Cyber law in india pdf

I'm not robot!

Cyber law in india in hindi. Cyber law in india book pdf. Cyber law in india malayalam. Cyber law in india pdf in hindi. Cyber law in india ppt. Cyber law in india wikipedia. Cyber law in india pdf. Cyber law in india it act 2000.

· Cyber Lawyers · Computer Forensics · How Cyber Crime Works · Popular Cyber Law Cases · Cyber Law in India · Cyber Laws Advantage · Two Sides of Cyber Laws · System Requirements · Computer Crime · Computer Insecurity · White Hat Hackers · Grey Hat Hackers · Black Hat Hackers · Internet Crime · Internet Fraud IT Act 2000 · · IT Act 2000 IT Amendment Bill 2006 · View More Downloads · Contact Us Useful Links For more information on a Chicago criminal defense attorney, click here. Commercial Litigation Law and Legal Help Cyber Laws in India, Cases, Internet Crime, Information Technology Act 2006, Lawyers in Jaipur and Rajasthan, High Court, Supreme Courts, Cyber crime, Criminals, Amendment 2006, Legal Consultants, Consultancy, Advocates, Website Laws, Data, Security, Legal Services Cy IT Act, · Cyber Laws in India, Cases, Internet Crime, Arbitration, Legal Services Outsourcing, Cyber crime, Criminals, Terrorism, IT act, Hacking, Contact Mr.Vivek Tripathi. .... Cyberlaw in India is not a separate legal framework. Its a combination of Contract, Intellectual property, Data protection, and privacy laws. With the Computer and internet taking over every aspect of our life, there was a need for strong cyber law. Cyber laws supervise the digital circulation of information, software, information security, e-commerce, and monetary transactions. The Information Technology Act, 2000 addresses the gamut of new-age crimes. Computer technology, mobile devices, software, and the internet are both medium and target of such crimes. All Traditional criminal activities are such as theft, fraud, forgery, defamation, and mischief are part of cyberspace. These were addressed in the Indian Penal Code already. Table of Content: Importance of Cyber Law in India Types of Cyber Crimes Evolution of Cyber Law in India The Need for Cyber Laws What is the Information Technology Act, 2000? How to Prevent Cyber Crime? Frequently Asked Questions Strong cyber Law was needed to address: Importance of Cyber Law in India Cyber laws in India or cybercrime law in India are important because of the prime reason that cybercrime act in India encompasses and covers all the aspects which occur on or with the internet - transactions, and activities which concern the internet and cyberspace. "The Cyber Laws in India has paved the way for electronic commerce and electronic governance in the country by ensuring maximum connectivity and minimum cybersecurity risks. Also, enhancing the scope and expanding the use of digital mediums," says Advocate Krishnamohan K Menon. Types of Cyber Crimes Different types of cybercrimes have different punishments in India. Evolution of Cyber Law in India With an increase in the dependency on the use of technology, the need for cyberlaw was necessary. Much like every coin has two sides, therefore, the dependency on technology has its pros and cons. The rise of the 21st century marked the evolution of cyberlaw in India with the Information Technology Act, 2000 (popularly known as the IT Act). The first-ever cybercrime was recorded in the year 1820[pdf]. The objective of the Information Technology Act in India is as follows: The Indian IT law updated the Reserve Bank of India Act and the Indian Evidence Act. With the evolution of cyberlaw, almost all online activities came under scrutiny. However, one thing about cyber law is that there are certain areas on which cybercrime laws in India do not apply such as: The Need for Cyber Laws In the present world which is more tech-savvy, the words cyber law and cyber crimes have also become more sophisticated. Internet and technology were launched for research purposes and making the lives of humans easy but as the use and number of people on the internet increased, the need for cyber laws in India was felt. As the nature of the internet is anonymous it is easy to commit cybercrimes. Thereby many could misuse this aspect largely. Advocate Tanuj Aggarwal says, "With the exponential growth in the digital space, the establishment of certain reforms was highly needed for the security of the citizen’s privacy and data protection." What is the Information Technology Act, 2000? When the emphasis was on the need for cyber law or cybersecurity laws, then, it was imperative to implement an IT law in India. Thus, the Information Technology Act, 2000[1], or also known as the Indian Cyber Act or the Internet Law came to force in India. Since the enactment, the Indian Internet Laws were drafted to bring in view all the electronic records and online/electronic activities to legal recognition. The IT Act also addresses the important issues of security, which are critical to the success of electronic transactions. The Internet Laws in India not only validates digital signatures but also provides for how authentication of the documents, which has been accepted and generated by using the digital signatures, can be done. As IT Act is a cybersecurity law introduced to secure cyberspace, the Information Technology Law was amended under; The prime focus of cyber law in India is to prevent: IT Act, 2000 went through amendments[2]in the year 2008. These were made in light of the laws on cybercrime - IT Act, 2000 by way of the IT Act, 2008. They were enforced at the beginning of 2009 to strengthen the cybersecurity laws. Modifications in the Information Technology Act, 2008 included the change in the definition of some terms such as communication devices. The amendment for the definition of communication device was to include: How to Prevent Cyber Crime? No doubt that the cybersecurity laws or cyber laws in India provide protection from cybercrime. However, prevention is always better than cure. Therefore, one should take the following steps for preventing a cybercrime: Frequently Asked Questions: What is Intellectual Property and how it is protected? Intellectual