INDIAN PERSPECTIVE ON DATA PRIVACY AND PROTECTION

Written by ***Chetandeep Singh Batra***

Advocate, Punjab and Haryana High Court, Chandigarh, India

ABSTRACT

Data collection has become a great asset for many organisations, leading to more efficient operations and new growth opportunities. Despite this, the data collection load has increased access to sensitive information that may violate data protection laws and jeopardise the privacy of individuals. As a result, data controllers and processors may be imposed harsh penalties for non-compliance, which may even lead to bankruptcy. We explore the present status of legal restrictions in this study and data protection and privacy-preserving strategies under Indian Law.

Keywords: Data Privacy; Data Protection; IT Act; Cyber Rules; Information Security

INTRODUCTION

In today's world, data accumulation is omnipresent, therefore, is data sharing. Google collects information about all users visiting it; Facebook collects and shares information. These firms sell information to others that use it for promoting what's referred to as targeted advertising-supported social behaviour. Even though it's users' personal information, those assembling it share it with others for business functions. Firms are speculated to use truthful data principles like notice, choice, and consent and inform the users before assembling their information. Though firms do take steps like declaring their privacy policy, abundant is left to be termed a fair data transfer. Countries worldwide have enacted entirely different laws to shield people's privacy act of globalisation is gripping people's privacy daily. The fact that more and more personal information is crossing borders in trans-border data flows leads to data being processed into the wrong hands and eventually resulting in cyber and finance-related frauds. Such crimes need to be addressed in national data protection laws. A robust data protection regime requires that cyber crimes of all types be covered to ensure data security and privacy. The amended IT Act does precisely that - it has tried to respond in a way that enhances the trustworthiness of the entire cyberspace.[i]

Organisations must manage and safeguard personal information and address their risks and legal responsibilities regarding the processing of personal data to deal with the growing thickness of applicable data protection legislation, not only on the national level as well at the international level.[ii]

A well-designed and comprehensive compliance program can solve these competing interests and is an essential risk management tool.[iii]

WHAT IS DATA PRIVACY?

In data protection, data privacy refers to how sensitive data is collected, stored, accessed, retained, immutable, and secured. [iv]

Personal data and personally identifiable information (PII) such as names, addresses, Social Security numbers, and credit card numbers are typically considered private data. Besides financial data, intellectual property, and personal health information, the idea extends to other

valuable or confidential information. Industry guidelines often govern data privacy and protection initiatives and regulatory requirements of different governing bodies.

Data privacy is not a single concept or approach.[v] Instead, it's a discipline involving rules, practices, guidelines, and tools to help organisations establish and maintain required levels of privacy compliance.[vi] Data privacy is generally composed of the following six elements:

1. Legal framework- Data privacy laws, for instance, are enacted and applied to data issues.
2. Policies- Developed business rules and policies to protect the privacy of employees and users.
3. Practices- IT infrastructure, data privacy, and security best practices.
4. Third-party associations- Third-party organisations that interact with data, such as cloud service providers.
5. Data governance- Store, secure, retain, and access data using standards and practices.
6. Global requirements- Data privacy and compliance requirements differ or vary among legal jurisdictions worldwide, such as the U.S. and EU).[vii]

A subset of data protection is data privacy. A traditional data protection strategy includes data backups, disaster recovery considerations, and security. Data protection ensures that sensitive business data is kept private and secure while maintaining its availability, consistency, and immutability.

Three key elements to keep data safe are security, access control, and protection.

WHY IS DATA PRIVACY IMPORTANT?

The importance of data privacy directly relates to its business value. As the data economy evolves, more data is being collected and stored by businesses of all sizes. Data is used for a variety of business purposes[viii], including:

- Provide goods and services to customers by understanding their needs;

- Using network and device data to analyse business infrastructure, facilities, and human behaviour;
- Using databases and data sources to gain insight;
- Toto train AI and machine learning systems.

DATA PRIVACY AND PROTECTION UNDER INDIAN LAW

The Constitution of India does not patently grant the fundamental right to privacy. However, the courts have read the right to privacy into the other existing fundamental rights, i.e., freedom of speech and expression under Art 19(1)(a) and the right to life and personal liberty under Art 21 of the Constitution of India. However, these Fundamental Rights under the Constitution of India are subject to reasonable restrictions given under Art 19(2) of the State may impose imposed by the State. Recently, in the landmark case of Justice K S Puttaswamy (Retd.) & Anr. Vs Union of India and Ors., the constitution bench of the Hon'ble Supreme Court, has held the Right to Privacy as a fundamental right, subject to certain reasonable restrictions.[ix]

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, of 2000 and the (Indian) Contract Act, of 18. A data protection bill still awaits a green signal from authorities.

