Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2022 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rishikesh Dave; Publisher – Ayush Pandey

Evolution of Cyber Laws in India

Lavkesh Gaur[a]

[a]Chandigarh University, Chandigarh, India

Received 25 September 2022; *Accepted* 07 October 2022; *Published* 15 October 2022

The Internet is often considered as a signifying invention in the sphere leading the US to the path of development and growth but now has turned down the optimism of invention leading it to negative impacts in society. The Internet has given an opportunity to potential criminals who in a vague of mental psyche indulge themselves in criminal disgracing activities. Cybercrime deals with activities forbidden by law and disapproved in the eyes of civilized society. Criminal activities surrounded in cyberspace are an emerging problem in modern India. The governing bodies need to realize the seriousness of this domain and form some unyielding laws that are collateral to the increasing crimes. India being a state of democracy and popular sovereignty works on the principle that government is of the people for the people, by the people, hence safety and dignity of citizens are the foremost protection granted to them. The ground reality is that country with such a high population consisting of brilliant minds is wasting its potential to the bin by indulging itself to trash criminal activities. The cognitive functioning of a such hugely populated country can do wonders and top the charts of brilliance but the influence and manipulations of wicked parts of society are turning them barren. Cyber laws circumference the crimes via the Internet and provide legal protection to the aggrieved party. With the growing crime the loopholes within the existing cyber laws came into being and then they realized that the evolution of cyber laws is necessary to administer the increasing rate of cybercrimes. This paper will focus on e-crimes, types of e-crimes, laws implemented to lower cybercrime, need and background of cyber laws. The paper most importantly outlines the evolution of cyber law in India highlighting the landmark judgments challenging the formal laws.

Keywords: *cybercrime, hackers, crackers, spamming, computer vandalism.*

INTRODUCTION

A man was discovered from a fauna creature that further evolved to be a human being. From fire to ovens, from animal skins to passable clothing, we are the revolutionaries of materialized things turning coal into diamonds with our cognitive capabilities. From advancing as an ape to a human, time passed by with the evolution of creativity. Humans formed a group and started to reside together, with arising needs they realized that working and staying together is the only way that can survive in this rough environment. Hence a group of people staying together formed villages and later developed into society. With society, further comes certain norms that needed to be followed to regulate society peacefully and harmoniously. These norms are constructed to avoid any illicit conduct and wrong in society, and when these rules aren't followed then it leads to violation of righteous conduct. Therefore crime arose out of this non-fulfillment of norms out of unsatisfactory standards of living. Originally, the unfolding of human capabilities to change raw into usage arose out of needs and necessities but later, resultant of human tendency, humans always want more. The aversion inside us of never getting satisfied in what we have desired to live a luxurious life irrespective of limited means. Thus the gaze of having fairytale lifestyles sometimes lands us into bad perspectives of earning, involving criminal activities. Crime is an act or omission forbidden by law that is harmful to the people living in society resulting in fines or punishment. And now a day's cyber crimes are increasing at an alarming rate due to the above-mentioned reasons which are unlimited wants in limited means for which they chose to disgrace the dignity of society to gain their own good, but it can protect or prevent by cyber laws. Because it touches almost all aspects of transactions and activities on and involving the internet, World Wide Web, and cyberspace. A firm legal infrastructure has been defined to encounter the daily emerging cyber crimes. Therefore the illegal activities taking place have a reaction in legal form by producing strict cyber laws in retaliation to the crimes committed. Cyber crimes are encountered via computers and other electronic devices disapproved by society. This paper will focus on the e-crimes and laws implemented to deflate these activities. Crimes taking place via the Internet is the biggest bane

of technological advancement lagging behind our country in development and forefront growth[1].

WHAT IS CYBERCRIME?

An action or omission that constitutes an associate offence and is punishable by law is called a crime. Each crime and criminal are indeed looked upon with the greatest hatred by all the sections of the individuals in society, however, it is conjointly true that the study and analysis of the law of crimes have forever been one of the foremost engaging branches of jurisprudence since the first years of human civilization. After all the law of crimes has been as recent because of the civilization itself. Where people organized themselves into groups or associations the necessity for few forms of rules to control the behavior of the members of that cluster repose has been felt, where there have been rules of society, its violation was inevitable. And there lies the requirement of fashioning some ways in which and suggest to curb such tendencies within the society in the society that lead to violation of its rules. In each organized society sure acts are impressible on the pain of punishment. Wherever one person harmed another and also the injury might adequately be remunerated by cash value, the wrongdoer was needed to pay damages or compensation to the wronged individual. However, in certain the liability to pay compensation the state imposes certain penalties upon the wrongdoer with the object of protective peace within the society and promoting smart behavior towards one another and towards the community at large.

