Data Protection and Privacy

Prof.Vivekanandan

Defining data and privacy

- **Information privacy** is the relationship between the collection and dissemination of data, technology, the public expectation of privacy, legal and political issues surrounding them.
- It is also known as **data privacy** or **data protection**,
-
-

The application

-
- Healthcare records
- Criminal justice investigations and proceedings
- Financial institutions and transactions
- Biological traits, such as genetic material
- Residence and geographic records
- Privacy breach
- Location-based service and geolocation
- Web surfing behavior or user preferences using persistent cookies
- Academic research

The existing framework

- 1.**General Application**: Information Technology (Reasonable Security Practices and Sensitive Personal Data or Information) Rules, 2011
- 2.**Govt. Collection of Data**: Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016; Aadhaar (Data Security) Regulations, 2016
- 3.**Banking Sector**: Credit Information Companies (Regulation) Act, 2005; Credit Information Companies Regulations, 2006; circulars of Reserve Bank of India including KYC circulars; Master Circulars on credit cards, etc.; Master Circulars on Customer Services; Code of Bank's commitment to Customers
- 4.**Telecom Sector**: Unified License Agreement issued to telecom service providers by the Department of Telecommunications; Telecom Commercial Communication Preference Regulations, 2010
- 5.**Healthcare Sector**: Clinical Establishments (Central Government) Rules, 2012; Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002

The Justice Sri Krishna Bill

- The Government of India constituted a committee, chaired by Justice Srikrishna (retired), Supreme Court of India in August 2017 to design and draft data protection laws for India.
- The committee after a year of deliberations and public consultations has released a draft bill titled 'The Personal Data Protection Bill, 2018' (**Draft Bill**).
- The Draft Bill will now be discussed in both houses of the Parliament of India before it is passed and adopted with modifications as deemed f

Data principal	· Only natural persons (not restricted to Indian citizens)
Data fiduciary	· Private entity or public entity or individual who determines the purpose and means of processing of personal data
Data processor	· Private entity or public entity or individual who processes personal data on behalf of data fiduciary (not an employee of data fiduciary)

Two types of personal data	· 'Personal Data' and 'Sensitive Personal Data' · Personal Data has been defined to mean data relating to natural person, who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person · Sensitive Personal Data has been specifically defined to include, inter alia, passwords, financial data, health data, biometric data, genetic data, etc.

Applicability	· To data fiduciary or data processor in relation with personal data (not applicable on anonymised data or non-personal data)
Territoriality	· Extra-territorial in operation and is not restricted to Indian entities · Test is 'connection with any business carried on in India' or 'systematic activity of offering goods or services to data principals within India' or 'connection with activity which involves profiling of data principals within India'
Exemptions	· Security of the State; Prevention, detection, investigation and prosecution of contraventions of law; Processing for legal proceedings; Research, archiving or statistical purposes; Personal or domestic purposes; Journalistic purposes; Manual processing by small entities have been exempted from the application of the Draft Bill

Obligations of data fiduciary/ data processor	· Fair and reasonable processing · Lawful processing · Purpose limitation · Collection limitation · Data quality · Data storage limitation · Accountability · Notice to data principal
Grounds for processing personal data	· Consent – free, informed, specific, clear and capable of being withdrawn · Functions of the State · Compliance with law or orders of court · For prompt action · For employment · For reasonable purposes
Grounds for processing sensitive personal data	· Explicit consent · Similar to grounds for processing personal data

Personal data of children	· Safeguards for processing personal data of children
Rights of Data Principal	· Right to confirmation and access · Right to correction · Right to data portability · Right to be forgotten
Transparency and accountability measures	· Privacy by Design · Personal Data Breach notification · Security Safeguards · Data Protection Impact Assessment · Record keeping and Data Audits · Data protection officer · Classification of data fiduciaries as significant data fiduciaries
Transfer of personal data outside India	· Data localization by keeping one copy of personal data in India · Critical personal data (as notified) to be only processed in India · Personal data other than critical data may be transferred outside India on the basis of approved contractual clauses or to countries approved by the Indian regulator

Data protection authority	· Dedicated regulatory authority to be established to monitor implementation of the data protection obligations
Remedies	· Heavy penalties extending up to INR15 Crores (approximately USD 2,143,000) or 4% of total worldwide turnover of preceding FY
Transitional provisions	· Notified data to be within 12 months from the date of enactment · Most provisions to be in force within 18 months from the notified date

A critique

- The data localization section of the new privacy bill might be the most prominently controversial element of the legislation. The bill requires data fiduciaries to store “at least one serving copy” of personal data on a server or data center located in India.

- The government can exempt certain categories of personal data from this requirement. It can also declare certain categories of data “critical” and require that they be stored only in India.

- In other words, foreign internet intermediaries and services, such as Facebook, Uber, Google, Twitter, AirBnB, Telegram, WhatsApp, and Signal may all be required to physically host user data in India. The only discernible reason for such a requirement is to give law enforcement easy access to this data.

- This leads to the second problem with the bill: it allows the processing of personal data in the interests of the security of the state if authorized and according to procedure established by law.
- In addition, it permits processing of personal data for prevention, detection, investigation and prosecution of any offence or any other contravention of law.
- This access to all personal data by the state poses an enormous threat to the right to privacy given the weak safeguards that exist in India against state surveillance.
- In combination with the data localization requirement, the Indian government will have unprecedented access to information about Facebook users.

- The legal framework for government surveillance in India continues to be governed by the PUCL v. Union of India framework which was intended as a stopgap measure by the Supreme Court in 1996, but seems to have been adopted permanently.

- These rules concentrate the power to order and review surveillance in the hands of the executive, without introducing court orders, any form of third party review, or any requirement to notify the subject of surveillance.
- They fall short of all international human rights standards for acceptable safeguards for state surveillance. Under the circumstances, there will be little to prevent the government from helping itself to the detailed datasets collected about citizens.

- Lastly, the draft bill creates a regulatory structure that is not sufficiently independent: the central government has significant control over the regulatory regime, and it is vulnerable to capture by industry.

- The draft bill gives the central government the power to appoint members of the data protection authority upon the recommendation of an outside committee.

- The appointment is for a term of five years, which seems much too short to give a new institution sufficient time to learn the ropes and gain the independence it needs to be an effective regulator.

- The central government also has the ability to remove members of the authority for reasons specified in the law.

Sources

Wikepedia

http://www.mondaq.com/india/x/744160/Data+Protection+Privacy/Data+Protection+In+India

https://www.cfr.org/blog/three-problems-indias-draft-data-protection-billn the law.