ISSN: 2582 - 2942

LEX FORTI

LEGAL JOURNAL

VOL- I ISSUE- V

JUNE 2020

ISSN: 2582 - 2942

DISCLAIMER

ISSN: 2582 - 2942

EDITORIAL BOARD

ISSN: 2582 - 2942

EDITORIAL BOARD

ISSN: 2582 - 2942

ABOUT US

LEXFORTI IS A FREE OPEN ACCESS PEER-REVIEWED JOURNAL, WHICH GIVES INSIGHT UPON BROAD AND DYNAMIC LEGAL ISSUES. THE VERY OBJECTIVE OF THE LEXFORTI IS TO PROVIDE OPEN AND FREE ACCESS TO KNOWLEDGE TO EVERYONE. LEXFORTI IS HIGHLY COMMITTED TO HELPING LAW STUDENTS TO GET THEIR RESEARCH ARTICLES PUBLISHED AND AN AVENUE TO THE ASPIRING STUDENTS, TEACHERS AND SCHOLARS TO MAKE A CONTRIBUTION IN THE LEGAL SPHERE. LEXFORTI REVOLVES AROUND THE FIRMAMENT OF LEGAL ISSUES; CONSISTING OF CORPORATE LAW, FAMILY LAW, CONTRACT LAW, TAXATION, ALTERNATIVE DISPUTE RESOLUTION, IP LAWS, CRIMINAL LAWS AND VARIOUS OTHER CIVIL ISSUES.

Cybercrime- A new threat to the society

Kritika Mundra

INTRODUCTION

The use of internet in Indian economy as well as the world economy, has changed the way of doing business. The role of internet has become vital in today's world. It has become a mode of communication with one another, a way for consumers to communicate with a service company. The growth of internet has led to new opportunities in every field of life. It has many advantages but the internet also has many disadvantages. One of the serious disadvantages of the use of internet is Cyber Crime. It is an illegal activity which is committed over the internet. There are various kinds of cyber-crimes that are committed now a days like credit card frauds, e-mail spying, software piracy and so on. Cyber Crime is a crime which is committed over the internet by using computer and another electronical tool. It is an illegal activity committed by someone having a professional skill for the for the purpose to gain an unfair advantage over some other person due to that deception or misrepresentation. Lack of cyber security increases the vulnerability to criminals to disrupt or interrupt with the business deals in various ways. Cyber criminals can involve in activities like denial of certain services, false online applications for various kinds of bank loans, extracting credit or debit card information for the purpose of selling or buying goods or services. As the use of internet has enabled the people all over the world to conduct business transaction beyond borders, it has become more difficult to investigate and prevent the happening of such crimes.

Thus, we can say that cyber law is constantly evolving over time. With the growth of the internet, some more important issues are coming up relating to the jurisdiction, growth of cybercrimes, admissibility of electronic transaction and many more.

The advent of the digital economy and technology, has provided various opportunities because cyberspace provides mediums through which work can be done in a significant and efficient manner. The advancement of the internet and digital technology has been a boon to the students, doctors, lawyers, teachers and even to the criminals. Unauthorised access of the internet and damage to one's property and distribution of obscene pictures and indecent materials lead to cybercrimes. The internet has become a part of life for billions of people. However, these advancements have been transformed into a shelter for criminals. So far as cyberspace is concerned, hijacked emails and frauds are being done and used as a way for fraud by cybercrimes.

MEANING OF CYBERCRIME

Crime is not a legal term. It derives it meaning in the backdrop of the society than the State as such. However, the word crime is generally used as a synonym for a 'wrong', 'an offence', or 'a felony'. Crime is an economic as well as a social phenomenon. It is an old and historical subject. Many ancient books, right from the pre-historic days and many mythological stories have discussed and spoken about crimes committed by individuals like ordinary theft, burglary, kidnapping, or against the whole nation at large like treason and so on.

Assuredly, the information and communication progress in the country has led to emergence of a new kind of crime which is known as Cyber Crime. For proper understanding to the term Cyber Crime, we must clearly understand the term crime first and then go to the term cybercrime.

