CHAPTER 1

INTRODUCTION

What is a cyber crime?

Cyber crime is a generic term that refers to all criminal activities done using the medium of communication devices such as computers, mobile phones, tablets etc., the Internet, cyber space and the worldwide web. Cyber crime also can be committed on individuals who don't have any knowledge of computers or the Internet.

The simplest and one among the first official definitions was given by a group of experts constituted by OCED (Organisation for Economic Cooperation and Development) in 1983. They defined the term computer crime as any illegal, unethical or unauthorised behaviour involving automatic processing and transmission of data. According to Cambridge Dictionary defines cyber crime as crimes committed with the use of computers or relating to computers especially through the internet.

There isn't really a comprehensive definition for cyber crime. The Indian Law the IT Act, 2000 has not defined the term 'cyber crime'. In fact, the Bhartiya Nyaya Sanhita, 2023 does not use the term 'cyber crime' at any point even after its amendment. The IT Act, 2000 the Indian Cyber law. But "Cyber Security" is defined under Section (2) (nb) as means of protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

What is a Cyber Law?

Cyber Law is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace", i.e. the Internet. It is less a distinct field of law in the way that property or contract are, as it is an intersection of many legal fields, including intellectual property, law of torts, privacy, constitutional law and jurisdiction. In essence, cyber law is an attempt to apply laws designed for the physical world to human activity on the

Internet. In India The IT Act, 2000 is the primary cyber law. It has been amended several times, and as of February 2026, the latest amendments relate to the regulation of artificial intelligence and synthetic content under the IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026. IT Act, 2000, DPDPA, BNS, Cert-in guidelines along with various sectoral cyber security regulations from different regulators can be called as the complete Cyber law.

Jurisdiction

History of policing and law is always plagued with questions of jurisdiction and the fights are still on in this cyber era. Issues of jurisdiction have quickly come to the fore in the era of the Internet. The Internet does not tend to make geographical and jurisdictional boundaries clear, but Internet users remain in physical jurisdictions and are subject to laws independent of their presence on the Internet. As such, a single transaction may involve the laws of at least three jurisdictions. Under Section 75 of the IT Act, 2000, the Act applies to offences committed outside India if the act involves a computer, computer system or computer network located in India. A victim of cyber crime may file a police complaint at the nearest police station where the crime was committed or where the victim first comes to know of it. Online complaints can also be made at the National Cyber Crime Reporting Portal (www.cybercrime.gov.in).

What is Cyber Security?

Cyber Security plays a significant role in the ongoing development of information technology, as well as internet services. Enhancing cyber security and protecting critical information infrastructures is essential to each nation's security and economic well-being. Making the internet safer (and protecting Internet users) has become integral to the development of new services as well as governmental policy. Deterring cybercrime is a vital component of the national cyber security and critical information infrastructure protection strategy. In particular, this includes the adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes and activities intended to affect the integrity of national critical infrastructures. At the national level, this is a shared responsibility requiring coordinated action related to the prevention, preparation,

response, and recovery from incidents on the part of government authorities, the private sector and citizens. At the regional and international level, it entails cooperation and coordination with relevant partners. The formulation and implementation of the national framework as well as strategy for cyber security requires a comprehensive approach. Cyber security strategies for example, the development of technical protection systems or the education of users to prevent them from becoming victims of cybercrime can help to reduce the risk of cybercrime. The development and support of cyber security strategies is vital for the fight against cybercrime.

The legal, technical and institutional challenges posed by the issue of cyber security are global and far-reaching, and can only be addressed through a coherent strategy taking into account the role of different stakeholders and existing initiatives, within a framework of international cooperation.
The fight against cybercrime needs a comprehensive approach. Given that technical measures alone cannot prevent any crime, it is critical that law enforcement agencies are allowed to investigate and prosecute cybercrime effectively.

What is Cyber Forensics?

Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for its presentation in the court of law. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.

What is a Cyber War?

Cyber war is a form of war which takes place on computers and the Internet, through electronic means rather than physical ones. Cyber-warfare, as it is also known, is a growing force in the international community, and many nations regularly run cyber war drills and games so that they are prepared for genuine attacks from their enemies. With an increasing global reliance on technology for everything from managing national electrical grids to ordering supplies for

troops, cyber war is a modern means of attack to which many nations are vulnerable.