Cybercrime is characterized as crimes conducted online that use a computer as a tool or a specific target. It is very difficult to classify crimes in general into distinct groups as many crimes evolve on daily basis. The emergence of cybercrime rationalizes the fact that people are technologically expanding their vision and coming on modern criteria of committing crimes which are growing in the country leaving a terrible impact. The Internet is a powerful tool to influence people from both perspectives and hence the varied aspects of people having expert knowledge use this to

[1] T Sowmya, 'Crime: A Conceptual Understanding' (*Indian Journal Of Applied Research*, October 2011) <https://www.researchgate.net/publication/270238380_Crime_A_Conceptual_Understanding> accessed 18 September 2022

target the audience in illicit conduct disgracing one's reputation. The dependency of people on the internet and their addiction to using it for feature grants is the main reason for cybercrime evolution in today's world. some of the cyber crimes that disgrace human integrity and societal safety are: cyberstalking, cyber terrorism, phishing, cyberbullying, cyber pornography, cyber defamation, email bombing, and email spoofing. To monitor these crimes laws came into effect to lower the crime rate growing in modern India via the internet through the information technology act taking an Initiative to monitor criminal activities and signifying the law.

NEED FOR CYBER LAWS

With the increasing use of technology and Internet variations, the bad side also started to emerge growingly. The Internet crimes happening via cyberspace were not getting under control and hence the intensity of crimes was unstoppable and evitable, the existing laws weren't able to curtail the problem and hence the need arise to stop this act immediately by passing the information technology act. To tune in with the increasing cyber crimes, we needed a firm legal infrastructure to match the parallel needs of society signifying the lowering of the crimes. Hence, cyber laws came Into effect in order to stop these crimes and match the pace of illegal activities. Cyber laws in India were implemented in order to show a red flag to emerging cyber crimes. The hour of emergency was demanding some firm legal infrastructure in order to lower the crime rate surrounding cyberspace. Cyberspace includes computers, emails, networks, phones, electronic devices, Atm, data storage devices, etc. cyber law deals with cyber crimes, electronic or digital signatures, intellectual property, and data protection and privacy. In cybercrime, the computer is used as a tool for committing these crimes with the help of telecommunication technology.

LAWS IMPLEMENTED TO MONITOR CYBERCRIME

The Computer Fraud and Abuse Act of 1986[2] was the first cyber law ever to be enacted. It prohibits unauthorized access to computers as well as the misuse of digital data. In India, cyber

[2] Computer Fraud and Abuse Act 1986

crimes are governed by the Information Technology Act of 2000[3] and the Indian Penal Code of 1860.[4] The legislation that deals with issues related to online crime and internet trading is the Information Technology Act of 2000. However, a term and penalty for cybercrime were added to the Act in 2008. The Reserve Bank of India Act and the Indian Penal Code 1860 were also amended. The Information Technology Act's Section 67(B)[5] stipulates that it is forbidden to produce or distribute any electronic content that depicts youngsters acting in a sexually explicit manner[6].

INFORMATION TECHNOLOGY ACT, 2000 (IT ACT): OVERVIEW OF THE ACT

Important Provisions of the Act:

It is the first cyber law that the Indian Parliament has approved. . "To facilitate electronic filing of documents with Government agencies, to supply legal recognition for transactions carried out by electronic data interchange and other means of electronic communication, commonly mentioned as electronic methods of communication and storage of information, and further to amend the Indian legal code, the Indian Evidence Act, 1872,[7] and therefore the Banker's Book Evidence Act, 1891.[8]

The IT Act may be a significant part of the overall Indian legal system since it governs how cybercrimes are investigated and prosecuted. the acceptable sections are as follows:

Section 43[9]: This section of the IT Act applies to anyone who commits cybercrimes, like harming the victim's computer without the victim's express authorization. If a computer is broken in such a case without the owner's permission, the owner is totally entitled to our funds for the whole damage.

