Law Related to Cyber security & Data Privacy

Part-1 IT Act 2000

1. IT Act 2000 objectives

1) Legal recognition to electronic transactions
2) Facilitate electronic filing of documents and retention in Govt records.
3) Consequent amendment to other acts
4) Set up licensing, monitoring and certifying authority.

2. Dispatch and Receipt of Records

1) E-dispatch and E-Receipt are absolutely valid.
2) Dispatch happens when it enters a resource outside the control of originator
3) Receipt happens when it enters a designated computer resource. or it is retrieved by addressee.
4) Unless otherwise agreed, Place of dispatch shall be place of Business.

3. controller of certifying Authorities

1. appointed by central Government.
2. It recognise, license, regulate, standardise, supervise certifying authorities
3. Can intercept any information in any computer
4. can declare any system as Protected System
5. Can prevent general or specific access.
6. Certifying authorities license by controller shall issue Digital signature certificate.

4. Offences

1. Tampering with computer source documents.
2. Hacking: destruction, deletion, alteration of any data in any computer with intention of injury / damage.
3. Misrepresentation to controller or certifying authority
4. Breach of confidentiality and privacy.
5. Publishing False DSC.

5. Settlement of Disputes

1. No role of Civil courts.
2. Central Government has established various adjudicating authorities.
3. Appeal lies to Cyber Regulations Appellate Tribunal in 45 Days
4. Appeal against Tribunal lies in HC in 60 days.

Part 2 -

Information Technology (Reasonable security Practices and Procedures and sensitive Personal Data or Information) Rules 2011

1. Data Protection

1. It refers to set of privacy laws, policies and procedures that aim to minimise intrusion into one's privacy.
2. Intrusion may get caused by collection, storage, dissemination of personal data.
3. Personal data may be collected by any private organisation or Govt.

2. Data Protection Law in India

1. India doesnot have separate law for it.
2. IT ~~Act~~ act came into force on 17.10.2000 without Data Protection Provisions.
3. Amendment was done in 2008.
4. Data protection rules came in 2011
5. Section 43A was launched.
6. Right to privacy declared by SC as Fundamental right on 24.8.2017

3. Section 43A

Punishment	Offence
Compensation to aggrieved Party	Negligent in maintaining data security causing loss to any person.

4. Section 72A

Punishment	offence
Imprisonment Max 3 years Fine Max 5 Lakh	Disclosure of information and Breach of confidentiality.

5. Major Contents of Rules of 2011

1.) Notified by Dept of IT
2) Notified on April 11, 2011.
3) Apply to Body Corporate and Person located in India.
4) Defines a list of sensitive personal data :- Password / credit card info / Debit card info / Biometric info / Physical, Physiological, mental Health info.
5) Freely available info is not sensitive.
6) All Body Corporates to have Privacy Policy and should be published on website.
7) Prior permission of information provider before disclosing any information.
8) IS / ISO / IEC 27001 to be implemented for data security
9) Audit to be carried out once a year and whenever systems are upgraded.
10) Specified guidelines to be followed by Body corporates.

6. Specified Guidelines

1) obtain consent from the person providing information.
2) Collection of information only for lawful purpose.
3) Collection only if necessary.
4) Shall be used only for the purpose it is collected.
5) Shall not retained for a period longer than required.
6) Information provider must be aware about such collection and purpose.
7) Information provider must be given an opportunity to review provided information and make corrections.
8) Maintain Data security.
9) Designate Grievance officer whose name and contact details should be available on website.

Part 3 Basic Principles of Data Privacy and Business Intelligence

1. What is BI

→ A technology driven process for analysing data and delivering actionable information that helps executives, managers and workers to make informed business decisions.

2. Steps in BI

1. Data Preparation, in which data sets are organised and modelled for analysis.
2. Analytical querying of prepared data.
3. Distribution of Key Performance Indicator and other finding to Business users
4. Use of the information to help influence and drive business decisions.

3. Why BI is important

1. Improve an organisation's business operations through the use of relevant data.
2. Translate collected data into valuable insights about Business processes and strategies.
3. Such insights can be used to make Better business decisions that increase productivity and revenue leading to High Growth & Profits.

4. Benefits of BI

1. Speed up and improve decision making
2. Optimise internal Business process.
3. Increase operational efficiency & productivity.
4. Spot business problems that need to be addressed.
5. Identify emerging business & market trends
6. Develop Stronger business Strategies
7. Drive Higher Sales and new revenue
8. Gain competitive edge over rival companies.