In cyber war, people use technological means to launch a variety of attacks. Some of these attacks take a very conventional form. Computers can be used, for example, for propaganda, espionage, and vandalism. Denial of service attacks can be used to shut down websites, silencing the enemy and potentially disrupting their government and industry by creating a distraction. Cyber war can also be utilized to attack equipment and infrastructure, which is a major concern for heavily industrialized nations which rely on electronic systems for many tasks. Cyber war can be part of kinetic war known as hybrid war as seen from Ukraine and Iran war in 2026.

Using advanced skills, people can potentially get backdoor access to computer systems which hold sensitive data or are used for very sensitive tasks. A skilled cyber warrior could, for example, interrupt a nation's electrical grid, scramble data about military movements, or attack government computer systems. Stealthier tactics might involve creating systems which can be used to continually gather and transmit classified information directly into the hands of the enemy or using viruses to interrupt government computer systems.

✦✦✦

CHAPTER 2

HACKING

What is Hacking?

Hacking means unauthorized attempts to bypass the security mechanisms of an information system or network. Also, in simple words hacking is the unauthorized access to a computer system, programs, data and network resources. (The term "hacker" originally meant a very gifted programmer. In recent years though, with easier access to multiple systems, it now has negative implications.)

Hacking occurs when an individual, or group of individuals make use of a computer unauthorizedly, specifically when this use is trying to bypass a computer's or network's security measures. Cellular telephones are the latest targets for such attacks. The first worms capable of attacking cell phones were detected in 2004. Indications are that these attacks could prove even more prolific than those against personal computers because there are so many more cell phones than computers. In addition, computer hacking is a crime in itself; there are future consequences the victim will have to deal with as well. Now, the question arises who does the hacking?

Who is a hacker?

In the most general sense, a "hacker" is someone who enjoys modifying and subverting systems, whether technological, bureaucratic or sociological. Most often the term is used to describe someone who has learned about technology by picking apart systems. In the past decade, however, "hacker" has come to describe those people with a hands-on interest in computer security and circumventing such security.

Hacking Tools

Hacking largely is possible because of free tools disguised as network tools available on the internet tools like ping of death, hacker evolution, netstat live, advanced port scanner, ophcrack etc. are commonly used.

Law as Applicable and Illustration:-

Under the IT Act, 2000 as amended by the Information Technology (Amendment) Act, 2008, Section 43(a) read with section 66 and 66C is applicable and Section 379 & 406 of Indian Penal Code, 1860 also are applicable. (As per the Bharatiya Nyaya Sanhita, 2023 Section 303 and 316 are applicable). The victim can file a complaint in the nearest police station where the above crime has been committed or where he comes to know about the said crime. He also can claim for compensation upto Rs. 5 crores with the adjudicating officer of the state and compensation above Rs. 5 crores with the civil court of the relevant jurisdiction.

Punishment: If the crime is proved under the IT Act, 2000 accused shall be punished for imprisonment which may extend to three years or with fine which may extend to five lakh rupees or both.

Category of Crime: As per Section 77-B of the IT Act, 2000 the above offence shall be cognizable and bailable, while if Section 379 of IPC or 303 of BNS is applied along with other Sections the said offence is cognizable, non-bailable, compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate.

Illustration 1

If you physically take the mobile phone of your friend in your hand without his permission it amounts to “securing its access” i.e. hacking.

Illustration 2

Guessing of a sequence on a mobile phone to unlock the phone or guessing and keying in passwords on computers or ATM Pin Numbers amounts to hacking.

Illustration 3

The hacker in 2003 and his accomplices from Russia had stolen usernames, passwords, credit card information, and other financial data by hacking into computers of US citizens. They would then extort money from those victims with the threat of deleting their data and destroying their computer systems. A hacker was convicted in the USA for causing losses of almost $25 million. The defendant pleaded guilty to numerous charges of conspiracy, computer intrusion, computer fraud, credit card fraud, wire fraud, and extortion.