---

[3] Information Technology Act 2000
[4] Indian Penal Code 1860
[5] Information Technology Act 2000, s 67B
[6] Nikung Arora, 'Cyber Crime Laws in India' (*Ipleaders*, 28 April 2022) <https://blog.ipleaders.in/cyber-crime-laws-in-india/> accessed 18 September 2022
[7] Indian Evidence Act 1872
[8] Banker's Book Evidence Act 1891
[9] Information Technology Act 2000, s 43

Rajesh Aggarwal of Maharashtra's IT department, who served because the case's representative, ordered Punjab commercial bank to pay Rs 45 lakh to Manmohan Singh Matharu, the MD of Pane-based company Poona Auto Ancillaries, in Poona Auto Ancillaries Pvt. Ltd., Pune v Punjab commercial bank, HO New Delhi & Others (2018). In one instance, a fraudster used Matharu's account at PNB, Pune, to transfer Rs 80.10 lakh after the latter skilled a phishing email. The complainant has requested to touch the liability because they opened the phishing email. However, it had been determined that the bank was incompetent because no security checks were made against accounts that had been formed fraudulently to mislead the complainant. Any dishonest or fraudulent behavior covered by Section 43 is roofed by Section 66[10]. In such cases, the utmost penalty is three years in prison or a fine of Rs. 5 lakh.

Section 66: Applies to any conduct described in Section 43 that's dishonest or fraudulent. There are often up to three years of imprisonment in such instances, or a fine of up to Rs. 5 lakh. In Kumar v Whiteley (1991),[11] the accused acquired illegal access to the Joint Academic Network (JANET) throughout the investigation and modified, added, and removed files. Investigations revealed that Kumar had been accessing BSNL broadband Internet connections under the guise of a legitimate authorized user and altering computer records relevant to subscribers' broadband Internet user accounts. The CBI launched an inquiry into Kumar after discovering unlawful use of broadband Internet on his computer, which was the inspiration of an anonymous allegation. The subscribers also lost Rs 38,248 as a result of Kumar's wrongdoing. the extra Chief Metropolitan Magistrate condemned N G Arun Kumar. Following Sections 420 of the IPC[12] and 66 of the IT Act[13], the magistrate sentenced him to a stern year in prison and a fine of Rs 5,000.

Section 66B: This section outlines the results of receiving computer or communication equipment that has been unlawfully obtained, and it confirms a possible three-year jail sentence. A fine of up to Rs. 1 lakh can also be imposed, counting on the severity. Digital signatures,

[10] Information Technology Act 2000, s 66
[11] Hema Modi, 'All you need to know about hacking' (*ipleaders*, 23 October 2021) <https://blog.ipleaders.in/all-you-need-to-know-about-hacking/> accessed 18 September 2022
[12] Indian Penal Code 1860, s 420
[13] Information Technology Act 2000, s 66

password hacking, and other sorts of identity theft are the main topics of Section 66C. This section carries a fine of 1 lakh rupees and a maximum sentence of three years in prison.

Section 66D[14]: This section deals with impersonating somebody else while using computer resources to cheat. If found guilty, the penalty carries a maximum three-year prison sentence also as a maximum fine of Rs. 1 lakh.

Section 66E[15]: Violations of this section include publishing or transmitting images of personal spaces without the owner's permission. If found guilty, the penalty carries a maximum three-year prison sentence also as a maximum fine of Rs. 1 lakh.

Section 67[16]: This deals with publishing obscenities online. If found guilty, the utmost sentence is three years in prison, and there's also a potential fine of Rs 2 lakh.

The following IPC sections may be used by law enforcement agencies if the IT Act is insufficient to address particular cybercrimes:-

Section 292[17]: Although the first intent of this clause was to combat the sale of pornographic materials, it's since developed to cover a variety of cyber offenses as well. This clause also applies to how pornographic or sexually explicit activities or exploits of kids are publicized or distributed electronically. Such offenses are punishable by up to 2 years in jail and fines of Rs. 2000. For repeat (second-time) offenders, any of the aforementioned crimes may end in a sentence of up to five years in jail and a fine of up to Rs. 5000.