Property is the set of intangibles that you thought of, like logos, designs, symbols, taglines, books, slogans, product names, literature or businesses, and is legally protected by you or your company against outside use without permission. There are several cyber laws for the ownership and the right distribution of the Intellectual Property like Copyright, Patents, Trademarks or Service Marks, Trade Secrets, Domain Disputes, Contracts, Privacy, Employment, Defamation, Data Retention, and Jurisdiction. What are the advantages of Cyber Laws? Secured E-Commerce Infrastructure for online businesses. Digitally sign your contracts/ papers Introduced new businesses for Certifying Authorities Proficient use of E-Forms as prescribed Secured websites with Digital Certificates Meticulous monitoring on the web traffics Electronic Transactions safeguarded Emails are a legal form of communication and are approved in the court of law. How can MyAdvo help? MyAdvo acts as a client's legal concierge providing technology solutions for Lawyer Discovery, Price Discovery, and instant Case updates. With the use of technological solutions, we match the client’s requirements with cyber lawyers in India. Who informs you of the punishments applicable in accordance with the laws for cyber crime complaint online in India. MyAdvo metrics are based on expertise, experience, location, fees, etc. Over time, we have acquired a dedicated professional team that strives to do everything to help the client. From taking better-informed decisions by understanding his legal situation and requirement. Get legal advice from the best legal experts by emailing us at consult@myadvo.in or call us at +91-9811782573. External Links: [PDF] Read about the first-ever cybercrime recorded in the year 1820. [1] Information Technology ACT, 2002 - It is the law that deals with cybercrime and electronic commerce in India. [2] Information Technology ACT, 2008 - The main Indian act that addresses legal challenges specifically as they relate to the Internet is the Information Technology (Amendment) Act, 2008 This article has been written by Nikunj Arora of Amity Law School, Noida. This article provides a detailed overview of cyber crime and the related laws in India, along with the types of cyber crimes and the importance of cyber law. The article also gives a brief overview of cybersecurity. It has been published by Rachit Garg. Introduction According to a general cyber law definition, Cyber law is a legal system that deals with the internet, computer systems, cyberspace, and all matters related to cyberspace or information technology. Cyberspace law covers a wide range of topics including aspects of contract law, privacy laws, and intellectual property laws. It directs the electronic circulation of software, information, and data security as well as electronic commerce. E-documents are given legal recognition under cyber law. Moreover, the system provides a structure for electronic commerce transactions and electronic filing of forms. To put it simply, it is a law that deals with cyber crimes. As e-commerce has increased in popularity, it has become important to ensure there are proper regulations in place to prevent malpractices. There are many different laws governing cybersecurity, largely depending on each country’s territorial extent. The punishments for the same also vary according to the offence committed, ranging from fines to imprisonment. The Computer Fraud and Abuse Act of 1986 was the first cyber law that was ever to be enacted. It prohibits unauthorized access to computers and the illegal use of digital information. Internet usage has increased, and so has cyber crimes. There are several stories of cyber crimes in the media today ranging from identity theft, cryptojacking, child pornography, cyber terrorism etc. In cyber crimes, the computer is used either as a tool or a target, or both, in order to commit unlawful conduct. In our fast-moving digital age, there has been a phenomenal surge in electronic commerce (e-commerce) and online stock trading, leading to more cyber crimes. Overview of cyber crimes and cyber law Any criminal activity that involves a computer, networked device, or any other related device can be considered a cyber crime. There are some instances when cyber crimes are carried out with the intention of generating profit for the cybercriminals, whereas other times a cyber crime is carried out directly to damage or disable the computer or device. It is also possible that others use computers or networks to spread malware, illegal information, images, or any other kind of material. As a result of cyber crime, many types of profit-driven criminal activities can be perpetrated, such as ransomware attacks, email and internet fraud, identity theft, and frauds involving financial accounts, credit cards or any other payment card. The theft and resale of personal and corporate data could be the goal of cybercriminals. In India, cyber crimes are covered by the Information Technology Act, 2000 and the Indian Penal Code, 1860. It is the Information Technology Act, 2000, which deals with issues related to cyber crimes and electronic commerce. However, in the year 2008, the Act was amended and outlined the definition and punishment of cyber crime. Several amendments to the Indian Penal Code 1860 and the Reserve Bank of India Act were also made. Types of cyber crimes The following are considered to be types of cyber-crimes: Child pornography or child sexually abusive material (CSAM): In its simplest sense, child sexual abuse materials (CSAMs) include any material containing sexual images in any form, wherein both the child being exploited or abused may be seen. There is a provision in Section 67(B) of the Information Technology Act which states that the publication or transmission of material depicting children in sexually explicit acts in an electronic form is punishable. Cyberbullying: A cyberbully is someone who harasses or bullies others using electronic devices like computers, mobile phones, laptops, etc. Cyberbullying refers to bullying conducted