Illustration 4

A Student who was hailing from Jamnagar and had completed his Bachelor of Computer Application course (BCA). He allegedly got into the website of Gujarat Technological University (GTU) and changed its data to get admission in a post-graduation course. This student had allegedly broken into the GTU website for getting admission in Master of Computer Application (MCA). This act of the said student is called an act of hacking.

Illustration 5

On Aug 16, 2010 the liquor baron and Rajya Sabha member, Mr. Vijay Mallya's parliamentary website had been hacked by the Pakistan cyber army. The Pakistan cyber army not only hacked the website but also threatened to make "Indian cyberspace into hell". This act constitutes hacking into a web server.

Illustration 6

In 2011, a hacking group called lulzsec almost hacked the world by getting into CIA, US Senate, IMF, Sony, Nintendo websites and made critical information of clients and citizens public. This act constitutes group hacking on the internet, this act normally happens due to fallout of rival hacking groups on the internet.

Illustration 7
AI-Enabled Hacking (Claude Mythos)

Arjun, a rogue developer, crafts a carefully worded prompt to an AI assistant, disguising a request for a network

vulnerability scanner as a "security audit tool." The AI, unable to detect the malicious intent, generates functional exploit code. Arjun uses this code to gain unauthorised access to a hospital's patient database. He never writes a single line of code himself - the AI does it for him. This act of using an AI tool to generate or deploy hacking code constitutes hacking under Section 43(a) read with Section 66 of the IT Act, 2000, and Section 111 of the BNS, 2023 (organised crime facilitated through electronic means). The IT Amendment Rules, 2026 now mandate platforms offering AI-based computer resources to implement safeguards against generation of such unlawful content.

Case Law 1 - Sanjay Kumar v. State of Haryana

(JMFC Faridabad Sessions Court Faridabad Punjab Haryana High Court, CRR No. 66 of 2013, decided 10 January 2013)
Sanjay Kumar, a software vendor deputed to maintain a bank's computer system at Vijay Bank, Faridabad, fraudulently manipulated the bank's electronic accounting records to transfer Rs. 17,67,409 into his own account. The Judicial Magistrate First Class, Faridabad convicted him on 1 September 2011 under Sections 65 and 66 of the IT Act, 2000, and sentenced him to two years rigorous imprisonment with a fine of Rs. 1,000 under each section. The Sessions Court upheld the conviction in 2012. The Punjab-Haryana High Court dismissed his revision petition in 2013. This is one of the earliest small-court convictions under Section 66 IT Act where actual imprisonment was awarded for hacking a bank's computer system.

✦✦✦

CHAPTER 3

CYBERBULLYING AND TROLLING

What is Cyberbullying and Trolling?

Cyber bullying involves the use of information and communication technologies to support deliberate, repeated, and hostile behavior by an individual or group that is intended to harm others.

Cyberbullying can also be defined as, any communication posted or sent by a minor online, by instant messenger, e-mail, Social Networking Site, website, diary site, online profile, interactive game, handheld device, cell phone or other interactive device that is intended to frighten, embarrass, harass or otherwise target another minor.

According to internet sources, 'trolling' (also known as cyber bullying or internet-bullying) is the anti-social act of causing personal conflict and controversy online. Trolling is recognised as deliberately inflicting hatred, bigotry, racism, misogyny, or just simple bickering between others. People who partake in 'trolling' are referred to as 'trolls'. They use any environment where they are allowed to make public comments, such as blog sites, social networks (like Facebook and Twitter), news sites, discussion forums, and game chat.

Unfortunately, trolling is a phenomenon that has swept across websites in recent years. Supporters argue it's about humour or freedom of speech. However, for some the ferocity and personal nature of the abuse causes great distress.

Details of Cyberbullying

Cyberbullying is any harassment that occurs via the internet and mobile phones, vicious forum posts, name calling in chat rooms, posting fake profiles on websites, and mean or cruel email messages are all ways of cyberbullying.

While simple teasing regarding one's personal habits, figure, or any other object which generates curiosity in the young minds is not gravely harmful, but when the same verbal remarks makes a child suffer deep depression, withdrawal symptoms or even affect his studies, the seriousness of the issue does not remain bounded in only "just for fun sake". With the easy access to mobile phones and internet by the school students, the matter becomes more serious as the identity of the victim may be revealed to a bigger circle. It is however, a much neglected fact that the habit of bullying and cyberbullying in schools open the path for the offender to become a habitual ragger in colleges and even turn him into a bigger cyber-criminal.