Section 354C[18]: According to this law, photographing or publishing images of a woman's private or intimate acts without her agreement constitutes cybercrime. Voyeurism is the only topic covered in this section because it is illegal to watch a woman engage in sexual activity. Sections 292 of the IPC and Section 66E of the IT Act are broad enough to include offenses of a similar character in the absence of this section's essential components. First-time offenders may

[14] Information Technology Act 2000, s 66D
[15] Information Technology Act 2000, s 66E
[16] Information Technology Act 2000, s 67
[17] Indian Penal Code 1860, s 292
[18] Indian Penal Code 1860, s 354C

receive a sentence of up to three years in jail, while repeat offenders may receive a sentence of up to seven years.

Section 354D[19]: This chapter describes and penalizes stalking, including both physical and online stalking. Cyberstalking is the practice of following a woman through technology, such as the internet or email, or making contact with her despite her lack of interest. For the first offense, this crime carries a maximum sentence of 3 years in jail; for the second offense, it carries a maximum sentence of 5 years in prison and a fine.

Section 379[20]: In addition to a fine, theft is punishable by up to three years in prison under this section. The IPC Section is relevant in part because many cybercrimes involve stolen computers, data, or electronic equipment.

Section 420: In this section, it is discussed how to induce the delivery of property dishonestly and through deceit. Under this clause, cybercriminals who commit offenses including fabricating websites and conducting online fraud face a seven-year prison sentence in addition to a fine. This part of the IPC deals with offenses including creating phony websites or stealing passwords for financial gain.

Section 463[21]: This section deals with electronically fabricating documents or records. Under this clause, spoofing emails is punishable by up to 7 years in prison and/or a fine.

Section 465[22]: This clause often addresses how forgery is punished. Under this section, offenses like email spoofing and creating false documents online are dealt with and punished with up to two years in prison, fines, or both.

Section 468[23]: A seven-year prison term and a fine may be imposed for fraud committed with the purpose to defraud. This section also punishes email spoofing. In the 2005 case of Anil

[19] Indian Penal Code 1860, s 354D
[20] Indian Penal Code 1860, s 379
[21] Indian Penal Code 1860, s 463
[22] Indian Penal Code 1860, s 465
[23] Indian Penal Code 1860, s 468

Kumar Srivastava v Addl Director, MHFW, the petitioner falsely signed the AD's signature before filing a case that contained untrue accusations against the same person. The Court determined that the petitioner was accountable under Sections 465 and 471 of the IPC since he also tried to pass it off as a legitimate document.

Due to the overlap between the provisions of the IPC and the IT Act, certain offenses may wind up being bailable under the IPC but not under the IT Act and vice versa, or perhaps compoundable under the IPC but not under the IT Act and vice versa. For instance, offenses under sections 43 and 66 of the IT Act are bailable and compoundable if the behavior involves hacking or data theft, whereas offenses under sections 378 and 425 of the IPC are neither bailable nor compoundable. Additionally, if the crime involved receiving stolen goods, section 66B of the IT Act applied instead of section 411 of the IPC, which did not allow for bail. In a similar vein, under sections, 66C and 66D of the IT Act, the crimes of identity theft and defrauding by personation are punishable by a combination of fines and time in jail, although they are not for crimes under sections 463, 465, and 468 of the IPC and are not subject to bail. The Bombay High Court addressed the dispute between offenses that are not bailable and not compoundable under Sections 408[24] and 420 of the IPC and those that are under Sections 43, 65, and 66 of the IT Act in Gagan Harsh Sharma v The State of Maharashtra (2018).

LACUNAE IN CYBER LAW

The entire workforce has gone digital with the advent of the twenty-first century, including, among other things, banking, online shopping, and purchases. But one crime is quickly gaining ground in this digitally advanced society: cybercrime. Cybercrime is a type of criminal activity where hackers utilize computers as their main tool. They use the private information of consumers for evil reasons. Cybercrime is sometimes referred to as hacking, phishing, or spamming. The Indian Cybercrime Act (ITA-2000), which addresses e-commerce and cybercrime, has many flaws. Since the adoption of the cyber law, cybercrime has increased in

[24] Indian Penal Code 1860, s 408

India but has not decreased. An Act of India (No 21 of 2000) was notified on October 17, 2000, and that Act is known as the Information Technology Act of 2000.