The (Indian) Information Technology Act, 2000 addresses concerns related to civil and criminal penalties for improper disclosure, abuse, and breach of contract involving personal data.

According to section 43A of the (Indian) Information Technology Act, 2000, a corporate body that has, dealing with, or handling any sensitive personal data or information and is negligent in putting into place and maintaining reasonable security practices that result in wrongful loss or wrongful gain to any person may be held liable to pay damages to the person so affected.[x]

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, have been published in the Government's official

notification. The Rules only deal with protecting "Sensitive Personal Data or Information of a Person," which includes such personal information as 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 conditions;
- Sexual orientation;
- Medical records and history;
- Biometric information.

The regulations outline the acceptable security policies and procedures that the body corporate, or any individual acting on the body corporate's behalf, is obligated to adhere to while handling "Personal Sensitive Data or Information." In a breach, the body corporate or any other person acting on its behalf may be held responsible for compensating the individual harmed.

Information disclosure made knowingly and wilfully without the subject's consent and in violation of a valid contract is punished by up to three years in jail and a fine of Rs 5,00,000 (about $8,00) under section 72A of the (Indian) Information Technology Act, 2000.

As an exception to the general practice of maintaining the privacy and secrecy of the information, it should be noted that Section 69 of the Act states that when the Government is satisfied that it is necessary for the interest of:

- the sovereignty or integrity of India,
- defence of India,
- security of the State,
- friendly relations with foreign States or
- public order or
- for preventing incitement to the commission of any cognizable offence relating to the above or

- for investigation of any offence,

Any government agency may be ordered to intercept, monitor, or decrypt information created, sent, received, or stored in any computer resource. It may also induce information to be intercepted, monitored, or interpreted. Under this provision, the government can block, monitor, or decrypt any information, including sensitive personal information, on any computer resource.[xi]

The government has the right to demand the disclosure of information where doing so would be in the public interest. Information on illegal activities against the nation that compromise national security, transgressions of the law or statutory obligations, or fraud may fall into this category.

INFORMATION TECHNOLOGY ACT, 2000

The purpose of the Information Technology Act, 2000 (from now on referred to as the "IT Act") is to establish legal recognition for transactions made through electronic data interchange and other forms of electronic communication, also known as "electronic commerce," which involves the use of alternatives to paper-based methods of communication and information storage to facilitate electronic filing of documents with government agencies.

Grounds on which Government can interfere with Data

Under section 69 of the IT Act, any person authorised by the Government or any of its officers specially assigned by the Government, if satisfied that it is necessary or expedient so to do in the interest of sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any crime, for reasons to be recorded in writing, by order, can direct any agency of the Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource. Section 69 of the IT Act covers interception, monitoring, and decryption to investigate cybercrime. Under the preceding

section, the government has also announced the Information Technology (Procedures and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009.[xii]

The Government has also notified the Information Technology (Procedures and Safeguards for Blocking for Access of Information) Rules, 2009, under section 69A of the IT Act, which deals with the blocking of websites. The Government has blocked access to various websites.

Penalty for Damage to Computer, Computer Systems, etc., under the IT Act

Section 43 of the IT Act imposes a penalty without prescribing any upper limit, doing any of the following acts:

1. accesses or secures access to such computer, computer system, or computer network;

2. downloads, copies, or extracts any data, computer data base or information from such computer, computer system, or computer network, including information or data held or stored in any removable storage medium;

3. introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system, or computer network;

4. damages or causes to be damaged any computer, computer system or computer network, data, computer database, or any other programs residing in such computer, computer system, or computer network;

5. disrupts or disrupts any computer, computer system, or computer network;

6. denies or causes the denial of access to any person authorised to access any computer, computer system, or computer network by any means; provides any assistance to any person to facilitate access to a computer, computer system, or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;

7. charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network; he shall be liable to pay damages by way of compensation to the person so affected.