With today's technology bullying has become easier, the children and youth of this generation do not even need to have personal confrontation. Cyber bullying can be defined as "any communication posted or sent by a minor online, by instant messenger, e-mail, social networking site, website, diary site, online profile, interactive game, handheld device, cell phone or other interactive device that is intended to frighten, embarrass, harass or otherwise target another minor".

Law as Applicable and Illustration:-

Under Indian Penal Code, 1860 Section 500, 506 & 507 are applicable. **(As per the Bharatiya Nyaya Sanhita, 2023**

Section 356(2), 351(2)/(3) and 351(4)). The victim can file a complaint in the nearest police station where the above crime has been committed or where he comes to know about the said crime.

Punishment: If the crime is proved under the IT Act, 2000 the accused shall be punished for imprisonment which may extend to two years and with fine.

Category of Crime: As per Section 77-B of the IT Act, 2000 the above offence shall be cognizable and bailable while if Section 500 of IPC or 356(2) of BNS is applied for the said offence in case of public servant is non-cognizable, bailable, compoundable with permission of the court before which any prosecution of such offence is pending and triable by court of session and in any other case non-cognizable, bailable, compoundable and triable by magistrate of the first class. If Section 506 of IPC or 351(2)/(3) of BNS is also applied for the said offence, then under criminal intimidation it is non-cognizable, bailable, compoundable and triable by the magistrate. If threat be to cause death or grievous hurt etc., it is triable by magistrate of the first class. If along with other Section 507 of IPC or 351(4) of BNS is also applied for, the said offence under criminal intimidation is non-cognizable, bailable, non-compoundable and triable by the magistrate of the first class.

Illustration 1

A student is bombarded by various threatening and taunting emails at home about him being squinted, even though there is no direct harassment at school. The victim has no idea who is sending the messages and starts to feel like everybody is against them. That student is being cyber bullied.

A school chat room is spammed with name-calling posts that spread vicious rumors about a specific student. The rumors aren't true but kids at school see the posts and believe them. The student is then teased by peers. This student is the victim of cyberbullying.

A defamatory fake profile is posted Facebook using a student's real name, photo and contact information. That student starts getting abusive email messages from strangers

who think the profile is real. Some of the messages are crude. Some of the messages are mean. This is another example of cyberbullying.

Illustration 2

Manali was a 13-year-old from Mumbai who struck up an online friendship on the popular social networking site Facebook with a person she believed was a new boy in her hometown. In actuality, the "friend" was a group of individuals, including adults, who were intent on humiliating the poor girl because of a friendship with another child that had gone away. Manali was very upset when she found out the truth, then later committed suicide once the friendship had terminated.

Illustration 3

Anna, an eighth standard student, lost two years of her life as a result of cyberbullying from classmates. Anna was forced to deal with websites created by her classmates that featured names like "Kill Anna Incorporated" that were filled with threatening, homophobic remarks about the young girl. These hurtful kids obtained screen names with handles close to Anna's name and used them to make suggestive remarks and sexual advances on Anna's teammates on the field hockey team. This act on Anna was cyberbullying.

Illustration 4

In a place near Mumbai, A fake Facebook profile with her picture, address and phone number was created of a widowed lady who stays in a chawl and in the status they wrote "I get fantasized when someone rapes me". She got all nasty phone calls and people landed on her door mid-night shouting we want to rape you open the door.

Illustration 5

Nokia has been active at attacking its competitors after entering the smartphone market. They tweeted "NOT THE SAMESUNG" after the release of the Samsung S5, in a bid to highlight the uniqueness of the Lumia. This act is trolling by Nokia.

Illustration 6

Anita, a small-time celebrity once mentioned on social media that she has gotten pregnant and doesn't know how? In response to this people across the world trolled her by putting remarks like Are you high on drugs? Are you lunatic? Did you forget the count of men? How many men would be the father of this child? Will the middle name of the child you deliver would be "Anonymous"? Do you think of donating this black income for the country by sending him in the military? The trolls made Anita suicidal, she was suggested by her doctors to close her social media accounts. This act of chasing a person is called trolling and when a single person trolls he is many times unaware of the consequences the victim has to face.