through the use of digital technology. The use of social media, messaging platforms, gaming platforms, and mobile devices may be involved. Oftentimes, this involves repeated behaviour that is intended to scare, anger, or shame those being targeted. Cyberstalking: Cyberstalking is the act of harassing or stalking another person online using the internet and other technologies. Cyberstalking is done through texts, emails, social media posts, and other forms and is often persistent, methodical, and deliberate. Cyber grooming: The phenomenon of cyber grooming involves a person building a relationship with a teenager and having a strategy of luring, teasing, or even putting pressure on them to perform a sexual act. Online job fraud: An online job fraud scheme involves misleading people who require a job by promising them a better job with higher wages while giving them false hope. On March 21, 2022, the Reserve Bank of India (RBI) alerted people not to fall prey to job scams. By this, the RBI has explained the way in which online job fraud is perpetrated, as well as precautions the common man should take when applying for any job opportunity, whether in India or abroad. Online sextortion: The act of online sextortion occurs when the cybercriminal threatens any individual to publish sensitive and private material on an electronic medium. These criminals threaten in order to get a sexual image, sexual favour, or money from such individuals. Phishing: Fraud involving phishing is when an email appears to be from a legitimate source but contains a malicious attachment that is designed to steal personal information from the user such as their ID, IPIN, Card number, expiration date, CVV, etc. and then selling the information on the dark web. Vishing: In vishing, victims’ confidential information is stolen by using their phones. Cybercriminals use sophisticated social engineering tactics to get victims to divulge private information and access personal accounts. In the same way as phishing and smishing, vishing convincingly fools victims into thinking that they are being polite by responding to the call. Callers can often pretend that they are from the government, tax department, police department, or victim’s bank.. Smishing: As the name suggests, smishing is a fraud that uses text messages via mobile phones to trick its victims into calling a fake phone number, visiting a fraudulent website or downloading malicious software that resides on the victim’s computer. Credit card fraud or debit card fraud: In credit card (or debit card) fraud, unauthorized purchases or withdrawals from another’s card are made to gain access to their funds. When unauthorized purchases or withdrawals of cash are made from a customer’s account, they are considered credit/debit card fraud. Fraudulent activity occurs when a criminal gains access to the cardholder’s debit/credit number, or personal identification number (PIN). Your information can be obtained by unscrupulous employees or hackers. Impersonation and identity theft: A person is impersonated or exposed to identity theft when they make fraudulent use of an electronic signature, a password, or any other unique identifier on another person’s behalf. Prevention of cyber crimes As per the recommendations of the International Maritime Organization (IMO), the cyber-attack risk must be approached using the following framework: The first step is to define the roles and responsibilities of the personnel responsible for cyber risk management. The second step is to identify the systems, assets, data, or capabilities that will put the operation at stake if disrupted. To protect against a potential cyber event and to maintain continuity of operations, it is important to implement risk-control processes and contingency plans. It is also important to develop and implement measures to detect a cyber-attack as quickly as possible. Preparation and implementation of plans to restore critical systems for continued operations by providing resilience. Finally, identify and implement measures to be taken to backup and restore any affected systems. The following can be the strategies can be used to prevent cyber crime: Analyze your risk exposure: In order to adequately prepare for a cyber attack, you must assess the threat and give due consideration. Companies should consider the following: They should consider all areas where they are susceptible to cyberattacks and any operational vulnerabilities resulting from them. A vulnerability assessment of all systems is necessary to identify those that are critical to the business, to understand the potential exposures each has, and to assess the impact of any cyber-attack on business continuity. IT systems and operational technology systems should be checked by businesses. Preventive measures: It is recommended that businesses adopt national or international technical standards that provide a high level of protection. These general prevention measures are recommended for companies that currently lack the necessary technical or financial capabilities. The following is the list of preventive measures: Applying multiple layers of defence, beginning with physical security, followed by management policies and procedures, firewalls and network architecture, computer policies, account management, security updates and finally antivirus applications. Implementing a principle of least privilege, which restricts information and access to only those set of people who needs to know that particular information. Implementing network-hardening measures, assuring patch management is sufficient and is proactively reviewed. Securing critical systems by utilizing technology such as protocol-aware filtering and segregation. Ensuring that removable devices are encrypted and that any USB used with any other device is tested for viruses. Furthermore, in order to prevent the negative impact of a cyberattack from further escalating and restoring business operations, it is important to develop business continuity plans, identify key personnel, and implement processes. Additionally, organising frequent