Data Protection Law – II
India’s legal regime

16 October 2020

Malavika Raghavan

COL865 Special topic on Computer Applications - Digitization and Privacy

Our Conversation - Tuesday (13th) & Today

1. Objectives of Data Protection

2. Key Concepts & Principles

3. Outline of Data Protection Law in India

Our Conversation - Tuesday

1. Objectives of Data Protection
    - *How is data protection different from privacy? Is it?*
    - *What are the objectives driving laws on data protection?*
    - *What do "data protection laws" look like?*

2. Key Concepts & Principles
    - *Six general concepts* that most data protection laws try to address*

*(*1. General principles – fair & reasonable processing; 2. Collection Principles; 3. Use & Disclosure Principles; 4. Security Principles; 5. User Rights; 6. Processing of Special Concern)*

Our Conversation - Today

1. Outline of Data Protection Law in India

    1. Current state of “data protection” law
       (if you can call it that)

    1. Proposed Personal Data Protection Bill 2018

1. Current law

- The Constitution and the Courts

- The Information Technology Act 2000 (Amended 2008)
    - *Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (RSPP Rules)*

- Sectoral Laws

1. Current law – Constitution & Case law

- The Constitution and the Courts
  - Several key cases covered in earlier sessions by Prof Banerjee
  - Line of cases expanding law on processing and disclosure of personal information in diverse contexts
    - intercepted phone communications (*PUCL v Union of India*, 1997), medical records (*Mr. X v. Hospital Z*, 1999), consumers records held with financial institutions (*District Registrar & Collector, Hyderabad v. Canara Bank*, 2005) to the use of the unique Aadhaar (*Justice K.S. Puttaswamy (Retd) & Anr v. Union of India & Ors,* 2018).
  - *Puttaswamy I (see Part S: Informational privacy)*

1. Current law – Statutes & Subordinate Regs

- The Information Technology Act 2000 (Amended 2008)
    - *S 43A (Compensation for failure to protect data)*
    - *Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (RSPP Rules)*
    - *S 72A (Punishment for disclosure of information in breach of lawful contract)*

- Sectoral Laws
    - Various guidelines and circulars
        - Financial Sector - a selection of **JUST** RBI instruments : (*Master Directions on Know Your Customer, 2016; Charter of Customer Rights; Master Circular on Credit Card, Debit Card and Rupee Dominated Co-branded Pre-paid Card Operations of Banks and Credit Card issuing NBFCs; Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks and NBFCs; Master Circular on Customer Service in Banks, 2015; Guidelines for Licensing Payments Banks; Guidelines on Internet Banking….)*

1. Current law – IT Act 2000 (Amended 2008)

Section 43A	**Section 73A**
❖ A body corporate which ○ Possess, deals or handles any sensitive personal data or information; ○ On a computer resource which it owns controls or operates; ❖ Is negligent in implementing and maintaining reasonable security practices and procedure; ❖ And due to such negligence causes wrongful loss or wrongful gain to any person; ❖ Such body corporate is liable to pay compensation by way of damages to the person so affected (Maximum cap of Rs. 5 crores)	❖ Any person including an intermediary, who; ○ While providing services under a lawful contract ○ has access to any material containing personal information of another person ❖ discloses such material with the intent to cause or knowing he is likely to cause wrongful loss or wrongful gain, either ○ without consent of the concerned person or ○ in breach of lawful contract ❖ such disclosure must not be permitted under the act or any other law for the time being in force ❖ shall be punished with imprisonment which must extend up to three years or with a fine that may extend to Rs. 3 lakhs

1. Current law – “RSPP Rules”

- Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (RSPP Rules)
    - *Issue 1: Vires? Could they have even been passed?!*
    - *Issue 2: “SPDI” coverage*
        - *Password*
        - *Financial information (bank accounts, card information)*
        - *Health condition*
        - *Sexual orientation*
        - *Medical records*
        - *Biometric information+ requirements*

1. Current law – “RSPP Rules”

- Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (RSPP Rules)

  - *Issue 3: Barebones requirements*
    - *Prior written consent + Privacy policy at collection + grievance officer*

  - *Issue 4: Enforcement architecture – poor in theory and wings further clipped in practice*
    - *Grievance officer → “Adjudicating Officer” → Cyber Appellate Tribunal → High Court*
    - *Non-reporting of AO orders or judgments, or even complaints*
    - *Single CAT, No CAT chairman from 2011 – 2016, collapsed to TDSAT in 2017 [Disputed]*

Personal Data Protection Bill 2019

- Definitions
- Key Actors
- Grounds and Exemptions
- Rights & Obligations

Personal Data Protection Bill 2019

- Definitions
    - Anonymisation and anonymised data
    - Personal data
    - Sensitive personal data
    - Processing
    - “harm”?