Precautions:

1. Protect your online reputation: use the services provided (e.g. privacy settings) to protect your 'digital footprint' and always think before you post. Information posted online can last forever and could be shared publicly by anyone.

2. Keep it private, only give your mobile number, personal email address, home address and other contact details to trusted friends, not to people you only know online.

3. Know where to find help: understand how to report abuse to service providers and how to use blocking and deleting tools. If something happens that upsets you online, it's never too late to tell someone. You can contact police for help and advice if you are scared or worried about online abuse.

4. Don't give in to pressure: if you lose your inhibitions, you've lost control; once you've pressed send you can't take it back. Don't share or send indecent pictures.

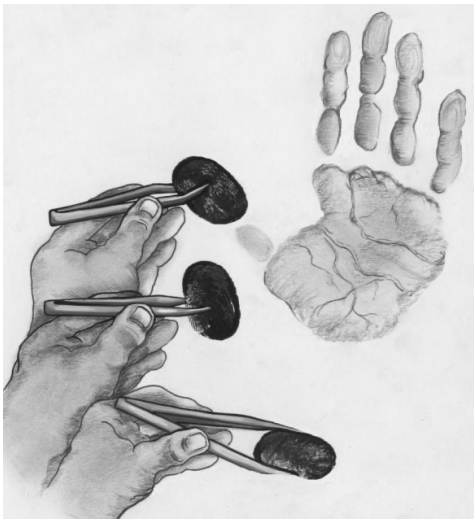
✦✦✦

CHAPTER 4

IDENTITY THEFT

What is Identity Theft?

According to Wikipedia, identity theft is a form of fraud or cheating of another person's identity in which someone pretends to be someone else by assuming that person's identity, typically in order to access resources or obtain credit and other benefits in that person's name. Under the Information Technology (Amendment) Act, 2008, crime of identity theft under Section 66-C, whoever, fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person known as identity theft. This section is frequently invoked by section 66D read with Section 420 IPC or Section 318 of the BNS, 2023, which carry a similar punishment and are procedurally more familiar to the judiciary.



Identity theft is a term used to refer to fraud that involves stealing money or getting other benefits by pretending to be someone else. The term is relatively new and is actually a misnomer, since it is not inherently possible to steal an identity, only to use it. The person whose identity is used can suffer various consequences when they are held responsible for the perpetrator's actions. At one time the only way for someone to steal somebody else's identity was by killing that person and taking his place. It was typically a violent crime. However, since then, the crime has evolved and today's white collar criminals are a lot less brutal. But the ramifications of identity theft are still scary. Over 5,00,000 people the world over are victims of identity theft each year.

In India, people are very ignorant & careless when it comes to privacy of personal information. We divulge our address and phone numbers to shops, restaurants etc., which is unnecessary and it is carelessness on our part. Identity theft can occur in multiple forms. One of the main areas of concern and places via which identity theft occurs is, through service providers who have our personal information. As per the non-profit Identity Theft Resource Center, identity thefts can be subdivided into four categories. These include financial identity theft, criminal identity theft, identity cloning, and business / commercial identity theft.

In many cases the victim is not even aware of what is being done till it is already too late. Identity theft may be used to facilitate crimes, including illegal immigration, terrorism, and espionage. It may also be used as a means of blackmail. There have also been cases of identity cloning to attack payment systems, including online credit card processing and medical insurance. Sometimes people may impersonate others for non-financial reasons too. This is often done to receive praise or attention for the victim's achievements. This is sometimes referred to as identity theft in the media and is a common trend seen by look-alikes. One does not have to think too far back before recollecting a probable victim of identity theft in India.

Law as Applicable and Illustration:-

Under the IT Act, 2000 as amended by the Information Technology (Amendment) Act, 2008, Section 66-C is applicable and Section 419 of Indian Penal Code, 1860 is applicable along with. (**As per the Bharatiya Nyaya Sanhita, 2023 Section 319 is applicable)**. The victim of identity theft can file a complaint in the nearest police station where the above crime has been committed or where he comes to know about the crime.