training and awareness sessions for all employees can also help.Compliance audits of third-party service providers will also be beneficial. In terms of cybersecurity, there are five main types of laws that must be followed. Cyber laws are becoming increasingly important in countries such as India which have extremely extensive internet use. There are strict laws that govern the use of cyberspace and supervise the use of information, software, electronic commerce, and financial transactions in the digital environment. India’s cyber laws have helped to enable electronic commerce and electronic governance to flourish in India by safeguarding maximum connectivity and minimizing security concerns. This has also made digital media accessible in a wider range of applications and enhanced its scope and effectiveness. Information Technology Act, 2000 (IT Act): Overview of the Act: It is the first cyberlaw to be approved by the Indian Parliament. The Act defines the following as its object: “to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as electronic methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker’s Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.” However, as cyber-attacks become dangerous, along with the tendency of humans to misunderstand technology, several amendments are being made to the legislation. It highlights the grievous penalties and sanctions that have been enacted by the Parliament of India as a means to protect the e-governance, e-banking, and e-commerce sectors. It is important to note that the IT Act’s scope has now been broadened to include all the latest communication devices. The Act states that an acceptance of a contract may be expressed electronically unless otherwise agreed and that the same shall have legal validity and be enforceable. In addition, the Act is intended to achieve its objectives of promoting and developing an environment conducive to the implementation of electronic commerce. The important provisions of the Act The IT Act is prominent in the entire Indian legal framework, as it directs the whole investigation process for governing cyber crimes. Following are the appropriate sections: Section 43: This section of the IT Act applies to individuals who indulge in cyber crimes such as damaging the computers of the victim, without taking the due permission of the victim. In such a situation, if a computer is damaged without the owner’s consent, the owner is fully entitled to a refund for the complete damage. In Poona Auto Ancillaries Pvt. Ltd., Pune v. Punjab National Bank, HO New Delhi & Others (2018), Rajesh Aggarwal of Maharashtra’s IT department (representative in the present case) ordered Punjab National Bank to pay Rs 45 lakh to Manmohan Singh Matharu, MD of Pune-based firm Poona Auto Ancillaries. In this case, a fraudster transferred Rs 80.10 lakh from Matharu’s account at PNB, Pune after the latter answered a phishing email. Since the complainant responded to the phishing mail, the complainant was asked to share the liability. However, the bank was found negligent because there were no security checks conducted against fraudulent accounts opened to defraud the Complainant. Section 66: Applies to any conduct described in Section 43 that is dishonest or fraudulent. There can be up to three years of imprisonment in such instances, or a fine of up to Rs. 5 lakh. In Kumar v. Whiteley (1991), during the course of the investigation, the accused gained unauthorized access to the Joint Academic Network (JANET) and deleted, added, and changed files. As a result of investigations, Kumar had been logging on to a BSNL broadband Internet connection as if he was an authorized legitimate user and modifying computer databases pertaining to broadband Internet user accounts of subscribers. On the basis of an anonymous complaint, the CBI registered a cyber crime case against Kumar and conducted investigations after finding unauthorized use of broadband Internet on Kumar’s computer. Kumar’s wrongful act also caused the subscribers to incur a loss of Rs 38,248. N G Arun Kumar was sentenced by the Additional Chief Metropolitan Magistrate. The magistrate ordered him to undergo a rigorous year of imprisonment with a fine of Rs 5,000 under Sections 420 of IPC and 66 of the IT Act. Section 66B: This section describes the penalties for fraudulently receiving stolen communication devices or computers, and confirms a possible three-year prison sentence. Depending on the severity, a fine of up to Rs. 1 lakh may also be imposed.Section 66C: The focus of this section is digital signatures, password hacking, and other forms of identity theft. Thi section imposes imprisonment upto 3 years along with one lakh rupees as a fine. Section 66D: This section involves cheating by personation using computer Resources. Punishment if found guilty can be imprisonment of up to three years and/or up-to Rs 1 lakh fine.Section 66E: Taking pictures of private areas, publishing or transmitting them without a person’s consent is punishable under this section. Penalties, if found guilty, can be imprisonment of up to three years and/or up-to Rs 2 lakh fine.Section 66F: Acts of cyber terrorism. An individual convicted of a crime can face imprisonment of up to life. An example: When a threat email was sent to the Bombay Stock Exchange and the National Stock Exchange, which challenged the security forces to prevent a terror attack planned on these institutions. The criminal was apprehended and charged under Section 66F of the IT Act.Section 67: This involves electronically publishing obscenities. If convicted, the prison term is up to five years and the fine is up to Rs 10 lakh. Positive and negative aspects of the IT Act This legislation contains the following benefits: Several companies are now able to conduct e-commerce without any fear because of the presence of this Act. Until recently, the development of electronic commerce in our country was hindered primarily due to a lack of legal infrastructure to govern commercial transactions online.Digital signatures are now able to be used by corporations to conduct