ILE MONTHLY REVIEW

Volume I and Issue V of 2023

ISBN - 978-81-961828-8-5

Published by

Institute of Legal Education

https://iledu.in

# DATA PROTECTION AND CYBER SECURITY

**Author:** Apoorva Chandra, Student at Aligarh Muslim University Centre, Malappuram

**Best Citation** - Apoorva Chandra, DATA PROTECTION AND CYBER SECURITY, ILE Monthly Review, 1 (5) of 2023, Pg. 07-13, ISBN - 978-81-961828-8-5

## I. ABSTRACT

Data protection and cyber security are critical aspects of information technology and have become increasingly important in today's digital age. Data protection involves and refers to the safeguarding of sensitive or personal information from unauthorized access, use, or disclosure, while cyber security involves and focuses on protecting computer systems, networks, and electronic devices from cyber threats such as hacking, malware, and phishing attacks. Effective data protection and cyber security measures are essential for organizations to protect their sensitive data and maintain the trust of their customers. These measures can include implementing strong passwords and authentication protocols, using encryption to protect data in transit and at rest, regularly backing up data, and educating employees on safe computing practices.

In addition to protecting sensitive data, cyber security is also important for ensuring the integrity and availability of computer systems and networks. Cyber-attacks can lead to significant financial losses, damage to reputation, and even the loss of life in certain cases. Overall, data protection and cyber security are critical components of any organization's information technology strategy and must be given the highest priority to ensure the safety and security of sensitive data and computer systems.

**Keywords:** Data Privacy, Data Protection, Information Technology, Cyber Security, Privacy Policy

## II. WHAT IS DATA PROTECTION?

Data protection refers to the process of safeguarding sensitive or personal information from unauthorized access, use, disclosure, modification, or destruction. It involves implementing a range of security measures to protect sensitive data from cyber threats such as hacking, malware, phishing attacks, and insider threats.

Data protection is important for individuals and organizations alike, as it helps to maintain the confidentiality, integrity, and availability of sensitive information. This can include personal information such as names, addresses, social security numbers, and financial information, as well as sensitive business information such as intellectual property, trade secrets, and financial data.

In many countries, data protection is regulated by laws and regulations that govern how personal information must be collected, processed, and stored. For example, in the European Union, the General Data Protection Regulation (GDPR) sets out strict rules for data protection and imposes severe penalties for non-compliance.

Overall, data protection is a critical component of any organization's information technology strategy and must be given the highest priority to ensure the safety and security of sensitive data.

## III. WHAT IS CYBER SECURITY?

Cyber security refers to the practice of protecting computer systems, networks, and electronic devices from cyber threats such as hacking, malware, phishing, and other forms of cyber-attacks. It involves implementing a range

of security measures to protect sensitive data and systems from unauthorized access, use, disclosure, modification, or destruction.

Cyber security is an essential aspect of information technology, as it helps to safeguard the integrity and availability of computer systems and networks, protect against data breaches, and prevent the theft of sensitive information. This can include personal information such as names, addresses, social security numbers, and financial information, as well as sensitive business information such as intellectual property, trade secrets, and financial data.

Cyber security measures can include implementing strong passwords and authentication protocols, using encryption to protect data in transit and at rest, deploying firewalls and intrusion detection systems, conducting regular vulnerability assessments and penetration testing, and educating employees on safe computing practices.

Overall, cyber security is a critical component of any organization's information technology strategy and must be given the highest priority to ensure the safety and security of computer systems, networks, and sensitive data.

## IV. NEXUS BETWEEN BOTH

Data protection and cyber security are closely linked and interdependent. In order to ensure effective data protection, organizations must implement strong cyber security measures to protect against cyber threats and prevent unauthorized access to sensitive data.

Effective cyber security measures can help to prevent data breaches and other cyber-attacks, which can compromise sensitive data and lead to financial losses, damage to reputation, and legal and regulatory consequences. Cyber security can also help to ensure the availability and integrity of computer systems and networks, which are critical for the operation of an organization.

Data protection, on the other hand, involves safeguarding sensitive data from unauthorized access, use, disclosure, modification, or destruction. This can include implementing measures such as encryption, access controls, and data backup and recovery procedures. Effective data protection measures can help to prevent data breaches and minimize the impact of cyber-attacks.

In summary, data protection and cyber security are closely intertwined, and organizations must implement both to ensure the safety and security of sensitive data and computer systems. By implementing effective data protection and cyber security measures, organizations can minimize the risks associated with cyber threats and maintain the trust of their customers and stakeholders.