Punishment: If the crime is proved under the IT Act, the accused shall be punishable with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

Category of Crime: As per Section 77-B of the IT Act, 2000 the above offence shall be cognizable and bailable while if Section 419 of IPC or 319 of BNS is applied in that case the said offence is cognizable, bailable, compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate.

Illustration 1

In Navi Mumbai, India an American national named Ken Haywood, had to pay huge price for his ignorance as his unsecured Wi-Fi Internet connection was hacked, theft of identity was committed by terrorist during Ahmadabad terrorist attacks and, terrorist committing identity theft used Haywood's Wi-Fi connection to send terror emails to various news channels.

Illustration 2

The biggest case of identity theft ever seen, took place in August of 2009. Eleven people, including a US secret service informant, had been charged in connection with the hacking of nine major retailers and the theft and sale of more than 41 million credit and debit card numbers. This data breach is believed to be the largest hacking and identity theft case. Three of those charged are US citizens, while the others are from places such as Estonia, Ukraine, Belarus and China. It is alarming that 11 people of different nationalities whose nation barely get along with each other, pull off a heist involving a whooping 41 million credit card and debit card numbers.

Illustration 3

Ms. Sweety an article clerk of a chartered accountant firm named v & v associates fraudulently obtains digital certificates of a client Mr. Sunil Oberoi from the CA's computer. Ms. Sweety then creates suniloberoi@yahoo.com a fake email id, and commits financial fraud amounting to rupees four crores. This act of Ms. Sweety is an act of identity theft committed on Mr. Sunil Oberoi.

Illustration 4

UTV Motion Pictures fell prey to identity theft. The company learnt that the perpetrators not only created a fake company profile on a popular social networking site, but also organized

auditions to cast aspiring actors in a film under the said banner. Reportedly, the scam set-up took quite a sum of

money from the actors to land roles in the film. A same type of case was also handled by me for Balaji Telefilms.

Precaution

Next time you move home, make sure you inform all your service providers about the change of address as even the telephone bills that land in your old house, can be misused by anti-social elements for getting a SIM card or a second-hand car. Another method criminals adopt for identity theft is to use documents given to agents procuring bank loans or mobile phone connections.

✦✦✦

Notes:

CHAPTER 5

DATA THEFT AND SOURCE CODE THEFT

What is Data Theft?

According to the IT Act, 2000 as amended by the Information Technology (Amendment) Act, 2008, The crime of data theft under Section 43(b) is stated as, If any person without the permission of the owner or any other person who is in charge of the computer, computer system or computer network downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium. According to Wikipedia, data theft is a growing problem primarily perpetrated by office workers with access to technology such as desktop computers and hand-held devices capable of storing digital information such as flash drives, iPods and even digital cameras. The damage caused by data theft can be considerable with today's ability to transmit very large files via e-mail, web pages, USB devices, DVD storage and other hand-held devices.

Data theft is, quite simply, the unauthorized copying or removal of confidential information from a business or other large enterprise. It can take the form of ID-related theft (the theft of customer records) or the theft of a company's proprietary information or intellectual property. The act of illegally downloading data from a networked computer to a USB flash drive is called thumb sucking. The use of an iPod or other portable music player for the same purpose is called pod slurping. Because of how easy it is to copy data to these types of devices, some companies are now outlawing the use

of any personal, portable data storage devices in their offices. Term used to describe when information is illegally copied or taken from a business or other individual. Commonly, this type of information is user information such as passwords, social security numbers, credit card information, other personal information, or other confidential corporate information. Because this information is illegally obtained, when the individual who stole this information is apprehended, it is likely he or she will be prosecuted to the fullest extent of the law.

What is Source Code Theft?

Computer source code or computer program is the most important asset of Information Technology companies. Source code is the programming instructions that are compiled into the executable files that are sold by software development companies. Most source code thefts take place in software companies. In simple words stealing a source code of the company is called source code theft.