online transactions. Digital signatures are officially recognized and sanctioned by the Act.Additionally, the Act also paves the way for corporate entities to also act as Certification Authorities for the issuance of Digital Signature Certificates under the Act. There are no distinctions in the Act as to what legal entity may be designated as a Certifying Authority, provided the government’s standards are followed.Furthermore, the Act permits the companies to electronically file any of their documents with any office, authority, body or agency owned or controlled by the appropriate government by using the electronic form prescribed by that government.It also provides information on the security concerns that are so crucial to the success of the use of electronic transactions. As part of the Act, the term secure digital signatures were defined and approved, which are required to have been submitted to a system of a security procedure. Therefore, it can be assumed that digital signatures are now secured and will play a huge part in the economy. Digital signatures can help conduct a secure online trade. It is common for companies to have their systems and information hacked. However, the IT Act changed the landscape completely. A statutory remedy is now being provided to corporate entities in the event that anyone breaches their computer systems or network and damages or copies data. Damages are charged to anyone who uses a computer, computer system or computer network without the permission of the owner or other person in charge. However, the said Act has a few problems: Section 66A is considered to be in accordance with Article 19(2) of the Constitution of India since it does not define the terms ‘offensive’ and ‘menacing’. It did not specify whether or not these terms involved defamation, public order, incitement or morality. As such, these terms are open to interpretation.Considering how vulnerable the internet is, the Act has not addressed issues such as privacy and content regulation, which are essential.A domain name is not included in the scope of the Act. The law does not include any definition of domain names, nor does it state what the rights and liabilities of domain name owners are. The Act doesn’t make any provision for the intellectual property rights of domain name proprietors. In the said law, important issues pertaining to copyright, trademark, and patent have not been addressed, therefore creating many loopholes. Indian Penal Code, 1860 (IPC): If the IT Act is not sufficient to cover specific cyber crimes, law enforcement agencies can apply the following IPC sections: Section 292: The purpose of this section was to address the sale of obscene materials, however, in this digital age, it has evolved to deal with various cyber crimes as well. A manner in which obscene material or sexually explicit acts or exploits of children are published or transmitted electronically is also governed by this provision. The penalty for such acts is imprisonment and fines up to 2 years and Rs. 2000, respectively. The punishment for any of the above crimes may be up to five years of imprisonment and a fine of up to Rs. 5000 for repeat (second-time) offenders.Section 354C: In this provision, cyber crime is defined as taking or publishing pictures of private parts or actions of a woman without her consent. In this section, voyeurism is discussed exclusively since it includes watching a woman’s sexual actions as a crime. In the absence of the essential elements of this section, Section 292 of the IPC and Section 66E of the IT Act are broad enough to include offences of an equivalent nature. Depending on the offence, first-time offenders can face up to 3 years in prison, and second-time offenders can serve up to 7 years in prison.Section 354D: Stalking, including physical and cyberstalking, is described and punished in this chapter. The tracking of a woman through electronic means, the internet, or email or the attempt to contact her despite her disinterest amounts to cyber-stalking. This offence is punished by imprisonment of up to 3 years for the first offence and up to 5 years for the second offence, along with a fine in both cases. A victim in the case Kalandi Charan Lenka v. the State of Odisha(2017) has received a series of obscene messages from an unknown number that has damaged her reputation. The accused also sent emails to the victim and created a fake account on Facebook containing morphed images of her. The High Court, therefore, found the accused prima facie guilty of cyberstalking on various charges under the IT Act and Section 354D of IPC. Section 379: The punishment involved under this section, for theft, can be up to three years in addition to the fine. The IPC Section comes into play in part because many cyber crimes involve hijacked electronic devices, stolen data, or stolen computers.Section 420: This section talks about cheating and dishonestly inducing delivery of property. Seven-year imprisonment in addition to a fine is imposed under this section on cybercriminals doing crimes like creating fake websites and cyber frauds. In this section of the IPC, crimes related to password theft for fraud or the creation of fraudulent websites are involved.Section 463: This section involves falsifying documents or records electronically. Spoofing emails is punishable by up to 7 years in prison and/or a fine under this section.Section 465: This provision typically deals with the punishment for forgery. Under this section, offences such as the spoofing of email and the preparation of false documents in cyberspace are dealt with and punished with imprisonment ranging up to two years, or both. In Anil Kumar Srivastava v. Addl Director, MHFW (2005), the petitioner had forged signed the signature of the AD and had then filed a case that made false allegations against the same individual. Due to the fact that the petitioner also attempted to pass it off as a genuine document, the Court held that the petitioner was liable under Sections 465 and 471 of the IPC. Section 468: Fraud committed with the intention of cheating may