5. Types of BI Tools and applications

1. Ad hoc analysis :-

Process of writing and running queries to analyse specific business issues on casual basis

2. Online Analytical Processing :-

Enables users to analyse data among multiple dimensions, which is particularly suited to complex queries and calculations.

3. Mobile BI :-

BI applications and dashboard available on smartphones and tablets. This may display 2 or 3 data visualisation and KPI so they can easily be viewed on a small screen.

4. Real time BI :-

Data is analysed as its is created, collected and processed to provide up-to-date view.

5. Operational Intelligence :

Also called operational BI, that delivers information to managers and frontline workers in business operations.

6. Open source BI :-

This typically includes 2 versions :

* a community edition that can be used free of charge.
* another is subscription based commercial release

7. Embedded BI :-

It puts BI and data visualisation functionality directly into business applications.

8. Collaborative BI :-

It involves combination of BI applications and collaboration tools to enable different users to work together.

9. Location Intelligence :-

It enables users to analyse location and geo spatial data with map based visualisation functionality.

(6) Business Intelligence Platforms

Modern BI platforms include:

1) Data visualisation software for charts and infographics
2) Tools for building BI dashboards, reports and performance scorecard
3) Data storytelling features for combining visuals and text.
4) Usage monitoring, performance optimisation, security controls and other functions.

(7) Enterprise BI uses

1) Monitoring Business Performance.
2) Supporting decision making and strategic planning
3) Evaluating and Improving business process
4) Giving operational workers information about customer, equipment, supply chain. and other element.
5) Detecting trend, pattern and relationship.

(8) Real life uses of BI

Airlines & Hotels ⇒ Flight capacity Tracking
Room occupancy Tracking
Selling & adjusting Prices
Scheduling workers.

Health Care ⇒ Diagnosis of diseases
Diagnosis of medical conditions

Universities, school ⇒ overall student Performance monitoring

(9) BI trends

1. BI teams generally include mix of BI architects, developers, analysts, specialists and managers.
2. They work closely with data architects data engineers and other data management professionals.
3. Many organisations are replacing traditional waterfall development with Agile BI and data warehousing approaches.

Part 4 Cyber crime - Cyber Fraud Meaning, Remedies and Penalties

① What is Cyber crime

→ It is a broad term
→ used to define criminal activity
→ in which computer or computer networks
→ are a tool, target or a place of criminal activity.

② Types of cyber crime

Category A Cyber crime against Persons

Category B Cyber crime against Property

Category C Cyber crime against Government

③ Cyber crime against Persons

1. Cyber-stalking :- To create physical threat.
2. Obscenity :- Pornography.
3. Defamation :- Imputing any person to lower down dignity
4. Hacking :- Unauthorised access / control

5. Cracking :- Stranger has broken into computer system without consent and has tampered.

6. Spoofing :- Email which misrepresents its origin. Also, unwanted uninvited messages.

7. Carding :- False ATM cards and credit cards

8. Fraud :- Stealing password and data storage

9. Threat :- Threatening a person with fear for their lives or their families' lives.

(4.) Cyber crime against Property

1. Squatting :- 2 persons claiming same domain name.

2. Vandalism :- Destroying or damaging data when a network service is stopped or disrupted.

3. Hacking :- Unauthorised access

4. Virus :- Program which attach themselves to a computer or file and then circulate themselves

5. Trespass :- Access without right and without knowledge of owner but not for

(5) Cyber crime against Government

1. Terrorism :- Distributed denial of service attack
   Hate website
   Hate emails
   attack on sensitive network

2. Warfare :- Politically motivated hacking to damage and spying.

3. Piracy :- Distributing Pirated software intending to destroy the data and official records of Govt.

4. Unauthorised Information :- Unauthorised access and possession for Political, religious, social and ideological objectives.

(6) Various offences related to Internet which have been made punishable under IT act and IPC

1. Cyber crimes under IT Act

1. Tampering with source document
2. Hacking with computer system and data alteration
3. Publishing obscene information
4. Unauthorised access to protected system
5. Breach of confidentiality and Privacy
6. Publishing false DSC.

2. Cyber crime under IPC and Special Laws

1. Sending threatening messages by Email
2. Sending defamatory messages by Email
3. Forgery of Electronic Records
4. Bogus websites, Cyber Frauds
5. Email Spoofing
6. Web Jacking
7. Email abuse

3. Cyber crime under special acts

1. Online Sale of Drugs under Narcotics Drugs and Psychotropic substances Act
2. Online Sale of Arms under Arms Act