## V. ITS NEED AND IMPORTANCE

Data protection and Cyber security are of utmost importance in today's digital age. Here are some reasons why:

a. Protection of Sensitive Data: Data protection and cyber security measures are essential for protecting sensitive or personal information from unauthorized access, use, or disclosure. This can include personal information such as names, addresses, social security numbers, and financial information, as well as sensitive business information such as intellectual property, trade secrets, and financial data.
b. Prevention of Data Breaches: Data breaches can result in significant financial losses, damage to reputation, and legal liabilities for organizations. Implementing effective data protection and cyber security measures can help prevent data breaches by reducing the likelihood of cyber attacks and providing early detection and response to incidents.
c. Compliance with Legal and Regulatory Requirements: Organizations are required to comply with a range of legal

and regulatory requirements related to data protection and cyber security, such as the General Data Protection Regulation (GDPR) in the EU and the Cybersecurity Information Sharing Act (CISA) in the United States. Compliance with these requirements is essential for avoiding fines and other legal penalties.

d. Safeguarding Critical Infrastructure: Critical infrastructure such as power grids, transportation systems, and healthcare facilities are increasingly reliant on digital technologies, making them vulnerable to cyber-attacks. Robust data protection and cyber security measures are necessary to safeguard these systems from attack and ensure their continued operation.
e. Protection of Individual Privacy: In addition to protecting sensitive data, data protection and cyber security measures are also necessary for protecting individual privacy. Privacy is a fundamental human right, and organizations have a responsibility to protect the privacy of their customers, employees, and other stakeholders.

Overall, data protection and cyber security are essential for maintaining the confidentiality, integrity, and availability of sensitive data and ensuring the safe and secure operation of digital systems and infrastructure.

## VI. INFORMATION TECHNOLOGY ACT, 2000

The Information Technology Act of 2000, also known as the IT Act, is legislation enacted by the Indian Parliament to provide a legal framework to regulate electronic commerce, electronic governance, and cyber security in India. It was introduced to align Indian laws with international best practices on electronic transactions, and to facilitate e-commerce growth in the country.

The IT Act was amended in 2008 to include new provisions that addressed cyber terrorism, the protection of critical information infrastructure, and the use of electronic signatures. The Act is enforced by the Indian Computer Emergency Response Team (CERT-In), which is responsible for monitoring and responding to cyber security incidents and promoting best practices in cyber security.

The IT Act is divided into 13 chapters that cover a range of topics related to electronic commerce, cyber security, and electronic governance, including:

a. Preliminary: Defines key terms used throughout the Act.
b. Digital Signatures: Establishes the legal validity of electronic signatures and creates a regulatory framework for their use.
c. Electronic Governance: Establishes guidelines for the use of electronic records and digital signatures in government.
d. Attribution, Acknowledgment, and Dispatch of Electronic Records: Establishes legal standards for the creation, transmission, and receipt of electronic records.
e. Secure Electronic Records and Secure Digital Signatures: Establishes standards for the security of electronic records and digital signatures.
f. Regulation of Certifying Authorities: Establishes a regulatory framework for certifying authorities that issue digital signatures.
g. Electronic Signature Certificates: Establishes standards for the issuance and revocation of electronic signature certificates.
h. Duties of Subscribers: Outlines the responsibilities of individuals and organizations that use digital signatures.
i. Penalties, Adjudication and Offences: Specifies penalties and adjudication procedures for violations of the Act.
j. The Cyber Appellate Tribunal: Establishes a tribunal for hearing appeals related to cyber security.

ILE MONTHLY REVIEW
Volume I and Issue V of 2023
ISBN - 978-81-961828-8-5
Published by
Institute of Legal Education
https://iledu.in

k. Offences: Outlines criminal offenses related to cyber security, including hacking, data theft, and cyber stalking.
l. Network Service Providers Not to Be Liable in Certain Cases: Limits the liability of network service providers for content posted by users.
m. Miscellaneous Provisions: Covers a range of miscellaneous topics, including the power of the central government to make rules and the applicability of the Act to offenses committed outside India.

Overall, the IT Act is an important piece of legislation that has helped to establish a legal framework for electronic commerce, electronic governance, and cyber security in India. It has played a crucial role in facilitating the growth of e-commerce in the country and has helped to establish India as a leader in the global IT industry.

