Journal for Re Attach Therapy and Developmental Diversities
eISSN: 2589-7799
2024 February; 7 (2): 152-158

Legal Framework For Developing And Implementing Robust Cybersecurity Policies In India

Neerja Sharma[1*], Anuj Kumar[2]

[1*][LLM (Business Law) Amity University, Noida, LLB Delhi University]
[2][LLM (Business Law) Amity University, Noida, LLB Delhi University]

Introduction

In recent years, India has witnessed a significant increase in cyber threats, highlighting the importance of robust cybersecurity policies for organizations. A strong legal framework is essential to ensure that organizations comply with cybersecurity requirements and protect sensitive information. This paper provides the legal framework for developing and implementing robust cybersecurity policies in India. With the increasing prevalence of cyber threats, organizations need to adhere to specific laws and regulations to protect sensitive information. The Information Technology Act, 2000, along with rules and policies such as the SPDI Rules and the National Cyber Security Policy, 2013, form the foundation for cybersecurity compliance in India. This article outlines key legal provisions and highlights the importance of cybersecurity measures to mitigate risks and ensure data protection.

Cyber security Laws and Regulations and obligation on businesses and organizations and Penalties
The Information Technology Act, 2000 (IT Act) is the primary legislation in India that addresses cybersecurity. The IT Act provides legal recognition for electronic records and establishes guidelines for the security of electronic data and information systems. Section 43A of the IT Act requires organizations to implement reasonable security practices and procedures to protect sensitive personal data from unauthorized access, disclosure, or destruction. Failure to comply with these requirements can result in penalties. This legislation provides a legal framework for regulating electronic commerce, digital signatures, cybersecurity, and data protection in India. It imposes obligations on businesses and organizations to maintain reasonable security practices and procedures to safeguard electronic records and secure digital transactions. Additionally, this Act outlines provisions for reporting cyber incidents and breaches to the Indian Computer Emergency Response Team (CERT-In) for investigation and remediation. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (hereinafter referred as SPDI rules). It provides detailed requirements for the protection of sensitive personal data. The rules specify the measures that organizations must take to secure sensitive personal information, such as passwords, financial information, and biometric data. mandates that businesses and organizations handling sensitive personal data or information implement reasonable security practices and procedures to protect such data from unauthorized access, disclosure, or misuse. It specifies requirements for the collection, storage, processing, and transfer of sensitive personal data or information, including the appointment of a grievance officer to address data protection concerns. Under the SPDI Rules, organizations are required to obtain consent from individuals before collecting or using their sensitive personal data. Organizations must also implement reasonable security practices and procedures to protect this information from unauthorized access, use, or disclosure.

Section 66 of the IT Act, 2000, addresses **hacking** offences. It provides that unauthorized access to a computer system or network with the intent to cause wrongful loss or damage to the data or property is punishable with imprisonment up to three years or a fine extending to five lakh rupees or both.Additionally, if hacking is done to obtain unauthorized access to any information contained in the computer system or to cause disruption of services, the offender may face enhanced penalties under Section 66B, which include imprisonment up to ten years and a fine. **Identity theft** is covered under Section 66C of the IT Act, 2000. It pertains to the dishonest or fraudulent use of another person's electronic identity to commit an offense, resulting in wrongful gain or causing harm to the person whose identity is stolen. The punishment for identity theft includes imprisonment up to three years and a fine. Furthermore, Section 66D of the IT Act addresses cheating by personation through the use of computer resources. Offenders engaging in impersonation for financial gain or causing harm to others can face imprisonment up to three years and a fine. In *Shreya Singhal Vs UOI AIR 2015 SC 1523* validity of Section 66A of the IT Act which provides that As per Section 66A of the IT Act 2000, if offensive messages are sent through communication devices and computers, then it will be considered to be a crime. If the messages are grossly offensive, mislead or deceive the recipient, then it is punishable under the law which was challenged before the Hon'ble Supreme Court of India wherein the Hon'ble apex court held that section 66A is ambiguous, and is violative of the right to freedom of speech and it takes within its range the speech that is innocent as well. It removed an arbitrary provision from IT Act, 2000 and upheld citizens' fundamental right to free speech in India. It was of the view that even though section 66A is struck down, provisions in the Indian Penal Code, 1860 will continue to be applicable prohibiting racist speech, any speech that outrages the modesty of a woman or speech aimed at promoting enmity, abusive language, criminal intimidation, racism, etc.