It is the primary piece of legislation in India covering electronic commerce and cybercrime. During the 2000 budget session, on June 9, President K.R. Narayana signed the measure. The bill was completed by a team of officials under the direction of Pramod Mahajan, who was then the minister of information technology. The Act gives "electronic commerce," which includes the exchange of data electronically and other types of electronic correspondence, legal character. Under the IT Act, there is no such thing as a data breach. Only "body corporates" may collect and disseminate information within the restrictions of the IT Act. The general rule that surveillance should only be conducted in situations of public emergency or public safety is not included in the IT Act. A person or intermediary who refuses to help the designated entity with the interception, surveillance, or disclosure of the information is also liable to criminal penalties, according to section 69 of the IT Act. Information stored in a digital resource that has been decrypted or disclosed is punishable by up to seven years in prison and a fine. The IT Act doesn't define the term "consent."

Puneet Bhasin, a digital law expert, was interviewed by Computer World India. He warns against passively "discussing" the ideal law amid ongoing threats to information security. Bhasin explains that the bill is a wonderful piece of legislation that emphasizes the value of viewing information as public property through the information limitation rule. Puneet Bhasin discusses several issues during her lecture, including the data breach that occurred at the Facebook and WhatsApp offices, how they could have been so irresponsible, and who will be held accountable. She has accurately characterized the value of data, and data localization can aid in reducing the everyday data breaches that cause consumers to lose their important data and make the data vulnerable to leaking. Additionally, she states that the government will not feel the need to change the current measure until a significant data leak occurs, at which point it will not be considered. The only way the Act can be improved with upcoming modifications is if the government takes data leaks more seriously and investigates every minor to the major case that arises.

LANDMARK CASES

Avnish Bajaj vs State (Bazee.com case)

The CEO of Bazee.com was detained in December 2004 after a CD with questionable content was sold on the website. Additionally, the CD was accessible in Delhi's markets. The police forces from Mumbai and Delhi were dispatched to the area. The CEO eventually received a parole discharge. The issue of how to distinguish between Internet Service Providers and Content Providers was brought up by this. The onus is on the accused to demonstrate that he was indeed the service provider and not the content provider. It also raises several issues regarding how law enforcement should handle cybercrime situations.

Ambiga vs The Additional Chief Secretary

The detainee filed a bail appeal with the learned Principal Sessions Judge in Cr.M.P.No. 1772 of 2019; the equivalent was dismissed on August 8, 2019. The Detaining Authority marked him as a Cyber Law Offender and imprisoned him under the provisions of the Tamil Nadu Act 14 of 1982, by cinching the reproved request of detention and testing the legitimacy of the equivalent, the present Habeas Corpus Petition is documented. The Detaining Authority, on scrutiny and thought of the materials, has inferred the abstract fulfillment that the detenu's activities were biased to the upkeep of the public request. The petitioner then proved that Thiru Saravanan, a child of Chinnathambi, is breaking the law and operating in a way that is biassed against maintaining public demand, and as a result, he (Thiru Saravanan) is a "Digital Law Offender" as considered under section 2(bb) of the Tamil Nadu Act 14/82. He has caused fear, alertness, and a sense of weakness in the characters of those in the area by committing the infractions shown above, and as a result, he has acted in a way that is biased against maintaining public order.

Yogesh Kumar Sharma vs The State of Jharkhand

The lawyer is accused in connection with Jamshedpur Cyber Crime P. S. Case No. 01 of 2020 in comparison to Cyber Crime Case No. 18 of 2020, both of which are filed under Sections 419, 420,

467, 468, 471, 34, and 66(C), (D) of the Information Technology Act and are scheduled to be heard by Additional Sessions Judge-II, Jamshedpur. However, I have now discovered that the A.P.P. has rejected the bail petition. Given the information in the file, the pre-conviction period of custody, and the fact that other co-accused have successfully been granted bail, the candidate is scheduled to be released on bail upon furnishing a bail obligation of Rs. 10,000/- (Ten Thousand specifically), with two guarantees of the same sum each, under the general preference of took in Additional Sessions. Regarding Jamshedpur Cyber Crime P. S. Case No. 01 of 2020 about Cyber Crime Case No. 18 of 2020, Judge-II, Jamshedpur, subject to the conditions that (I) one of the bailors ought to be his direct relations, and (ii) the applicant will report to the concerned police headquarters once every month until the conclusion of the Trial and (iii) under the watching eye of the learned court, the attorney will provide a self-confirmed copy of his Aadhar Card and also provide his mobile number. Right now, there is still time to address the problem that is making news due to misconduct. If we start airing news stories about cybercrime, start treating it seriously, and start educating people about it as well as advising them to make their records private and secured by the security software, this would also help to reduce the number of incidents. If we were to make our discipline more grounded and instill fear in programmers' minds, these programmers could think twice before engaging in this transgression. Making it mandatory to educate children about information security is important because it will help them develop the skills essential to fight cybercrime and make good decisions in the future. One additional thing that needs to be kept in mind is that we need to deal with information security escape clauses and fill out these conditions so that it can gradually recover**.**