The dictionary meaning of crime states that it is an action or omission which constitute an offence and is punishable under the law of the country. According to Merriam Webster Dictionary, Crime is an forbidden act or omission of duty, if committed makes the offender punishable under the Law-A gross violation of law.[1] Blackstone defines crimes as an act omitted or committed in violation of law. Stephen defined Crime as a violation of a right in reference to the evil tendency of such violation in respect of the community at large.

The increase in the internet network and the swift communication and information provided by it comes with a cost. The cost here means the crimes which is related to the internet, i.e., cybercrimes. These crimes involve the use to computer network.

The word 'Crime' has not been defined either in the Information Technology Act,2000 or the Information Technology (Amendment) Act, 2008 and neither in any legislation or law in the country. The word 'Offence' has been in the Indian Penal Code,1860. Cybercrimes means crimes associated with computer networks. Thus, we can say that, a crime or an offence in which computer network can be used is called Cyber Crimes. Consequently, even a small offence like stealing can also be covered under the purview of Cybercrime if the information is stored in the computer and such data is used by the offender to commit stealing. The information technology Act, 2000 defines words like computer, information, computer network data, that forms an important part of Cybercrime.

[1] https://www.merriam-webster.com/dictionary/crime, accessed on 1st June,2020

According to Council of Europe Convection on Cybercrimes, to which US is a signatory, defines Cybercrime as a wide range of spiteful activities, including illegal interception of data network, system interferences that compromise network integrity, and copyright infringement.[2]

In accordance to the Information Technology Act, 2000, a Cybercrime can be defined as an offence which is punishable under the Information Technology Act,2000. However, this cannot be concluded to be a conclusive definition because there are various provisions in the Indian Penal Code,1860 which also talks about Cybercrimes like email spoofing, cyber defamation and so on. In such kind of crimes, the basic objective of the offenders is to target the computer networks or data itself and hack or forge the essential information.

ESSENTIALS OF CYBERCRIMES

The definition of crime is a subject matter of difficulty as there is no precise definition for it. There is a basic principle in criminal law, i.e., the person may not be convicted for a crime unless the prosecution has proven his guilt beyond reasonable doubt. It has to be proved that:

1. He has caused the event or is responsible in the happening of it., and such event or action is forbidden by the law of the country.
2. He has a state of mind in relation to that action or event.

Thus, there are 2 basic essentials of crimes, namely, Actus Reus and Mens Rea. This basic essential is even need to be proved in Cybercrimes.

Thus, before convicting a person not only acuts reus but also mens rea has to be proven beyond reasonable doubt by the prosecution. If A Killed D and actus reus is done, before convicting A, mens rea also needs to be proved. In a case of **Woolmillgton V. Director of Public Prosecution,**[3] The House of Lords in this case stated that not only the jury must be just satisfied that A's defence is not true and this 'not true' has to be proven beyond doubt.

Actus Reus in Cybercrimes:

Actus reus in internet crimes or Cybercrimes is easy to identify but it is not easy to prove in court of law. The word actus means deed. Actus reus is a human conduct as the law seeks to prevent. It

[2] https://searchsecurity.techtarget.com/definition/cybercrime, accessed on 1st June,2020
[3] 1935 AC 462

is not only the conduct but also includes the consequences and circumstances.[4] The fact of the occurrence of the action is said to be as a crime when the person is:

- Trying to use and make a computer function or work.
- Trying to get the access of the data which is stored in a computer.
- When a person uses the internet to get access over the computer and then make these computer function according to his (unauthorised user) command.
- Attempting to login even if the unauthorised user has failed many times. [5]

To prove Actus reus in Cybercrimes is becoming a challenge as the entire set of action is committed in intangible surroundings.[6] The hackers may leave some footprint back in the machine itself, though it may become a tedious task for the law-enforcers to prove that in the court, as something has to be in physical form in order to be admissible in the court as evidence.