In *Shamsher Singh Verma Vs State of Haryana 2015 SCC OnLine SC 1242* the issue decided by the court was whether Compact Disc requires a personal admission or denial from the complainant or witness regarding a document under Section 294 (1) of the CrPC? Here the Hon'ble Supreme Court of India held that Compact Disc is likewise a document and is admissible, and that the accused, complainant, or witness does not need to personally admit or deny a document under Section 294 (1) of the CrPC.

Unauthorized access to computer systems, networks, or data is punishable under Section 43 of the IT Act, 2000. The section prescribes penalties for unauthorized access, unauthorized downloading, introduction of computer viruses, and damage to computer systems or data. Depending on the specific offense committed, penalties may include compensation for damages and monetary fines. In cases where unauthorized access leads to wrongful gain or loss, and the damage exceeds one crore rupees, the offender may face enhanced penalties under Section 66C, which include imprisonment up to three years and a fine.

The Indian Penal Code, 1860 (IPC) contains provisions that address cybercrimes, such as hacking, identity theft, and data breaches. Sections 43, 66, and 66B of the IPC impose penalties for unauthorized access to computer systems, data theft, and the misuse of electronic signatures, respectively. The Indian Penal Code, 1860 (IPC) is replacing The Bharatiya Nyaya Sanhita Bill, 2023 with effect from 1st July, 2024 which also has penalties under section 109, 334, 335, 337, 338, 340 pertaining to misuse of electronic signatures, cyber-crime and forgery. Certain provisions of the Indian Penal Code address cybercrimes and impose legal obligations on businesses and organizations to prevent and report such offenses. For instance, Section 43A of the Information Technology (Amendment) Act, 2008, imposes penalties on companies that fail to implement adequate security measures to protect sensitive personal data and cause wrongful loss or gain to individuals. In *CBI Vs Arif Azim (Sony Sambandh case)*. The complaint was lodged with CBI and a case under Section 419, 418, and 420 of IPC,1860 was registered. An investigation was held, and it was concluded that Arif Azim while working at the Noida Call Centre, got access to the credit card details of Barbara Campa which he misappropriated. The issue was whether IPC, 1860 can be reliable and effective legislation to rely on when the IT Act is not exhaustive? The court held Respondent guilty, but because he was a young boy and a first-time offender, the court was lenient. The convicted person was given a one-year probationary period. The Indian Penal Code, 1860, was cited by the court as an effective piece of legislation to depend on when the IT Act was not sufficient.

The National Cyber Security Policy, 2013 (hereinafter referred as NCSP) sets out the government's vision for cybersecurity in India and outlines strategies for enhancing cybersecurity capabilities. The NCSP emphasizes the importance of public-private partnerships in addressing cybersecurity challenges and encourages organizations to adopt best practices for cybersecurity. It was formulated by the Ministry of Electronics and Information Technology (MeitY), the National Cyber Security Policy outlines the strategic vision and objectives for enhancing cybersecurity capabilities across various sectors in India. It emphasizes the importance of collaboration between government, industry, academia, and other stakeholders to strengthen cyber resilience, promote cybersecurity awareness, and foster innovation in cybersecurity technologies and practices.

The Privacy Rules under the Information Technology Act, 2000 govern the collection, use, and disclosure of personal information by organizations. The rules require organizations to obtain consent from individuals before collecting their personal information and to implement security measures to protect this information from unauthorized access or disclosure.

The Personal Data Protection Bill, 2019 (PDP Bill): Although not yet enacted into law at the time of writing, the PDP Bill represents a significant legislative initiative aimed at regulating the processing and protection of personal data in India. Once enacted, it is expected to establish comprehensive data protection obligations for entities handling personal data, including provisions related to data localization, cross-border data transfers, and the establishment of a Data Protection Authority.

Payment Card Industry Data Security Standard (PCI DSS) which is not a law or regulation per se, PCI DSS sets forth security standards and requirements for organizations handling payment card data to prevent data breaches and protect cardholder information. Compliance with PCI DSS is often mandated by regulatory authorities and card networks to ensure the security of electronic payment transactions and mitigate the risk of fraud. The RBI issues guidelines and directives for banks, financial institutions, and payment service providers to enhance cybersecurity resilience and mitigate cyber threats. These guidelines include requirements for implementing robust security controls, conducting regular cybersecurity audits and assessments, and reporting cybersecurity incidents and breaches to the RBI and other relevant authorities.

