

Data Protection Laws in India

Published on: June 5th, 2020

Data Protection refers to the set of privacy laws, policies and procedures that aim to minimise intrusion into one's privacy caused by the collection, storage and dissemination of personal data. Personal data generally refers to the information or data which relate to a person who can be identified from that information or data whether collected by any Government or any private organization or an agency.

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 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 Constitution that may be 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 Right to Privacy as a fundamental right, subject to certain reasonable restrictions.

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. A codified law on the subject of data protection is likely to be introduced in India in the near future.

The (Indian) 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.

Under section 43A of the (Indian) Information Technology Act, 2000, a body corporate who is possessing, dealing or handling any sensitive personal data or information, and is negligent in implementing and maintaining reasonable security practices resulting in wrongful loss or wrongful gain to any person, then such body corporate may be held liable to pay damages to the person so affected. It is important to note that there is no upper limit specified for the compensation that can be claimed by the affected party in such circumstances.

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.

The rules provide the reasonable security practices and procedures, which the body corporate or any person who on behalf of body corporate collects, receives, possess, store, deals or handle information is required to follow while dealing with "Personal sensitive data or information". In case of any breach, the body corporate or any other person acting on behalf of body corporate, the body corporate may be held liable to pay damages to the person so affected.

Under section 72A of the (Indian) Information Technology Act, 2000, disclosure of information, knowingly and intentionally, without the consent of the person concerned and in breach of the lawful contract has been also made punishable with imprisonment for a term extending to three years and fine extending to Rs 5,00,000 (approx. US\$ 8,000). It is to be noted that s 69 of the Act, which is an exception to the general rule of maintenance of privacy and secrecy of the information, provides that where the Government is satisfied that it is necessary in 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 above

or

- for investigation of any offence,

It may by order, direct any agency of the appropriate 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. This section empowers the Government to intercept, monitor or decrypt any information including information of personal nature in any computer resource.

Where the information is such that it ought to be divulged in public interest, the Government may require disclosure of such information. Information relating to anti-national activities which are against national security, breaches of the law or statutory duty or fraud may come under this category.

Information Technology Act, 2000

The Information Technology Act, 2000 (hereinafter referred to as the "IT Act") is an act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternative to article-based methods of communication and storage of information to facilitate electronic filing of documents with the 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 officer specially authorised 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 offence, 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. The scope of section 69 of the IT Act includes both interception and monitoring along with decryption for the purpose of investigation of cyber-crimes. The Government has also notified the Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, under the above section.

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 the access of 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 data base or any other programmes residing in such computer, computer system or computer network;

5. disrupts or causes disruption of 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; (g) 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. steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage. Tampering with Computer Source Documents as provided for under the IT Act, 2000 Section 65 of the IT Act lays down that whoever knowingly or intentionally conceals, destroys, or alters any computer source code used for a computer, computer programme, 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, shall be punishable with imprisonment up to three years, or with fine which may extend up to Rs 2,00,000 (approx. US\$3,000), or with both. Computer related offences

Section 66 provides that if any person, dishonestly or fraudulently does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to Rs 5,00,000 (approx. US\$ 8,000)) or with both. Penalty for Breach of Confidentiality and Privacy

Section 72 of the IT Act provides for penalty for breach of confidentiality and privacy. The Section provides that any person who, in pursuance of any of the powers conferred under the IT Act Rules or Regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned, discloses such material to any other person, shall be punishable with imprisonment for a term which may extend to two years, or with fine which may extend to Rs 1,00,000, (approx. US\$ 3,000) or with both.

Amendments as introduced by the IT Amendment Act, 2008

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

How should a legal framework for data protection balance the imperatives of protecting privacy and ensuring innovation and productivity growth? This article examines the proposed data protection legislation in India from the perspective of whether it maintains this balance. In December 2019, the government introduced the Personal Data Protection Bill, 2019, in parliament, which would create the first cross-sectoral legal framework for data protection in India.¹

This article argues that the bill does not correctly address privacy-related harms in the data economy in India. Instead, the bill proposes a preventive framework that oversupplies government intervention and strengthens the state. This could lead to a significant increase in compliance costs for businesses across the economy and to a troubling dilution of privacy vis-à-vis the state. The article argues that while the protection of privacy is an important objective, privacy also serves as a means to protecting other ends, such as free speech and sexual autonomy. A framework for protecting personal data has to be designed on a more precise understanding of the role of privacy in society and of the harms that emanate from violations of individual privacy.

The jurisprudence on privacy therefore changed—from being valued as a right that protected other ends to being an end in itself. Along with holding that privacy is a fundamental right, the judgment also declared informational privacy to be a subset of the right to privacy.⁴ As this article highlights, this shift is consistent with the approach taken in the bill. The bill aims to protect the informational privacy of individuals by creating a preventive framework that regulates how businesses collect and use personal data, as opposed to protecting informational privacy with a view to the consequent harms caused by the violation of such privacy. In doing so, it focuses primarily on regulating practices related to the use of data.

Second, the preventive framework proposed in the bill could lead to significant compliance costs for private businesses. The bill will regulate data use in all sectors of economic activity and establishes significant new compliance requirements for the vast majority of affected businesses. The costs of compliance will be borne across small and big businesses except those that are specifically exempt. This is problematic since most businesses in India are small. Such compliance requirements would be especially onerous for them. This bill also allows the government to compel businesses to share nonpersonal data with it. This, as the article argues, could have deleterious consequences for innovation and economic growth in the long run.

The third major issue with the bill is the proposed design of the Data Protection Authority (DPA). This body will be tasked with regulating the provisions of the bill to frame regulations on issues such as mechanisms for taking consent, limitations on the

use of data, and cross-border transfer of data. The supervisory mandate of the DPA is sweeping, given the fact that it has to regulate a wide array of preventive obligations, such as security safeguards and transparency requirements, that have to be implemented by businesses.

This broad mandate is being proposed in the larger context of India's generally low regulatory capacity. It is likely that the DPA, therefore, may not be able to either effectively implement the bill or effectively protect informational privacy. This article argues that, given its cross-sectoral mandate, the DPA may struggle to build internal capacity, leading to either under regulation or overregulation.

Lastly, the bill allows the government to exempt any of its agencies from the requirements of this legislation and also allows it to decide what safeguards would apply to their use of data. This, as the article argues, potentially constitutes a new source of power for national security agencies to conduct surveillance—and, paradoxically, could dilute privacy instead of strengthening it.

The analysis set forth in this article has been supported by inputs from structured consultations with stakeholders and an empirical analysis of regulatory frameworks in data protection, as well as academic literature on the subject. Participants in roundtables organized by Carnegie India included academics working on privacy, representatives from technology companies and start-ups, and scientific experts. Most participants highlighted specific provisions of the bill that could lead to ineffective regulation or substantial compliance burdens due to the obligations proposed in it. These inputs were corroborated by secondary research, survey reports, and academic literature that highlighted similar issues with data protection regulations in other jurisdictions.

This concludes by proposing a framework for modifying the bill and addressing the issues highlighted. In doing so, it argues that there are structural limits to what problems regulation can solve in the data sharing and data processing markets. This is especially true in India, given the extremely low capacity of regulators across sectors. Therefore, data protection legislation must be narrowly focused and designed toward protecting individuals and society against any injury resulting from data processing. A framework designed with this end in mind would achieve a better balance between privacy and innovation.



Navigated to Data Protection Laws in India