### A. OBJECTIVES OF THE ACT

The objectives of the Information Technology Act of 2000 are as follows:

a. To provide legal recognition for transactions carried out by means of electronic data interchange and other electronic means of communication, and to facilitate electronic commerce.
b. To provide for the legal recognition of digital signatures and to create a regulatory framework for their use.
c. To provide for the establishment of a Controller of Certifying Authorities to regulate the functioning of certifying authorities, and to ensure that digital signatures are reliable and secure.
d. To provide for the establishment of a Cyber Appellate Tribunal to hear appeals against orders passed by the Adjudicating Officer under the Act.
e. To provide for the punishment of cyber crimes such as unauthorized access to computer systems, data theft, and the spread of computer viruses.
f. To provide for the protection of critical information infrastructure, and to ensure the confidentiality, integrity, and availability of electronic information.
g. To provide for the protection of personal information and sensitive personal data, and to establish rules for the collection, processing, and storage of such information.
h. To provide for the establishment of the Indian Computer Emergency Response Team (CERT-In) to serve as a nodal agency for responding to cyber security incidents and promoting best practices in cyber security.

Overall, the objective of the Information Technology Act of 2000 is to provide a legal framework to regulate electronic transactions, promote e-commerce, and ensure cyber security in India. It seeks to establish legal standards and guidelines for the use of electronic records and digital signatures, and to provide for the punishment of cyber crimes. The Act also aims to protect personal information and critical infrastructure, and to establish a regulatory framework for certifying authorities that issue digital signatures.

### B. AMENDMENTS TO THE ACT

The Information Technology Act of 2000 has undergone several amendments over the years to keep pace with technological advancements and emerging cyber threats. Some of the significant changes made to the Act by the amendments are as follows:

1. Amendment of 2008: The Amendment of 2008 introduced several new provisions related to cyber security, including the following:
   a. Definition of cyber terrorism and punishment for cyber terrorism offenses.

b. Obligation on organizations to implement reasonable security practices and procedures to protect sensitive personal data.
c. Provision for the establishment of a Cyber Appellate Tribunal to hear appeals related to cyber security.

2. Amendment of 2011: The Amendment of 2011 introduced several changes to the Act to promote e-governance and to protect citizens' rights to privacy. Some of the key changes were:
   a. Recognition of electronic records for the purpose of providing citizen services and benefits.
   b. Provision for the protection of sensitive personal data, including the requirement for explicit consent before collecting and processing such data.
   c. Expansion of the powers of CERT-In to respond to cyber security incidents and to promote best practices in cyber security.
3. Amendment of 2013: The Amendment of 2013 introduced changes to the Act to address the challenges of cloud computing and other emerging technologies. Some of the key changes were:
   a. Recognition of electronic contracts and signatures in cloud computing transactions.
   b. Provision for the establishment of a Digital Locker to store important personal documents in electronic form.
   c. Expansion of the powers of CERT-In to respond to cyber security incidents and to promote best practices in cyber security.

Overall, the amendments to the Information Technology Act of 2000 have helped to strengthen cyber security, promote e-governance, and protect citizens' rights to privacy in India. They have also helped to keep pace with technological advancements and emerging cyber threats.

## VII. IMPORTANT CASES LAWS

### *State of Tamil Nadu v. Suhas Katti*[16]

In the case of State of Tamil Nadu v. Suhas Katti (2004), In order to humiliate the woman, the accused posted pornographic remarks and also disclosed her mobile number, and opened a fraudulent account in her name. The court found the accused guilty. This case encourages citizens all around the nation to come forward and report incidents of online abuse.

### *Amar Singh v. Union of India*[17]

The petitioner in this case of Amar Singh v. Union of India (2011) claimed that his telecom service provider had secretly recorded his calls. The alleged monitoring violated his basic right to privacy under Article 21 of the Indian Constitution. It was held that the service provider must confirm the legitimacy of any government orders "to tap phones" when they include serious errors. To avoid unlawful call interception, the court ordered the central government to establish specific directives and rules.

### *Shreya Singhal v. Union of India*[18]

In the landmark case of Shreya Singhal v. Union of India (2015), the entire Section 66A was declared unconstitutional by the Supreme Court of India on the grounds that its intended protection against annoyance, inconvenience, danger, obstruction, insult, injury, and criminal intimidation went beyond the bounds of reasonable restrictions under Article 19(2) of the Indian Constitution.