Certain sectors, such as the banking, financial services, and telecommunications industries, are subject to data localization requirements mandating the storage and processing of sensitive personal data within the geographical boundaries of India. Compliance with these requirements entails implementing adequate security measures to protect data stored locally and reporting any breaches or incidents affecting the confidentiality or integrity of such data.

In addition to overarching cybersecurity laws and policies, various sectoral regulations and guidelines prescribe specific cybersecurity requirements for industries such as banking, healthcare, telecommunications, and critical infrastructure. For instance, the Reserve Bank of India (RBI) issues cybersecurity guidelines for banks and financial institutions, while the

Ministry of Health and Family Welfare establishes standards for protecting health data and ensuring the security of healthcare information systems.
In India, cybersecurity oversight and enforcement are entrusted to several governmental bodies and authorities tasked with formulating policies, regulating compliance, investigating cyber incidents, and enforcing cybersecurity laws and regulations. These entities play pivotal roles in safeguarding digital infrastructure, protecting sensitive information, and combating cyber threats. Key governmental bodies responsible for cybersecurity oversight and enforcement in India include:

Government Bodies responsible for enforcement of cyber security oversight.
Ministry of Electronics and Information Technology (MeitY) is the primary government agency responsible for formulating policies and programs related to information technology, MeitY plays a central role in coordinating cybersecurity initiatives at the national level. It oversees the implementation of the National Cyber Security Policy, provides strategic direction for cybersecurity capacity-building efforts, and collaborates with other stakeholders to enhance cyber resilience across various sectors.

Indian Computer Emergency Response Team (CERT-In) is established under the provisions of the Information Technology (Amendment) Act, 2008, CERT-In serves as the national nodal agency for responding to cybersecurity incidents and coordinating emergency response efforts. It operates under the aegis of MeitY and is responsible for analyzing cyber threats, disseminating threat intelligence, issuing advisories, and assisting organizations in mitigating cyber risks. CERT-In also collaborates with international CERTs and law enforcement agencies to address cross-border cyber threats and cybercrime.

National Critical Information Infrastructure Protection Centre (NCIIPC) is entrusted with safeguarding critical information infrastructure (CII) in sectors deemed vital for national security and public welfare, such as energy, transportation, telecommunications, and finance. It operates under the aegis of the National Technical Research Organization (NTRO) and works closely with sector-specific regulators and stakeholders to enhance the resilience of critical infrastructure against cyber threats and attacks.
Various **law enforcement agencies**, including the Cyber Crime Cells of state police departments and the Cyber Crime Investigation Cells of central agencies such as the Central Bureau of Investigation (CBI) and the National Investigation Agency (NIA), are responsible for investigating cybercrimes, prosecuting offenders, and enforcing cybersecurity laws. These agencies collaborate with CERT-In and other stakeholders to combat cyber threats, conduct digital forensics, and ensure the effective enforcement of cybersecurity regulations.

Regulatory authorities overseeing specific sectors, such as the Reserve Bank of India (RBI) for banking and financial services, the Telecom Regulatory Authority of India (TRAI) for telecommunications, and the Securities and Exchange Board of India (SEBI) for capital markets, have a role in enforcing cybersecurity regulations and guidelines tailored to their respective industries. They prescribe cybersecurity requirements, conduct audits, and impose penalties for non-compliance to ensure the security and resilience of sectoral infrastructure and operations.

Categorization of Cyber crimes in India
In India, cyber threats and cybercrimes are formally defined and categorized based on their nature, impact, and intent. Cyber threats refer to malicious activities or events that aim to compromise the confidentiality, integrity, or availability of digital information or systems. These threats encompass a wide array of techniques and tactics employed by malicious actors to exploit vulnerabilities in computer systems, networks, and electronic devices. Cybercrimes, represent unlawful acts committed using digital technologies or targeting digital assets. These crimes encompass a broad spectrum of illegal activities ranging from financial fraud and identity theft to hacking, cyberstalking, and online harassment. Cybercrimes often inflict significant harm on individuals, organizations, and society as a whole, leading to financial losses, reputational damage, and breaches of privacy.