8. destroys, deletes, or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;

9. steel, conceals, destroys or alters, or causes any person to steal, hide, destroy or limit any computer source code used for a computer resource to cause damage.[xiii]

Tampering with Computer Source Documents as provided for under the IT Act, 2000

Section 65 of the IT Act states that anyone who knowingly or intentionally conceals, destroys, or alters any computer source code used for a computer, computer program, computer system, or computer network when the computer source code is required to be kept or maintained by law for the time being in force is punishable by imprisonment for up to three years, a fine of up to Rs 2,00,000 (approximately US$3,000), or both. [xiv]

Computer related offences

Section 66 states that any person who dishonestly or fraudulently does any of the acts listed in Section 43 is punished by imprisonment for a term of up to three years. Penalty for Breach of Confidentiality and Privacy.[xv]

Section 72 of the IT Act establishes penalties for violations of confidentiality and privacy. The Section states that any person who, in the exercise of any of the powers conferred by the IT Act Rules or Regulations made thereunder, obtains access to any electronic record, book, register, correspondence, information, document, or other material without the consent of the person concerned and discloses such material to any other person is punishable by imprisonment for a term of up to two years or a fine of up to Rs 1,00,000, (approx. US$ 3,000) or with both.[xvi]

Amendments as introduced by the IT Amendment Act, 2008

Section 10A of the IT Act, which deals with the validity of contracts formed through electronic means, states that such agreements "shall not be deemed unenforceable solely on the ground that such electronic form or means was used for that purpose."

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

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

2. Section 66 – Computer Related Offences

3. Section 66A – 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 – Punishment for dishonestly receiving stolen computer resources or communication devices.

5. Section 66C – Punishment for identity theft.

6. Section 66D – Punishment for cheating by personation by using computer resources.

7. Section 66E – Punishment for violation of privacy.

8. Section 66F – Punishment for cyber terrorism.

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

10. Section 67A – Punishment for publishing or transmitting material containing sexually explicit acts, etc., in electronic form.

11. Section 67B – Punishment for publishing or transmitting material depicting children in sexually explicit acts, etc., in electronic form.

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

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

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

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

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

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

18. Section 84A –Modes or methods for encryption.

19. Section 84B –Punishment for abetment of offences.

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

CASE LAW

The judgment of the Supreme Court of India inspired modern Indian case rules on data protection and privacy. In Justice K S Puttaswamy and Anr v. Union of India and Ors [Writ Petition (Civil) No. 494 of 2012][xviii]. The Supreme Court unanimously held in Puttaswamy Case that the right to privacy was an inherent component of the promise of the right to life and personal liberty guaranteed by Article 21 of the Constitution and that it included, at its core, a negative obligation not to violate the right to privacy and a positive right to take all actions necessary to protect the right to privacy. Puttaswamy altered the parameters of Indian privacy law, reinterpreted existing privacy standards, and created the spectre of a substantial common law tort of privacy breach independent of statute restrictions.

The Supreme Court went on to say that any law that violated the right to privacy would be subject to constitutional scrutiny and would have to fulfil three criteria:

- legality;
- necessity; and
- proportionality.

Furthermore, the Supreme Court imposed a positive responsibility on the government to sufficiently establish legislation protecting the right to privacy. Currently, several High Courts are dealing with data privacy concerns in the post-Puttaswamy era. While no apparent judicial pattern can be observed, it is clear that initiatives in India to gather and handle data must examine and anticipate the influence of Puttaswamy on Indian data legislation.[xix]

Other decisions of impact from the Supreme Court include:

- *R Rajagopal and Ors v. State of Tamil Nadu* [Writ Petition (Civil) No. 422 of 1994], which recognised tortious remedies for breach of privacy and the ability to seek damages for invasions of privacy; and[xx]

- *Mr X v. Hospital Z* [Civil Appeal No. 4641 of 1998] dealt with privacy-related implications of disclosures of health data. The Court held that the public interest would override an individual's right to privacy in a conflict between the right to privacy and public interest.[xxi]

Various High Courts have been wrestling with exercising multiple facets of privacy rights in the post-Puttaswamy scenario. Recent decisions by different High Courts on the contours of the right to erasure and the right to be forgotten include Subhranshu Rout in Gugul v. State of Odisha [BLAPL No. 4592 of 2020], Sri Vasunathan v. the Registrar General, High Court of Karnataka and Ors [General Writ Petition No. 62038 of 2016]. Dharamraj Bhanushankar Dave v. State of Gujarat and Ors- Each of these courts took a different opinion. It is reasonable to suppose that the extent and implications of these rights will continue to be disputed in court until the Bill goes into force.[xxii]

Furthermore, the Competition Commission of India, the country's anti-trust authority, is now hearing several complaints involving data usage in conjunction with allegations about abuses of dominance and anti-competitive actions by particular corporations.