EVOLUTION OF CYBER LAW IN INDIA

As we know that cybercrime is the biggest crime not in our country but in all countries. Keeping in view all these cyber crimes after independence, the first law made by the government of India is the computer fraud and abuse act of 1986. A law was made by the govt. of India against cybercrime. Due to the non purely implementation of that law, they took a different step and introduced the Information Technology Act, 2000, and the Indian Penal Code, 1860.

Recently, In order to create a "comprehensive legal framework" for policing the online world, the government withdrew the Personal Data Protection Bill from Parliament. Separate regulations on data privacy, the internet ecosystem as a whole, cyber security, telecom rules, and the use of non-personal data to promote innovation in the country are all included in this framework. This comes after the Bill was in development for almost four years, during which time it underwent numerous revisions, was subjected to a Joint Committee of Parliament (JCP) assessment, and encountered opposition from a variety of parties, including tech corporations and privacy campaigners. The government intends to introduce the new legislation during the winter session of Parliament, according to sources in the IT Ministry. According to a senior official, the revised Bill would take into account the JCP's recommendations for stronger data protection and will be consistent with the Supreme Court's historic 2017 ruling that declared privacy to be a fundamental right. The official stated that it was necessary to completely redraft the outline of the legislation due to the JCP's substantial number of requested revisions. The data protection Bill has been in development since 2018, when a group headed by Justice B N Srikrishna, a former Supreme Court judge, produced a draught of the Bill. Following that, it was examined by a JCP, which in November 2021 gave its recommendations along with a draught Bill. Union IT Minister Ashwini Vaishnaw explained the rationale behind the bill's withdrawal in a note distributed to all lawmakers, stating, "The Personal Data Protection Bill, 2019 was examined in great detail by the Joint Committee of Parliament. 12 proposals and 81 changes were put out in an effort to create a thorough legal framework for the digital economy. In light of the JCP report, a comprehensive legislative framework is being created. Given the situation right now, it is advised that "The Personal Data Protection Bill, 2019" be withdrawn and replaced with a new Bill that complies with the overall statutory framework. A minister of state for information technology named Rajeev Chandrasekhar stated that the administration will "very soon" present new legislation in Parliament. The government has withdrawn the Personal Data Protection Bill, which was created in 2018 and updated by the JCP in 2021.[25]

[25] Soumyarendra Barik, 'Government withdraws data protection bill to bring revamped, refreshed regulation' (*Indian Express*, 4 August 2022) <https://indianexpress.com/article/india/government-withdraws-data-protection-bill-8068257/> accessed 19 September 2022

Withdrawn (introduction December 11, 2021) personal data protection bill, 2019. While promising to come back with a new draft.

AN OVERVIEW OF CYBERCRIME

Since computer systems have become a crucial component of businesses, organizations, governments, and people's daily lives, we have learned to put a lot of reliance on them. We've given them access to highly important and priceless information as a result. History has shown that valuable items have always been a target for criminals. Cybercrime is no different. Consumers give a target for thieves to aim at to profit from the activity as they load their personal computers, phones, and other gadgets with valuable information. In the past, a criminal would need to carry out some sort of robbery to gain access to a person's belongings. When data is stolen, the criminal must break into the facility and look through the files for the most precious and lucrative information. Because of the nature of the internet, criminals may now assault their victims from a distance, and these actions are unlikely to result in punishment today.