In India, cyber threats and cybercrimes are categorized into various types based on their characteristics and impact. These categories may include, but are not limited to:

Malware: Malicious software designed to disrupt, damage, or gain unauthorized access to computer systems or data, including viruses, worms, Trojans, and ransomware.
Phishing: Deceptive techniques used to trick individuals into divulging sensitive information such as passwords, credit card numbers, or personal identification details through fraudulent emails, websites, or messages.
Denial of Service (DoS) Attacks: Coordinated efforts to overwhelm a target system or network with a flood of illegitimate traffic, rendering it inaccessible to legitimate users.

Data Breaches: Unauthorized access or disclosure of confidential or sensitive information, including personal data, trade secrets, or financial records, often resulting in identity theft, fraud, or extortion.
Cyber Espionage: Covert activities aimed at infiltrating and stealing sensitive information from government agencies, businesses, or other organizations for intelligence or competitive advantage.
Cyberbullying: Online harassment, intimidation, or abuse targeting individuals or groups through social media platforms, messaging apps, or other digital channels.
Identity Theft: Unauthorized use of someone else's personal information to impersonate them or commit fraudulent activities, such as opening bank accounts, applying for loans, or making purchases.
Online Fraud: Deceptive schemes or scams conducted over the internet to deceive individuals or organizations into transferring money or valuable assets under false pretenses.

Implementation of Measures and Strategies for enhancing critical Infrastructure sectors against cyber attacks
National Cyber Security Policy (NCSP) formulated in the year 2013, provides a comprehensive framework for addressing cybersecurity challenges across critical sectors, including energy, transportation, telecommunications, banking, and healthcare. The policy emphasizes the importance of establishing a robust cybersecurity ecosystem, fostering public-private partnerships, and promoting cybersecurity awareness and capacity-building initiatives.

The Government of India recognizes certain sectors as **critical information infrastructure (CII)** and implements specialized measures to safeguard them from cyber threats. These sectors encompass essential services such as power generation and distribution, transportation networks, telecommunications systems, and financial services. CIIP initiatives include risk assessments, vulnerability assessments, incident response planning, and the development of sector-specific cybersecurity guidelines and standards.

National Critical Information Infrastructure Protection Centre (NCIIPC) acts as the nodal agency responsible for protecting critical information infrastructure from cyber threats and coordinating cybersecurity efforts across designated critical sectors. It conducts threat assessments, vulnerability assessments, and cybersecurity audits to identify and mitigate risks to critical infrastructure assets. NCIIPC also facilitates information sharing, cybersecurity incident response, and capacity-building initiatives to strengthen the resilience of critical infrastructure against evolving cyber threats.

Sectoral Computer Emergency Response Teams (CERTs) are established to address cybersecurity challenges and incidents within critical infrastructure sectors. These CERTs collaborate with NCIIPC, regulatory authorities, industry associations, and other stakeholders to monitor cyber threats, disseminate threat intelligence, and coordinate incident response activities. Sectoral CERTs play a vital role in enhancing situational awareness, facilitating information sharing, and promoting cybersecurity best practices among critical infrastructure operators.

Regulatory Compliance and Standards of Regulatory authorities such as the Reserve Bank of India (RBI), Telecom Regulatory Authority of India (TRAI), and Central Electricity Regulatory Commission (CERC) impose cybersecurity requirements and standards on critical infrastructure operators to ensure compliance and resilience against cyber threats. These regulations mandate the implementation of robust security controls, incident response mechanisms, and cybersecurity audits to protect critical infrastructure assets and services from cyber attacks.

India engages in **International Cooperation And Collaboration** initiatives to address cross-border cyber threats and enhance the cybersecurity resilience of critical infrastructure. Bilateral and multilateral partnerships, information sharing agreements, and participation in international cybersecurity forums contribute to the exchange of best practices, threat intelligence, and capacity-building efforts to safeguard critical infrastructure at the global level.

Facilitation of International Cooperation for Cyber security and cyber crime
Several key strategies and mechanisms employed to facilitate international cooperation in cybersecurity and cybercrime in India include:
Bilateral and Multilateral Agreements:
India enters into bilateral and multilateral agreements, treaties, and memoranda of understanding (MoUs) with other countries to enhance cooperation in combating cybercrime, exchanging cyber threat intelligence, and facilitating mutual legal assistance in cybercrime investigations and prosecutions. These agreements establish frameworks for cooperation, information sharing, capacity building, and joint action to address common cybersecurity challenges and protect national interests.