DATA PROTECTION BILL 2021

The JPC's report shaped India's data privacy and legal protection regime. The bill has not yet been tabled in Parliament. In its current form, the bill proposes deviations from its earlier two predecessors (2018 and 2019 drafts). The DPB aims to regulate personal data collection, storage, transfer, and use in its latest draft. Furthermore, it extends the provision to foreign-based entities when Indians are subject to their data processing activities.[xxiii]

The bill's central tenets include Individual consent, data breach notification, transparency (prior notice and a privacy policy describing data processing practices), purpose-based processing, technical security, and the rights of individuals who share sensitive personal data like social security numbers or names and email addresses. These rights would allow individuals more control over the processing of their data, as they would be able to remove, correct, and access their data easily.[xxiv]

Perhaps these norms reflect India's economic, national security, and data protection concerns. Individuals' data may be transferred if they consent if the DPA has duly approved a contract in place o if the receiving entity can comply with applicable data protection laws. For validating such data transfers, the receiving entity could also implement adequate technical (e.g., encryption and access control) and administrative (e.g., privacy policies and breach management processes).

The glaring concerns with localisation norms are the costs and technical capabilities required to segregate data and create a single point of failure since data would have to be stored only on a server based in India rather than the conventional practice of using distributed servers across various jurisdictions.

Organisations must implement a consent manager platform to enable individuals to gain, withdraw, review, and manage consent in an accessible, transparent, and interoperable manner. Although the idea seems novel, it is untested.

As we wait for this measure to be passed by the Parliament, it may likely mandate that businesses update their operational methods concerning data-related operations and incorporate privacy into their operating practices.[xxv]

CONCLUSION

By comparing Indian law with the laws of developed countries, it is possible to analyse the ethical requirements for Indian law. In terms of utility and importance, data differ from one another. It is, therefore, necessary to frame separate categories of data with different utility values, as the U.S. does. Additionally, the provisions of the IT Act pertain mainly to the extraction, destruction, and storage of data. The lack of complete data protection ultimately forced companies to enter into separate private contracts to protect their data.

In the modern age, India urgently needs to expedite the passage of the new Personal Data Protection Bill. Millions of Indians' data will be decided by how and when the said Bill gets enacted and how it is enforced.

ENDNOTES

[i] Data Protection - Security and Privacy Information Technology Laws Workshop Delhi University 19 – 21 March 2010 Kamlesh Bajaj, CEO, DSCI
[ii] Ibid
[iii] https://www.scribd.com/document/369822443/Data-Protection-Full
[iv] https://iapp.org/about/what-is-privacy/
[v] https://www.techtarget.com/searchcio/definition/privacy-compliance
[vi] Ibid
[vii] Ibid
[viii] https://www.integrate.io/blog/what-is-data-privacy-why-is-it-important/
[ix] https://www.legalserviceindia.com/article/l37-Data-Protection-Law-in-India.html
[x] Ibid
[xi] https://blog.ipleaders.in/data-protection-laws-in-india/
[xii] https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf
[xiii] Ibid
[xiv] Ibid
[xv] Ibid
[xvi] Ibid
[xvii] https://prsindia.org/theprsblog/explained-draft-amendments-to-the-it-rules-2021
[xviii] https://platform.dataguidance.com/legal-research/justice-k-s-puttaswamy-and-anr-v-union-india-and-orswrit-petition-civil-no-494-2012
[xix] https://www.legalserviceindia.com/article/l37-Data-Protection-Law-in-India.html
[xx] Data Protection - Security and Privacy Information Technology Laws Workshop Delhi University 19 – 21 March 2010 Kamlesh Bajaj, CEO, DSCI
[xxi] Ibid
[xxii] https://www.legalserviceindia.com/article/l37-Data-Protection-Law-in-India.html
[xxiii] https://iapp.org/news/a/the-evolution-of-indias-data-privacy-regime-in-2021/
[xxiv] Ibid
[xxv] https://iapp.org/news/a/the-evolution-of-indias-data-privacy-regime-in-2021/