behalf of minors under the age of 18.

An individual, whose data is being processed (data principal), will have the right to: (i) request information regarding processing; (ii) request rectification and erasure of personal data; (iii) designate a substitute for the data principal in the case of death or incapacity; and (iv) file a grievance. Some obligations will fall on data principals. They may not: I file a fictitious or baseless complaint; (ii) provide any false information; (iii) withhold information; or (iv) impersonate another individual in certain circumstances. Duty violations are penalised by fines of up to Rs 10,000.

A data fiduciary, is required to: (i) take reasonable steps to ensure the accuracy and completeness of data; (ii) put in place reasonable security measures to prevent a data breach and notify the Data Protection Board of India and affected individuals in the event of a breach; and (iii) stop keeping personal data as soon as the purpose has been achieved and retention is no longer required by law (storage limitation). When processing is done by government organisations, the storage limits requirement will not be applicable.

Exemptions: In certain circumstances, such as the prevention and investigation of crimes and the enforcement of legal rights or claims, the rights of the data principal and the duties of data fiduciaries (apart from data security) will not apply. Some activities may be excused from the Bill's restrictions by notification from the central government. They consist of (i) processing by government agencies for the sake of state security and public order, and (ii) gathering information for research, archiving, or statistical purposes.

Data Protection Board of India: The Data Protection Board of India will be established by the national government. The Board's main duties include (i) enforcing penalties for noncompliance, (ii) requiring data fiduciaries to take appropriate action in the event of a data breach, and (iii) listening to grievances brought forth by impacted parties. The composition of the Board, the selection process, the terms and conditions of appointment and service, and the removal procedure are all subject to central government regulations.

Penalties: The Bill's schedule lists fines up to Rs. 250 crore for failing to take security precautions to avoid data breaches and up to Rs. 150 crore for failing to fulfil commitments to children, among other offences. The Board will issue penalties following an investigation.

IP RIGHTS & DATA PRIVACY

Due to the anonymous nature of online piracy, it is difficult for IP owners to identify the infringers and act against online pirates. In order to address this issue, relief is found in the form of John Doe orders (also called Ashok Kumar orders in India), whereby the courts can grant an injunction against anonymous person(s) to protect the rights of IP owners. To elaborate, a John Doe order is an injunction sought against a person whose identity is not known at the time of the issuance of the order. It enables the right holders to serve notice and take action against anyone who is found to be infringing their IP rights. It also allows the plaintiff to search the premises and seize evidence of infringement of its rights by unknown defendants. To obtain a John Doe order, the plaintiff needs to establish (i) a prima facie case, (ii) likelihood of irreparable damage if the order is refused, and (iii) balance of convenience in favour of the plaintiff.

In India, the jurisprudence of John Doe orders originated from **Taj Television Limited v Rajan Mandal[25],** wherein the Delhi High Court issued a John Doe order against cable operators, restraining the

[25] [2003] F.S.R 24

unauthorised broadcasting of the World Cup football tournament. Subsequent to this order, seeking a John Doe injunction became a practice before the launch of any major film or sporting event.

Recently in 2019, the Delhi High Court issued an ex-parte interim injunction against the unauthorised audio broadcast of the **ICC Cricket World Cup 2019 in Channel 2 Group Corporation v Http://Live.Mycricketlive.Net/ and Others[26].** The suit was filed by Channel 2 Group Corporation in anticipation of a likely abuse of its audio rights by a number of defendants, including various websites, radio channels, internet service providers and unknown defendants, by filing an application praying for a John Do order/Ashok Kumar order. The High Court referred to the principle laid down in **Star India Pvt. Ltd. v Piyush Agarwal[27]** which directed that any person wishing to gratuitously relay ball-by-ball or minute-by-minute score updates or match alerts without a license can do so, provided a time lag of 15 minutes is maintained in transmitting such updates.

This 15-minute time lag principle was also upheld by the Supreme Court vide its order of 30 September 2013 in **Star India Pvt. Ltd. v Akuate Internet Services Pvt. Ltd.,[28]**. Placing reliance on the above discussed principle, the High Court granted the ex-parte ad-interim injunction, restraining the defendants from broadcasting/transmitting/communicating to the public any audio/radio streaming of the subject ICC tournament, whether by way of live reporting or deferred updates, through any means without authorisation of the plaintiff. However, it was further clarified that any defendant complying with the interim order may relay the score update gratuitously, maintaining the time lag of 15 minutes. The issued interim order was also directed to operate as a John Doe order against unknown defendants. The High Court further directed the search engines to take down/delete from their search result pages listings of websites/URLs which infringe upon the plaintiff's copyright and broadcast reproduction rights, as and when notified by the plaintiff. The ISPs were directed to comply with the plaintiff's requests to block access to the unlicensed content of the infringing websites, upon the plaintiff giving notice of the infringing activity to the said ISPs.

[26] [CS (COMM) 326/2019, I.A. 8510/2019 and 8508/2019]
[27] 2013 (54) PTC 222 (Del)
[28] SLP (C) No 29633 of 2013

THE EUROPEAN UNION SOLUTION - GENERAL DATA PROTECTION REGULATION (GDPR)

The Global Impact of GDPR

GDPR has affected significant improvements in the governance, monitoring, awareness, and strategic decision-making regarding the use of consumer data. Further, the risk of incurring and paying out hefty fines has made companies take privacy and security more proactively.

Improved Cybersecurity

Organisations have been in a continuous battle for almost as long as the internet has existed. Security upgrades in networks, servers and infrastructures have been a primary source of cyber protection along with other policy and security changes until recently. The passing of GDPR has directly impacted data privacy and security standards while also indirectly encouraging organisations to develop and improve their cybersecurity measures, limiting the risks of any potential data breach.

General Data Protection Regulation (GDPR) imposes significant new restrictions on the collection and processing of personal data by virtually *any* company that has *anything* to do with *any* EU resident. Violators can be fined up to 20 million euros — or 4% of their global annual revenue, whichever is greater.

Overall, the GDPR message is very much in favour of the customer. The new regulations that have been implemented allow users to discover who has their data, why they have it, where it's stored and who is accessing it.

CONCLUSION

The new data protection bill need to be implemented as soon as possible as to protect the people from cyber attract and as the people data is not secure there are numerous attract on India in the terms of data protection after corona India has suffered from many cyber-attacks as from China too there was huge accounts which was hacked which cannot be denied due to which people lost so much of their money and so of the cases where so vast as they have lost their life long earning due to which these news laws need to be amended and protect the people of the country due to which we can safeguard the people. These bills have some boundaries and some boundations on the government to help the people out in that situation as of now the new laws are not implicated and they are in the form of draft. It has only has been presented in the parliament twice and many other times there are always amendments being suggested due to which till now the bill has not been able to be passed as a law in our country.

These amendments need to be done because people are not only losing their money but they are losing their personal data due to which many fake accounts and details are sold in the market due to which the other persons can be cheated and frauded due the details so these new laws and the rest of the laws need to be followed strictly for the fair and justice which needs to be given to the people.