Participation in International Forums and Organizations
India actively participates in international forums, organizations, and initiatives dedicated to cybersecurity, such as the United Nations (UN), International Telecommunication Union (ITU), Interpol, and the Global Forum on Cyber Expertise

(GFCE). Engagement in these forums enables India to contribute to global cybersecurity discourse, share best practices, promote capacity building, and strengthen international cooperation frameworks for addressing cyber threats and challenges.

Law Enforcement Collaboration
India collaborates with foreign law enforcement agencies, including the Federal Bureau of Investigation (FBI), the United States Secret Service (USSS), and the European Cybercrime Centre (EC3), to investigate and combat transnational cybercrimes, cyberattacks, and cyber-enabled crimes. Joint investigation teams, information sharing mechanisms, and operational partnerships facilitate coordinated responses to cyber threats and enhance law enforcement capabilities in detecting, disrupting, and prosecuting cybercriminal activities across borders.

Information Sharing and Threat Intelligence Exchange
India engages in information sharing and threat intelligence exchange initiatives with international partners, cybersecurity agencies, and industry stakeholders to enhance situational awareness, early warning capabilities, and response readiness to cyber threats. Participation in global cybersecurity information-sharing platforms, such as the Cyber Threat Alliance (CTA) and Information Sharing and Analysis Centers (ISACs), enables India to access timely and actionable cyber threat intelligence and collaborate with international peers in addressing emerging cyber threats and vulnerabilities.

Capacity Building and Technical Assistance
India provides technical assistance, capacity-building support, and training programs to partner countries, particularly in the developing world, to strengthen their cybersecurity capabilities, regulatory frameworks, and institutional capacities. Bilateral technical cooperation initiatives, workshops, and training courses organized by Indian cybersecurity agencies, such as the Indian Computer Emergency Response Team (CERT-In), enable partner countries to enhance their cyber resilience, develop cybersecurity expertise, and effectively respond to cyber threats and incidents.

Cyber Diplomacy and Policy Engagement
India conducts cyber diplomacy initiatives and policy dialogues with foreign governments, diplomatic missions, and international organizations to advance shared cybersecurity interests, promote norms of responsible state behavior in cyberspace, and shape international cyber policy agendas. Diplomatic engagements facilitate consensus-building, norm development, and confidence-building measures to strengthen international cooperation frameworks and promote a rules-based approach to cybersecurity governance at the global level.

Sources to improve cyber security policies
In India, numerous resources and platforms are available for organizations and individuals to enhance cybersecurity practices, acquire knowledge, skills, and capabilities, and stay updated on emerging threats, best practices, and regulatory requirements. These resources and platforms serve as valuable sources of information, training, guidance, and collaboration opportunities, empowering stakeholders to strengthen their cybersecurity posture, mitigate risks, and foster a culture of cyber resilience. Some of the key resources and platforms available for improving cybersecurity practices in India include:

Government Initiatives and Agencies:
Indian Computer Emergency Response Team (CERT-In) which is under the Ministry of Electronics and Information Technology (MeitY), serves as the national nodal agency for cybersecurity incident response, coordination, and capacity building. CERT-In offers cybersecurity advisories, guidelines, and training programs for organizations and individuals to enhance their cybersecurity awareness and readiness.

National Cyber Coordination Centre (NCCC) is operated by the Indian government, facilitates real-time monitoring, analysis, and response to cyber threats and incidents across the country. NCCC provides threat intelligence, situational awareness, and coordination support to government agencies, critical infrastructure sectors, and law enforcement authorities.

Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) is further operated by CERT-In, the Cyber Swachhta Kendra offers free security tools, malware detection and removal utilities, and cybersecurity awareness resources for individuals and organizations to protect their devices and networks from malware infections and cyber threats.

Sector-Specific Information Sharing and Analysis Centers (ISACs) such as the Financial Sector Computer Emergency Response Team (FINCERT), Healthcare Information Sharing and Analysis Center (H-ISAC), and Telecom Security Assurance Center (TSAC), facilitate information sharing, threat intelligence collaboration, and capacity building within

critical sectors. ISACs provide sector-specific cybersecurity advisories, training programs, and incident response coordination services to strengthen sectoral resilience against cyber threats.