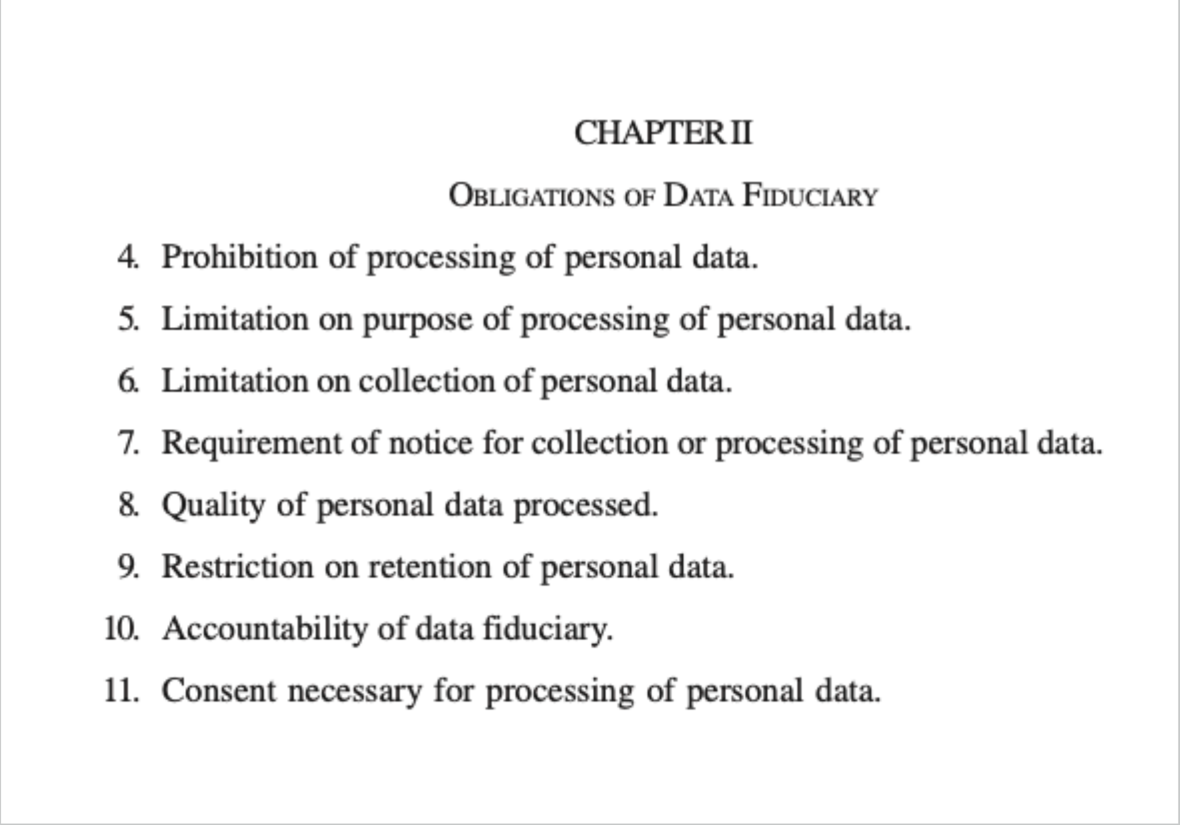
- Key actors
    - Data principals
    - Data fiduciaries
        - *Significant data fiduciaries*
    - Data processors
    - Data Protection Authority

Personal Data Protection Bill 2019

- Grounds and Exemptions
  - In general, you need to have VALID GROUNDS (s. 11 & Ch III) to process personal data
    - Consent
    - Functions of State authorised by law (medical emergency, compliance w/ court order etc.)
    - Employers
    - “Reasonable purposes”
  - UNLESS YOU HAVE EXEMPTIONS (Ch. VII)
    - C Gov can exempt ANY AGENCY OF GOVT (s.35)
    - Law enforcement
    - Domestic use
    - Journalism
    - Limited exemption for Research
    - Manual processing by small entities