Mens Rea in Cybercrimes:

Another most essential condition for a crime to take place is Mens rea. It indicates the intention of the accused for the commission of the crime for which he is charged.[7] It must be proved that the accused had knowingly committed such a crime. In case of Cybercrime, for determining Mens rea on the part of the accused is that the accused must be aware that at the time of causing someone else computer function or work is done in an unauthorised manner and his access is unauthorised. There must be an intention to access the computer though he may have intention to access any computer not any particular computer. His intention to get secure access need not to be directed at any particular kind of, programme or data. It should be enough that the hacker intended to secure access to the programmes as per S-18 of the Information Technology Act, 2000. There are 2 main essentials for the application of mens rea, they are:

1. The access by the Hacker should be unauthorised.
2. He must be aware of the same at the time when he is trying to get secure access of the computer.

The second essential becomes easier to prove in the court if the hacker is a person who has no authority to get access over the data stored in the computer but again this essentials becomes difficult to prove if the hacker is a person who has limited authority to access the computer.[8]

---

[4] https://blog.ipleaders.in/mens-rea-actus-reus-essentials-crime/, accessed on 1st June,2020
[5] the hacker attempts to use the password himself, but fails owing to the remote computer allowing only one login each day. This would still be actus reus.
[6] https://shodhganga.inflibnet.ac.in/bitstream/10603/7829/12/12_chapter%203.pdf, accessed on 1st June,2020
[7] https://blog.ipleaders.in/mens-rea-actus-reus-essentials-crime/, accessed on 1st June,2020
[8] https://shodhganga.inflibnet.ac.in/bitstream/10603/7829/12/12_chapter%203.pdf, accessed on 1st June,2020

With the advent of Cybercrimes, the legal world has faced difficulty to prove Mens rea in Cybercrimes. In Cybercrimes, one should pinpoint what the state of mind of the hacker was at the time he was trying to get secured access and that he knew he was unauthorised to do so.
Hence, there is no need that the intention has to be related to a particular computer, it would be enough to prove that it was an unauthorised access.
Consciousness on the part of the hacker becomes easy to prove if he is an outsider and has no authority to access. But in cases where the hacker has limited or little authority to access the computer like in cases where he is an employee of a company, it becomes difficult to state that he has exceeded his limits and was even aware of that he is exceeding his limit.

CLASSIFICATION OF CYBERCRIMES

1) Cybercrimes against Person(s)

There are various kinds of offences which can be committed against an individual person. These Cybercrimes consist of:

1. **Cyber Stalking and Harassment**: Cyber Stalking means following a person and the movement through the individual activity over the internet. Cyber Stalking is a way in which the attacker harasses the victim using electronical technologies like e-mail, instant messages, video and photo sharing and so on. The attacker also known as the cyber stalker, relies upon the obscurity enabled by the internet which allows him to stalk or follow the movement of the victim without being detected by the victim. The term Cyber stalking has not been defined in any legislation in the country. But the word Stalking has been defined **under S- 354D of the Indian Penal Code,1860**. In this case, stalking means following a person physically and through any electronic means. This kind of stalking is done by the offender just to instil fear in the minds of the victim. While, cyberstalking and cyber harassment is done in order to damage an individual's reputation and results in more severe physical as well as emotional harm.[9]

Stalking and Harassment both are malicious activities which are directed to be committed against a particular person. As these activities are committed over the computers, S-66, 66A, 67 of the Information Technology Act, 2000 cover these kinds of issues. S-66 of the Information Technology Act, 2000 states that, "If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three

[9] https://www.tripwire.com/state-of-security/security-awareness/what-cyberstalking-prevent/, accessed on 1st June,2020

years or with fine which may extend to five lakh rupees or with both."[10] S-43 of the Act states that if any person tries to access a computer or computer network, without the permission of the owner, they will be liable to pay compensation to the person affected. The offence of hacking is covered herein.[11]

S-66A of the Act (now repelled) provides that, "Any person who sends, by means of a computer resource or a communication device -