result in a seven-year prison sentence and a fine. This section also punishes email spoofing. Furthermore, there are many more sections of the IT Act and the Indian Penal Code, which pertain to cyber crimes, in addition to the laws listed above. Even though there are laws against cyber crime in place, the rate of cyber crime is still rising drastically. It has been reported that cyber crime in India increased by 11.8% in the year 2020, which accounted for reporting around only 50,000 cases. Cyber crime is one of the toughest crimes for the Police to solve due to many challenges they face including underreporting, the jurisdiction of crime, public unawareness and the increasing costs of investigation due to technology. Certain offences may end up being bailable under the IPC but not under the IT Act and vice versa or maybe compoundable under the IPC but not under the IT Act and vice versa due to the overlap between the provisions of the IPC and the IT Act. For example, if the conduct involves hacking or data theft, offences under sections 43 and 66 of the IT Act are bailable and compoundable, whereas offences under Section 378 of the IPC are not bailable and offences under Section 425 of the IPC are not compoundable. Additionally, if the offence was the receipt of stolen property, the offence under section 66B of the IT Act was bailable while the offence under Section 411 of the IPC was not. In the same manner, in respect

of the offence of identity theft and cheating by personation, the offences are compoundable and bailable under sections 66C and 66D of the IT Act, whereas the offences under Sections 463, 465, and 468 of the IPC are not compoundable and the offences under sections 468 and 420 of the IPC are not bailable. In Gagan Harsh Sharma v. The State of Maharashtra (2018), the Bombay High Court addressed the issue of non-bailable and non-compoundable offences under sections 408 and 420 of the IPC in conflict with those under Sections 43, 65, and 66 of the IT Act that is bailable and compoundable. Information Technology Rules (IT Rules): There are several aspects of the collection, transmission, and processing of data that are covered by the IT Rules, including the following: The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011: According to these rules, entities holding individuals' sensitive personal information must maintain certain security standards that are specified.The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021: To maintain the safety online of users' data, these rules govern the role of intermediaries, including social media intermediaries, to prevent the transmission of harmful content on the internet.The Information Technology (Guidelines for Cyber Cafe) Rules, 2011: According to these guidelines, cybercafés must register with an appropriate agency and maintain a record of users' identities and their internet usage.The Information Technology (Electronic Service Delivery) Rules, 2011: Basically, these regulations give the government the authority to specify the delivery of certain services, such as applications, certificates, and licenses, by electronic means.Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (the CERT-In Rules): There are several ways in which the CERT-In rules provide for the working of CERT-In. In accordance with rule 12 of the CERT-In rules, a 24-hour Incident response helpdesk must be operational at all times. Individuals, organisations and companies can report cybersecurity incidents to Cert-In if they are experiencing a cybersecurity Incident. The Rules provide an Annexure listing certain Incidents that must be reported to Cert-In immediately. Another requirement under Rule 12 is that service providers, intermediaries, data centres, and corporate bodies inform CERT-In within a reasonable timeframe of cybersecurity incidents. As a result of the Cert-In website, Cybersecurity Incidents can be reported in various formats and methods, as well as information on vulnerability reporting, and incident response procedures. In addition to reporting cybersecurity incidents to CERT-In in accordance with its rules, Rule 3(1)(I) of the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021 also requires that all intermediaries shall disclose information about cybersecurity incidents to CERT-In. Companies Act, 2013: A majority of the corporate stakeholders consider the Companies Act of 2013 to be the most pertinent legal obligation to properly manage daily operations. This Act enshrines in law all the techno-legal requirements that need to be met, implementing the law as a challenge to the companies that are not compliant. As part of the Companies Act 2013, the SFIO (Serious Fraud Investigation Office) is entrusted with powers to investigate and prosecute serious frauds committed by Indian companies and their directors. As a result of the Companies Inspection, Investment, and Inquiry Rules, 2014 notification, the SFIOs have become even more proactive and serious in regard to this. By ensuring proper coverage of all the regulatory compliances, the legislature ensured that every aspect of cyber forensics, e-discovery, and cybersecurity diligence is adequately covered. Moreover, the Companies (Management and Administration) Rules, 2014 prescribe a strict set of guidelines that confirm the cybersecurity obligations and responsibilities of corporate directors and senior management. Cybersecurity Framework (NCFS): As the most credible global certification body, the National Institute of Standards and Technology (NIST) has approved the Cybersecurity Framework (NCFS) as a framework for harmonizing the cybersecurity approach. To manage cyber-related risks responsibly, the NIST Cybersecurity Framework includes guidelines, standards, and best practices. According to this framework, flexibility and affordability are of prime importance. Moreover, it aims at fostering resilience and protecting critical infrastructure by implementing the following measures: A better understanding, management, and reduction of the risks associated with cybersecurity.Prevent data loss, misuse, and restoration