Personal Data Protection Bill 2019

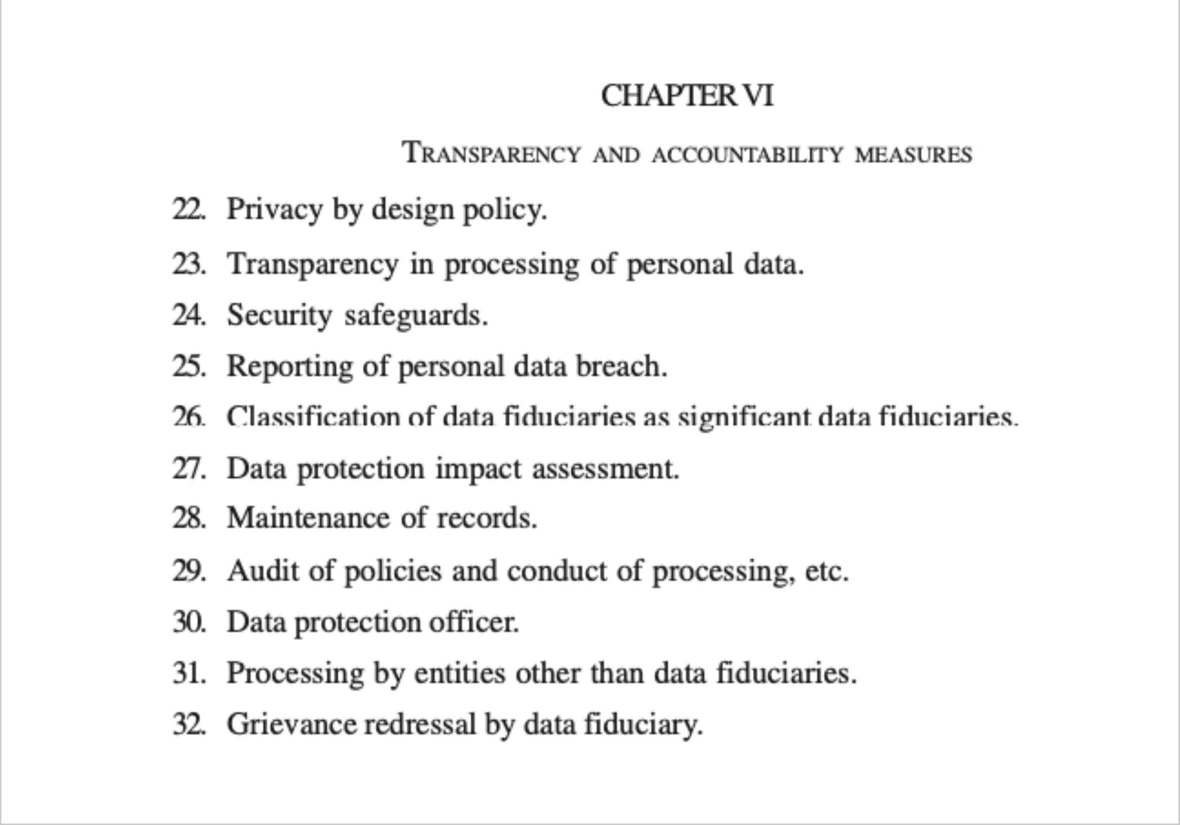
- Obligations (II & VI)
- Rights (V)



CHAPTER II

OBLIGATIONS OF DATA FIDUCIARY

4. Prohibition of processing of personal data.
5. Limitation on purpose of processing of personal data.
6. Limitation on collection of personal data.
7. Requirement of notice for collection or processing of personal data.
8. Quality of personal data processed.
9. Restriction on retention of personal data.
10. Accountability of data fiduciary.
11. Consent necessary for processing of personal data.