CYBERCRIME IN 70S AND 80S

The tone mechanism used on phone networks in the 1970s was abused by criminals. The attack, known as "phreaking," entailed the assailant reverse-engineering the long-distance call tones of the telephone providers. In 1988, the first computer worm that affected businesses appeared on the internet.[26] The first worm was called the Morris worm after its creator, Robert Morris. Even though this worm wasn't intended to be malicious, it still caused a lot of harm. The United States Government Accountability Office estimated that the damage could have cost up to $10,000,000.00 in 1980. In 1989, the healthcare industry was the victim of the first known ransomware attack. A type of harmful software called ransomware encrypts and locks a user's data until a small ransom is paid, at which point a cryptographic unlock key is sent. Evolutionary researcher Joseph Popp sent 20,000 floppy discs to 90 countries, claiming they

[26] 'Evolution of cybercrime' (*Packt*, 29 March 2018) <https://hub.packtpub.com/the-evolution-cybercrime> accessed 19 September 2022

included software that could be used to analyze a person's risk factors for contracting the AIDS virus. On the other hand, the CD contained malware that, when activated, displayed a message asking for payment for a software license. With the healthcare sector remaining a key target, ransomware attacks have evolved dramatically over time.

WEB'S INCEPTION AND THE COMMENCEMENT OF A NEW ERA FOR CYBERCRIME

In the 1990s, email and the web browser became extensively used, giving hackers additional tools to use. As a result, the cybercriminal was able to significantly expand their reach. Until the cybercriminal had to make a physical transaction, like giving a floppy disc, for example. These modern, highly vulnerable web browsers could now be used by cybercriminals to spread virus code online. Cybercriminals used their previous knowledge to operate online, which had terrible effects. Cybercriminals were also able to con people from a distance thanks to phishing attacks. One-on-one interactions with people were no longer necessary. You may try to deceive millions of users at once. You may still earn a sizable sum of money as a cybercriminal even if just a small proportion of people fell for the trap. Identity theft and social networking both began to take off in the 2000s. Due to the development of databases containing millions of users' personal identifying information, identity theft has evolved into the new financial piggy bank for criminal organizations around the world (PII). Due to this information and the general public's ignorance of cybersecurity, hackers were able to commit several financial crimes, including opening credit cards and bank accounts in other people's identities.

CYBERCRIME IN A QUICK-CHANGING TECHNOLOGICAL ENVIRONMENT

In recent years, cybercrime has only gotten worse. As computer systems have become faster and more complex, we have observed that cybercriminals have become more skilled and challenging to catch. To control millions of infected computer systems around the world, criminals have already become accustomed to using botnets, which are networks of private computers that have been infected with malicious software. These botnets give hackers the ability to overwhelm corporate networks while hiding their origins: Ransomware attacks are ongoing in every sphere of the economy. People are always on the watch for financial fraud and identity theft. The most

recent point-of-sale attack against large merchants and hospitality groups has been the subject of ongoing news headlines. Globally, organizations are trying to thwart these attacks in some way.

On the other hand, hackers are one step ahead of the game because of their always-evolving and innovative approaches. Future information security specialists, however, will defend us and help us create a safer online environment. Internet users need to supply a few necessities to be ready for the upcoming wave of cybercrime. Antivirus software is a useful first step in keeping computers secure, but recognizing current threat trends may also help you prevent your data from being viewed by unauthorized people.

With over 6.7 lakh cases already documented in 2022, the Center claimed that there has been a significant increase in cybersecurity-related risks in India. A total of 6,74,021 cyber security incidents have been registered this year, the administration informed the Lok Sabha on Wednesday. Ajay Kumar Mishra, the Union Minister of State for Home, informed the Lok Sabha that the government issues alerts and advisories regarding the most recent cyber threats and runs an automated cyber threat exchange platform for proactively gathering, analyzing, and sharing tailored alerts with organizations across sectors for proactive threat mitigation actions. Before being hosted, all government websites and applications are subject to a cyber security audit. The Cyber Swachhta Kendra, which alerts the government to harmful software and free tools, is also run by the government. According to the minister, the government has provided chief information security officers (CISOs) with instructions regarding their primary tasks and duties for securing applications, infrastructure, and compliance. In 2019, 2020, and 2021, respectively, there were reported 3,94,499, 11,58,208, and 14,02,809 cyber security incidents, according to data compiled by the Indian Computer Emergency Response Team (CERT-In).[27]

[27] 'India records 36.29 lakh cyber security incidents since 2019 till June this year, says Govt' (*The Economic Times*, 19 July 2022) <https://economictimes.indiatimes.com/news/india/india-records-36-29-lakh-cyber-security-incidents-since-2019-till-june-this-year-says-govt/articleshow/92980278.cms> accessed 19 September 2022