costs.Determine the most critical activities and operations that must be secured.Provides evidence of the trustworthiness of organizations that protect critical assets.Optimize the cybersecurity return on investment (ROI) by prioritizing investments.Responds to regulatory and contractual requirementsAssists in the wider information security program. Using the NIST CSF framework in conjunction with ISO/IEC 27001 simplifies the process of managing cybersecurity risk. Moreover, NIST's cybersecurity directive also allows for easier collaboration in the organization as well as across the supply chain, allowing for more effective communication. Why cyber crime laws in India Just like the other countries, our country is too concerned about the issue of cyber security and related crimes. Particularly in India, there are a growing number of cyber security concerns, and its responsibility to resolve them is of critical importance. It has recently been revealed that the government is losing nearly R. 1.25 lakh crore per annum to cyber-attacks overall, according to an Economic Times analysis of cyber crime. According to another study published by Kaspersky, the number of attacks in India increased from 1.3 million to 3.3 million from the first quarter of 2020 till the end of that quarter. A total of 4.5 million attacks were recorded by India in July 2020, which was the largest number recorded so far. In July 2021, In violation of the Reserve Bank of India's directions on the storage of payment system data, Mastercard Asia/Pacific Pte Ltd (Mastercard) was banned from onboarding new domestic customers. A cyber security policy, however, does not offer an adequate method of preventing the hazards posed by the internet, and the most effective means of confronting these threats is through training. There are significant resources that the government must dedicate to safeguarding important data assets. Cyberlaw needs to be updated to incorporate the latest legal and technological developments and to address the challenges posed by the rapid development of technology. Importance of cyber crime laws The following points can highlight the importance of cyber laws: An important goal of any cyber law is to prosecute those who undertake illegal activities using the internet. To effectively prosecute these types of crimes, such as cyber abuse, assaults on other websites or individuals, theft of records, disrupting every company's online workflow, and other criminal activities, significant efforts should be undertaken, and hence, which is where cyber laws come into the picture.In the cases involving a violation of cyber law, the action is taken against the individual on the basis of his location and how was he involved in that violation.Prosecuting or retracting hackers is the most important thing since most cyber crimes are beyond the reach of a felony, which is not a crime.The use of the internet is also associated with security concerns and there are even some malicious individuals who want to gain unauthorised access to the computer device and commit fraud using it in the future. Hence, all rules and cyber laws are designed to protect internet businesses and internet users from unwanted unauthorized access and malicious cyber-attacks. There are a variety of ways in which individuals or associations can take action against others who commit criminal acts or break cyber laws. Need for cyber crime laws in India Cyberlaw is of particular importance in countries such as India, where the internet is used widely. In order to protect both individuals and organizations against cyber crime, the law was enacted. The cyberlaw allows other people or organizations to take legal action against someone if that person violates and breaks the provisions of the law. Cyberlaw may be required in the following circumstances: Due to the fact that all the transactions associated with stocks are now executed in demat format, anyone who is involved with these transactions is protected by cyber law in the event of any fraudulent transactions.Almost all Indian companies have electronic records. A company may need this law to prevent the misuse of such data.As a result of the rapid development of technology, various government forms are being filled out electronically, such as income tax returns and service tax returns. Anybody can misuse those forms by hacking government portal sites, and thus, cyberlaw is required under which legal action can be taken.Shopping today is done through credit cards and debit cards. Unfortunately, some frauds perpetrated by means of the internet clone these credit cards and debit cards. The cloning of a credit or debit card is a technique that allows someone to obtain your information via the Internet. This can be prevented by cyberlaw as under Section 66C of the IT Act, there is 3-year imprisonment along with a fine up to one lakh rupees if anyone tries to make use of any electronic password fraudulently or dishonestly.Business transactions are typically carried out by means of digital signatures and electronic contracts. The misuse of digital signatures and electronic contracts can be easily accomplished by anyone involved with them. Cyberlaw provides protection against these types of scams. Cyber crime and security Cybersecurity can be defined as the collection of technologies, processes, and practices that are intended to prevent networks, devices, programs, and data from being attacked, damaged or accessed by unauthorized persons. Alternatively, cyber security may also be referred to as information technology security. Several types of organizations, including government, military, corporations, financial institutions, and medical facilities use computers and other devices to process, store, and process extremely large amounts of data. Many of those records contain sensitive data including intellectual property, financial information, personal information, etc. for which unauthorized access or exposure could have negative repercussions. There is a growing area of cyber security dedicated to protecting the systems for processing