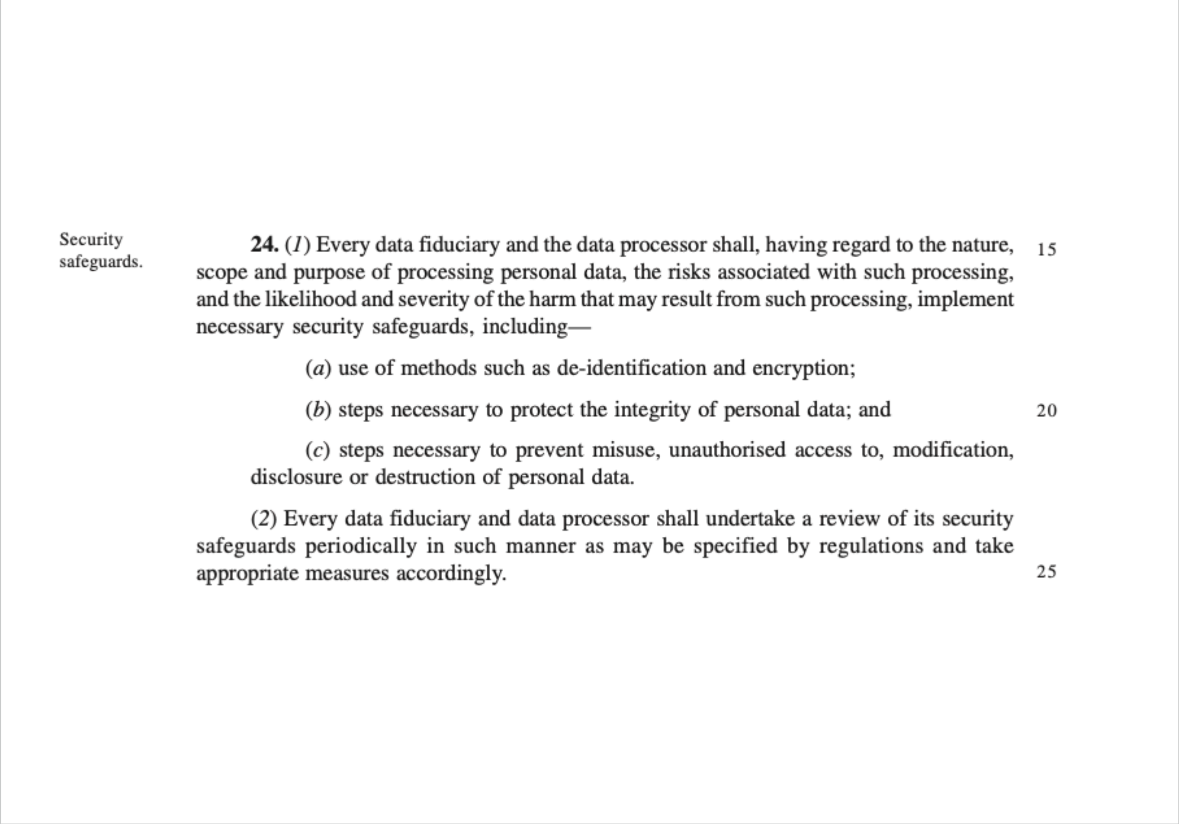
CHAPTER VI

TRANSPARENCY AND ACCOUNTABILITY MEASURES

22. Privacy by design policy.
23. Transparency in processing of personal data.
24. Security safeguards.
25. Reporting of personal data breach.
26. Classification of data fiduciaries as significant data fiduciaries.
27. Data protection impact assessment.
28. Maintenance of records.
29. Audit of policies and conduct of processing, etc.
30. Data protection officer.
31. Processing by entities other than data fiduciaries.
32. Grievance redressal by data fiduciary.

Personal Data Protection Bill 2019

- Transparency, PbD and Data Security



Security safeguards.

24. (*1*) Every data fiduciary and the data processor shall, having regard to the nature, scope and purpose of processing personal data, the risks associated with such processing, and the likelihood and severity of the harm that may result from such processing, implement necessary security safeguards, including—

(*a*) use of methods such as de-identification and encryption;

(*b*) steps necessary to protect the integrity of personal data; and

(*c*) steps necessary to prevent misuse, unauthorised access to, modification, disclosure or destruction of personal data.

(*2*) Every data fiduciary and data processor shall undertake a review of its security safeguards periodically in such manner as may be specified by regulations and take appropriate measures accordingly.

Let's look at

22 (PbD Policy)
23 (Transparency in processing personal data)
24 (Security safeguards)
25 (Reporting of data breaches)

See also s. 27 on DPIAs

Organisation	Dimensions of Risk-based framework	
CNIL, France	Severity*Likelihood	
	Severity: Level of identification of personal data, impact of identification	Likelihood: Vulnerabilities of the supporting asset, capabilities of the risk source
NIST, USA	Likelihood*Impact	
EU GDPR Article 35*	The Risk that the data action poses to then rights and freedoms of natural persons. For activities categorised as high risk activities there is a Data Protection Impact Assessment.	
*Contained in but not limited to article 35	Article 35 has three prominent dimensions: (i) if the data action deals with automated decision regarding or profiling of natural persons (ii) if it deals with special category data (Article 9) and (iii) systematic monitoring of large public areas.	

1. General Principles ✓

- **Fair and lawful processing**
- **Maintaining data quality**

2. Collection Principles ✓

- Limiting data collection to specified purpose ✓
- Means of collection to be lawful, fair and non-intrusive ✓
- Notice on collection
- Collection only with consent ✗

3. Use & Disclosure Principles ✓

- Limiting use or disclosure for specified purpose ✓
- Limiting use or disclosure for secondary or compatible use ✗
- Processing data for new uses after notice ✓
- Exceptions to limitations based on Notice or Consent

4. Security Principles ✓

- **Requiring security safeguards**
- **Issuing breach notifications**

5. User Rights ✓

- Right to access
- Right to correct
- Right to data portability
- Right to deletion or anonymization after use completed/ on request
- Right to withdraw consent or block use of data on request

6. Data & Processing of Special Concern

- Protections for ‘sensitive’ data ✓
- Objections or disclosure of automated processing ✗
- Direct marketing protections ✗

Issues to watch

- Enormous exemptions & powers to Government
- Enormous powers to DPA without sufficient fetters, good Board controls
- High barriers to exercise of rights
- Data localisation – how will it pan out?
- Who will be a “Significant data fiduciary”? And a “social media intermediary”???
- “Consent manager”
- Sandbox
- Non-Personal Data

Data Protection Law – II
India’s legal regime

16 October 2020

Thank you!

Malavika Raghavan - @teninthemorning
raghavan.malavika@gmail.com