Law as Applicable and Illustration:-

Under the IT Act, 2000 as amended by the Information Technology (Amendment) Act, 2008, Section 43(b) read with Section 66 is applicable and Section 379, 405 & 420 of Indian Penal Code, 1860 applicable for data theft and for source code theft section 43(j), 65, 66 & 66B of the Information Technology Act, 2000 and section 63 of the Copyright Act are applicable. **(As per the Bharatiya Nyaya Sanhita, 2023 Section 303, 316 and 318(3) applicable).** The victim can file a criminal complaint in the nearest police station where the above crime has been committed or where he comes to know about the said crime. He also can claim compensation upto Rs. 5 crores with the adjudicating officer of the state and compensation above Rs. 5 crores with the civil court of the relevant jurisdiction.

Punishment: If the crime of data theft is proved under the IT Act, 2000 the accused shall be punished for imprisonment which may extend to three years or with fine which may extend to five lakh rupees or both and if the crime of source code theft is proved under the IT Act, 2000 the accused shall be punished for imprisonment which may extend to three years or with fine which may extend to five lakh rupees or

both and under the Copyright Act, shall be punishable with imprisonment for a term which shall not be less than six months but which may extend to three years and with fine which shall not be less than fifty thousand rupees but which may extend to two lakh rupees.

Category of Crime: As per Section 77-B of the IT Act, 2008 the above offence shall be cognizable and bailable while if Section 379 of IPC or 303 of BNS is applied along with Section 420 of IPC or 318 of BNS the said offence is cognizable, non-bailable and compoundable by the person cheated and triable by any magistrate.

Illustration 1

Ms. Riya visits her cousin Ms. Ruchi's house, Riya finds the desktop computer switched on, when Riya surfs into the hard disk, she likes certain Pdf files, Riya fraudulently copies certain files to her pen drive without Ruchi's permission, this act of Riya constitutes crime of data theft.

Illustration 2

A famous builder's, sister applied a rule to the email's of client's received on the builder's laptop. This rule forwarded all emails and files received by builder fraudulently to sisters email id. This builder had a corporate email id as anil.builder@company.com, a fraudulent emails aniil.builder@gmail.com was made and all emails were forwarded automatically here. This fraudulent act of the lady is the act of data theft as the act was done without the permission of the builder and the theft was committed for commercial benefit.

Illustration 3

Mr. Sunil Verma working with an MNC, for the last 4 years, had just got a lucrative job with the competitor company, and he was on a notice period for one month. On his last day with the current employer, Sunil attaches all data files with regards to clients and certain software source code to his personal Gmail id. Sunil Verma thus commits the crime of data theft on his employer. This crime gets proved by the proxy server and firewall logs of the company and is substantiated by the data received from Gmail Inc.

Illustration 4

A newly launched website called www.crickymasala.com for want of content, copies without permission verbatim to verbatim content from established website www.cricknext.com. This act of www.crickymasala.com was done to gain commercial benefit to self. This act gets classified as the crime of data theft.

Illustration 5

Two employees of a textile shop were arrested for stealing important data from an establishment in Tirupur city. R Pugalenthi of Tiruvarur district completed Plus Two and was working as a purchase manager at Chennai silks in Tirupur town. He quit the job and joined as manager in a textile shop in Namakkal district. Prabhu Sankar of Attaiyam palayam in Tirupur district completed a computer related diploma course and was working as a purchase manager in Chennai silks in Tirupur city. But Pugalenthi and Prabhu Sankar had close contact and shared important documents of Chennai silks. The textile shop management suspected that Prabhu Sankar had downloaded all the customers' contacts and other important data from the office computer to his mobile phone and he had sent the data to Pugalenthi and thus committed crime of data theft.

Illustration 6

Mr. Anil used to work for a homeopathic doctor and his Doctor had written a software program for homeopathy. Anil with malicious intention copied i.e. uploaded the whole source code from his working office computer to www.codeguru.com, which is a website where you get free source code or free computer programs. This act of Anil to willfully cause loss by leaking the software with dishonest intention to cause losses to his employer is an act of source code theft.

Illustration 7

Big deal Pvt. ltd is a Raj Kundra and actor Akshay Kumar promoted company. Naaptol is an earlier established e-commerce competitor company and client of the author. A senior Ex-employee of Naaptol allegedly stole source-code and data. This data he shared with the Director of one Viral