MEASURES TO PREVENT CYBER CRIMES

Due to the transnational character of cybercrimes, creative solutions are needed to address the problem of technological crime. Therefore, in addition to respecting the Cyber Laws, one should bear in mind the following things to ensure their safety when using the Internet:

- Every person should become more knowledgeable about cybercrimes and cyber laws and should be made aware of them. Students in computer centers, schools, colleges, and universities should also receive instruction in cyber literacy. Any educational institution can host a cyber law awareness workshop to teach students the fundamentals of the internet and its security.
- In order to lessen the effects of identity theft and crimes committed online, it is advisable to regularly monitor bank and credit card statements.
- Keep your operating system updated to deter hackers from accessing your computer. By keeping your computer updated, you can stop attackers from taking advantage of software flaws that could otherwise give them access to your system and allow them to hack it for illegal purposes.
- For online activities like online banking, it is best to use eight-character strong passwords that are both unique and secure. Avoid using passwords that are easily traceable, such as your email address, login name, last name, date of birth, or month of birth.
- You shouldn't use the same password for each online service you use. Keep various passwords on hand for various internet activities.
- To secure your webmail or social media account, enable two-step authentication in the webmail. Add your cell phone number to your email account so you can be alerted if someone tries to access your account. Your username and password are necessary to open your account with two-step authentication. However, for your personal protection, a verification code is sent to your listed mobile number if you forget your password. Even if a hacker is able to guess your password, he or she will be unable to access your account without the temporary verification code.

- Your computer needs security software installed since it helps shield you from online threats and is therefore necessary for basic online security. These programs are therefore essential for maintaining online safety. It comes with a firewall and anti-virus software. The firewall regulates who and what is able to communicate with your computer over the internet. By maintaining all online activities, including email and web browsing, antivirus safeguards the machine against viruses, worms, Trojan horses, and other malicious programs. Since they provide all the security software required for online protection in a single package, integrated security programs like Norton Internet Security, which combines Firewall, Antivirus, Antispyware, and other features like Antispam and parental controls, have gained popularity in recent years.
- Responding to emails that request personal information or clicking on the links in them could lead you to phony and harmful websites. Read the privacy policies on a company's website and software before you give them your data. You won't receive emails from trustworthy businesses requesting personal information

CONCLUSION

India is one of the most densely populated countries in the world with accumulating wealth and a firm base in the development era. To accommodate peace and harmony in this emerging population a well defined legal system is to be defined in the place. Many laws have been enacted and then amended to the arising need of the crimes prevailing in society. The foremost law is the constitution of India. Every law made in India is discussed with the relevance of social, political, economical, and cultural scenarios of the ongoing time. However, the beginning of the internet led to the arrival of new, unexpected, and complex legal issues. Nobody could anticipate the arrival of internet crimes and thus it was impossible for the draftsmen of our laws to visualize the need of cyber laws in the country. Despite having acumen brains and cognitive abilities they were not aware of the idea that the internet invention we all are proud of can also turn into a disadvantaged face of society leading to crimes and illegal activity happening via the computer and electronic devices. Hence enactment of new relevant laws was in need to cope up with the emerging cyberspace. The information technology act was made to give legal

recognition to the laws pertaining to internet misconduct and provide protection to the victims of computer-based crimes. This internet technology is widely used in different parts of the world and this law ensures security procedures for the citizens of India. This paper focuses on the evolution of cyber laws to provide legal security and put a stop to the steady growth of these crimes. Cyber crimes touch all aspects of illegal transactions, unauthorized computer trespassing, stealing secret information and data, the transmission of obscene material, and computer vandalism, and also cyber crimes are done against persons, property, and government.

India is turning into a digitalized world now and everybody is getting dependent on computers and internet devices to keep their valuable data. Technology is like 2 sides o the coin but now the evil side is what coming to notice, hence it is the duty of governing law-making bodies should ensure that technological advancement over the internet should run in a healthy manner and divert the invention into legal as well as a right entity. Cyber laws came into being for the surreal running of our country in good deeds. It's very important for our country to have control over the increasing crime rate to ensure safety and a protective environment where citizens feel proud to live but not in a fear of getting trapped in this vicious circle of criminal conduct. Laws are made with the view that citizens of our country can sleep peacefully and hence observe the destructive activities in the ongoing state. Evolution is very important in every aspect either laws, technology, etc to match the growing needs of society as time changes everything.