### *K.S. Puttaswamy (Privacy-9J.) v. Union of India*[19]

[16] State of Tamil Nadu v. Suhas Katti, C. No. 4680 of 2004, order dt. 4-11-2004 [Additional Chief Metropolitan Magistrate, Egmore, Chennai]

[17] (2011) 1 SCC 210

[18] (2015) 5 SCC 1

The nine-judge bench of the Supreme Court of India upholds the right to privacy as a right protected by the Constitution of India.

***Praveen Arimbrathodiyil v. Union of India***[20]

The Union Government published a set of regulations in 2021. Using the authority granted to it by Section 87 of the IT Act of 2000, the Information Technology (Intermediaries Guidelines) Rules, 2011, are replaced by these regulations. The government aims to control internet streaming services, social media intermediaries, and digital news outlets through these regulations.

As stated in the guidelines, the intermediaries who violate them forfeit the protection granted to them by Section 79 of the IT Act. The regulations also mandate that the digital news media establish an internal grievance redressal system and adhere to an ethical code of conduct.

**PROPOSED DATA PROTECTION LAW IN INDIA**

India has been working on a new data protection law for several years to provide comprehensive protection for personal data and to regulate the collection, storage, and use of such data. The proposed law, called the Personal Data Protection Bill, 2019, was introduced in the Indian Parliament in December 2019 and has been under discussion and review since then. Here are some key features of the proposed law:

a. Applicability: The law will apply to any person or entity that processes personal data in India or outside India, if such processing is related to the provision of goods or services to individuals in India.
b. Data protection obligations: The law requires data controllers to take reasonable steps to ensure that personal data is processed fairly, transparently, and securely. It also requires data processors to process personal data only for the purposes specified by the data controller and to implement appropriate security measures.
c. Rights of individuals: The law gives individuals the right to access, correct, and delete their personal data. It also gives them the right to restrict or object to the processing of their data and to receive a copy of their personal data in a structured, machine-readable format.
d. Sensitive personal data: The law recognizes certain categories of sensitive personal data, such as health data, financial data, and biometric data, and imposes stricter obligations on the processing of such data.
e. Data localization: The law requires certain categories of personal data to be stored only in India and imposes restrictions on the transfer of personal data outside India.
f. Enforcement and penalties: The law provides for the establishment of a Data Protection Authority to oversee compliance with the law and to impose penalties for non-compliance. The penalties for violations of the law can be up to 4% of an entity's global turnover.

The proposed Personal Data Protection Bill, 2019 is currently under review by a Parliamentary Committee, and its provisions are subject to change. However, if enacted, it will be a significant step towards protecting the privacy and personal data of Indian citizens and regulating the use of such data by businesses and other entities.

**VIII. CONCLUSION**

In conclusion, data protection and cyber laws are critical components of modern legal frameworks that seek to protect individuals, organizations, and critical infrastructure from the increasing threat of cyber-attacks and data breaches. These laws are designed to establish legal obligations for the collection, processing,

[19] (2017) 10 SCC 1

[20] Praveen Arimbrathodiyil v. Union of India, WP (C) No. 3125 of 2021, order dated 28-6-2021.

and storage of sensitive data, as well as to promote the adoption of best practices for cyber security.

The importance of data protection and cyber laws lies in their ability to establish legal precedents, set standards for compliance, and provide a basis for regulatory action. Through the examination of case laws and legal frameworks, organizations can gain a better understanding of the legal risks associated with data breaches and cyber-attacks and take steps to mitigate those risks through the implementation of appropriate security measures.

Ultimately, data protection and cyber laws are essential for maintaining the confidentiality, integrity, and availability of sensitive data and ensuring the safe and secure operation of digital systems and infrastructure. As the digital landscape continues to evolve and threats become increasingly sophisticated, it is crucial that organizations remain vigilant and continue to prioritize data protection and cyber security.

**REFERENCES**

a. https://blog.ipleaders.in/data-protection-laws-in-india-2/#Information_Technology_Act_2000
b. What about the Intermediary? Demystifying the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 | SCC Blog
c. https://www.analyticsinsight.net/data-protection-vs-cyber-security-why-you-need-both/
d. https://amtrustfinancial.com/blog/small-business/cybersecurity-vs-data-privacy
e. https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/
f. https://ssrana.in/articles/data-protection-privacy-cyber-security-india/#:~:text=a)%20Section%2043A%3A%20Section%2043A,wrongful%20gain%20to%20any%20person%2C
g. https://blog.ipleaders.in/data-protection-and-privacy-policies-in-cyber-law/
h. https://www.legalserviceindia.com/articles/Data_Safety.htm