Industry Associations and Forums include the National Association of Software and Service Companies (NASSCOM), Data Security Council of India (DSCI), and Internet and Mobile Association of India (IAMAI), organize cybersecurity conferences, seminars, workshops, and training programs to promote cybersecurity awareness, knowledge sharing, and best practices adoption among industry stakeholders.

Training and Certification Programs provided by various educational institutions, and cybersecurity training providers offer certification programs, workshops, and courses on cybersecurity topics, such as ethical hacking, digital forensics, incident response, and security management. Training programs accredited by international bodies, such as EC-Council, CompTIA, and (ISC)², provide globally recognized certifications and credentials for cybersecurity professionals.

Online Resources and Portals
Online platforms and portals, such as the National Cyber Security Portal (https://www.cybersecurity.gov.in), provide access to cybersecurity resources, tools, guidelines, and best practices curated by government agencies, industry experts, and cybersecurity organizations. These portals offer cybersecurity awareness materials, self-assessment tools, and interactive resources to help individuals and organizations improve their cybersecurity posture.

Cybersecurity Awareness Campaigns
Cybersecurity awareness campaigns, such as Cyber Surakshit Bharat, Secure India, and Cyber Swachhata Kendra, are launched by government agencies, industry associations, and cybersecurity organizations to raise awareness about cyber threats, promote best practices, and educate citizens about safe online behavior. These campaigns leverage social media, educational materials, and outreach activities to reach diverse audiences and empower them to protect themselves against cyber threats.

Conclusion

In the contemporary cybersecurity landscape in India, several prominent challenges and emerging trends are shaping the dynamics of cyber risk, threat landscape, and cybersecurity readiness. These challenges and trends reflect the evolving nature of cyber threats, technological advancements, regulatory developments, and socio-economic factors influencing cybersecurity practices and resilience in India. Cyber threats continue to evolve in sophistication, scale, and complexity, posing significant challenges to organizations, government agencies, and individuals in India. Advanced persistent threats (APTs), ransomware attacks, supply chain vulnerabilities, and nation-state-sponsored cyber operations target critical infrastructure, government systems, financial institutions, and high-value assets, highlighting the need for proactive defense measures and threat intelligence capabilities. The shortage of skilled cybersecurity professionals, cybersecurity expertise, and specialized technical skills hinders organizations' ability to address cyber threats, implement effective security controls, and respond to incidents. Regulatory compliance requirements, data protection regulations, and privacy laws, such as the Personal Data Protection Bill, 2019, and the General Data Protection Regulation (GDPR), impose obligations on organizations to safeguard personal data, uphold privacy rights, and ensure compliance with data protection principles. Achieving regulatory compliance, implementing privacy-enhancing measures, and addressing cross-border data transfer requirements present compliance challenges and operational complexities for organizations operating in India's digital ecosystem. Moreover, emerging trends such as digital transformation, AI-driven technologies, and quantum computing introduce new opportunities for innovation, economic growth, and societal advancement, while also posing novel security risks and vulnerabilities that require careful consideration and proactive risk management strategies. As India continues its journey towards a secure and resilient digital future, it must remain vigilant, adaptive, and proactive in addressing evolving cyber threats, safeguarding critical infrastructure, and protecting the interests of its citizens, businesses, and institutions in cyberspace. By embracing the principles of cybersecurity by design, promoting a culture of cyber hygiene, and fostering collaboration and information sharing, India can effectively navigate the complexities of the cybersecurity landscape and emerge as a global leader in cybersecurity innovation, excellence, and governance.

In conclusion, India has a robust legal framework for developing and implementing cybersecurity policies. Organizations must comply with the provisions of the IT Act, SPDI Rules, IPC, NCSP, and Privacy Rules to protect sensitive information and mitigate cyber risks. By adopting best practices and staying updated with legal requirements, organizations can enhance their cybersecurity posture and safeguard against cyber threats.

References

1. The Information Technology Act, 2000
2. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
3. The National Cyber Security Policy, 2013
4. The Personal Data Protection Bill, 2019 (once enacted)
5. The Payment Card Industry Data Security Standard (PCI DSS)
6. Relevant sections of the Indian Penal Code, 1860
7. Shamsher Singh Verma Vs State of Haryana 2015 SCC OnLine SC 1242
8. Shreya Singhal Vs UOI AIR 2015 SC 1523
9. Bharatiya Nyaya Sanhita Bill, 2023