and storing sensitive information that organizations send over networks and to other devices. Thus, cybersecurity is the field dedicated to securing this sensitive information as well as the systems by which such information is transmitted or stored. With the number of cyber attacks and the sophistication of those attacks moving up, companies and organizations, especially those that are tasked with safeguarding sensitive data, (including attacks pertaining to national security, health information, or financial information), there must be steps taken for ensuring the security of their proprietary business and personnel data. Cyber security strategies It is also extremely important for an organisation to develop and build an effective cybersecurity strategy. The following must be included in cybersecurity strategies: Ecosystem: The ecosystem of an organisation needs to be strong in order to prevent cyber crime. Generally, an organisation's ecosystem has 3 components, i.e, automation, interoperability, and authentication. By developing a safe and strong system, the organisation would be likely to protect these components and could not be attacked by malware, attrition, hacks, insider attacks, and equipment thefts. Framework: A framework for compliance with security standards is an assurity that can help to ensure that these standards are adhered to. Updating infrastructure is made possible as a result of this. Furthermore, it also facilitates collaboration between governments and businesses. Open standards: Enhanced security against cyber crime is a direct result of open standards. Through open standards, both businesses and individuals can easily implement proper security measures. These standards will also facilitate a greater level of economic growth and a broader range of new technologies. IT mechanisms: A variety of IT measures or mechanisms are available that can be beneficial. In the fight against cyber crime, it is essential to promote these measures and mechanisms. End-to-end protection measures, association-based protection, link-based protection, and data encryption are a few of the measures. E-governance: It is possible for the government to provide services online through e-governance. E-governance, however, is not taken advantage of in many countries. Cyberlaw should focus on advancing this technology to give citizens greater control. Infrastructure: As part of cybersecurity, protecting the infrastructure is one of the most crucial steps. This applies especially to the electrical grid as well as data transmission lines. Cyber crime is often perpetrated against outdated infrastructure. Differences between cyber crime and cyber security There is more to cybersecurity than just a set of guidelines and actions designed to prevent cyber crime. Ultimately, cyber-security aims to prevent hackers from finding and exploiting vulnerabilities in government and corporate networks, and therefore to make life difficult for them to do so. By contrast, cyber crime, compared to traditional crime, tends to focus more on preserving the privacy of individuals and their families while engaging in online activities. Here is a list of the differences between cyber security and cyber crime that you should know about: Types of crime: The type of crime in cyber security is defined by those crimes in which a computer program, hardware, or computer network serves as the main target of an attack if it is compromised. On the other hand, cyber crime is concerned with a specific person or group of people, along with their data, as the main targets. Victims: Secondly, there are also differences in the types of victims in these two fields. Governments and corporations are the primary targets in cyber security while, in cyber crime, victims can range from individuals, families, organizations, governments, and corporations.Subject matter: Both of these fields are studied in different disciplines. Information technology, computer science, and computer engineering are the fields that cover cybersecurity. Code writing, networking and engineering are used to enhance network security. In contrast, cyber crime falls under the criminological, psychological, and sociological categories. It refers to a theory of how crime occurs and how it can be prevented. Conclusion With the advancement in technology, disturbing elements are appearing on the dark web that is disturbing. The Internet has become a tool of evil deeds that are exploited by intelligent people for evil motives and sometimes for financial gain. Thus, at this point in time, cyber laws come into the picture and are important for every citizen. Due to the fact that cyberspace is an extremely difficult territory to deal with, some activities are classified as grey activities that cannot be governed by law. In India as well as across the globe, with the increasing reliance of humans on technology, cyber laws need constant up-gradation and refinement to keep pace. There has also been a significant increase in the number of remote workers as a consequence of the pandemic, which has increased the need for application security. There is a need for legislators to take extra precautions to keep ahead of the imposters so that they can act against them as soon as they arise. It can be prevented if lawmakers, internet providers, banks, shopping websites and other intercessors work together. However, ultimately, it is up to the users to participate in the fight against cyber crime. The only way for the growth of online safety and resilience to take place is through the consideration of the actions of these stakeholders, ensuring they stay within the confines of the law of cyberspace. References Students of Lawsikho courses regularly produce writing assignments and work on practical exercises as a part of their coursework and develop themselves in real-life practical skills. LawSikho has created a telegram group for exchanging legal knowledge, referrals, and various opportunities. You can click on this link and join: Follow us on Instagram and subscribe to our YouTube channel for more amazing legal content.