(a) any information that is grossly offensive or has menacing character; or

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device; or

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages,

shall be punishable with imprisonment for a term which may extend to three years and with fine."[12] S-66A of the Information Technology Ac, 2000 was so vague that the law enforcement could and did, interpret opinions liberally in a manner of putting the citizens behind the bars. By repealing this section, India took a step towards the maturing of democracy principles.[13]

In the landmark case of, **Shreya Singhal V. UOI,**[14] the Supreme Court held that S-66A was vague and stood be struck down and was not saved by Art. 19(2) of the Indian Constitution on account of the words used in the section such as 'annoying', 'causing annoyance', 'grossly offensive'. The court considered considered the 1st two words fall within the freedom of speech

and expression under Art 19(1)(a) of the Indian Constitution and held that it was just an incitement which attracted the Art 19(2) Of the Constitution.

In another case of **Dr. Prakash V. State of Tamil Nadu,**[15] the petitioner in this case of a remand prisoner in Vadapalani Police Station, Tamil Nadu and was detained under S-3(1) of the Tamil Nadu Preventive Detention of Bootleggers, Drug Offenders, Goondas, Immoral Traffic

[10] https://indiankanoon.org/doc/326206/, accessed on 1st Jne,2020
[11] https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india, accessed on 1st June,2020
[12] https://indiankanoon.org/doc/170483278/, accessed on 1st June,2020
[13] https://www.lexology.com/library/detail.aspx?g=8ca29f1a-6e00-45ab-ad8f-ee6ff3ab6161, accessed on 1st June,2020
[14] Writ Petition (Criminal) No.167 of 2012 held on March 24, 2015.
[15] AIR 2002 SC 3533

Offenders and Slum-Grabbers for preventing there Dangerous activities Prejudicial to the Maintenance of Public Order. The ground for the detention was that the petitioner was indulged in offences as mentioned under S-67 of the Information Technology Act, 2000. But the petition was failed and the same was dismissed.

Most of the Cyber stalkers are familiar with the victim. Many of the Cyber stalker involves the person who have motive to take revenge, or attention. These communications generally begin as mere acquaintance then the stalker gradually starts getting familiar and his communication may also become unwanted. If this unwantedness occurs, one can stop it by either blocking or reporting it to the proper authorities. While, other cases of Cyber stalking which involves high profile individuals or celebrities, might involve a complete stranger. It is one of such crimes that can be committed either by an individual or a group of people.

2. **Cyber Bullying:** Bullying is a way to raise oneself by defaming others. Cyber bulling refers to that bullying that takes place over digital technology like cell phones, e-mails, SMS, texts and various online platform. Cyber bullying involves sending, posting, sharing harmful or false contents relating to someone. It also includes sharing of personal information, which can cause humiliation if that content is spread.

The 2017 Youth Risk Behaviour Surveillance System (Centres for Disease Control and Prevention) indicates that an estimated 14.9% of high school students were electronically bullied in the 12 months prior to the survey.[16]

3. **Hacking:** Hacking is an attempt to exploit the computer system. In other words, it is an unauthorised access by a person to control a computer network for some illegal purpose.

Hackers are generally those, who have a good control over the computer network and they are highly skilled in handling computers. In computer parlance, Hackers can be categorised as White hats, Black hats and Grey hats. White hats are professional hackers to check their own system and to make it more hack proof. It involves organisations. Black hat hackers, generally hack the computers to take control over the system for their personal gain. They get an unauthorised access over it. Grey hat hackers have just enough knowledge of the computer language, so that they are able to hack a system to locate loopholes in the systems. Black hat differs from Grey hat as the latter notify about the weakness discovered in the system to the admin whereby the former is the

[16] https://www.stopbullying.gov/cyberbullying/what-is-it, accessed on 1st June,2020

one who looks only for his own potential gain. Both black hat and grey hat hacking is illegal except that of White hat hacking.[17]

Hacking has evolved from a teenage mischief to a billion-dollar business, whose disciples have established a criminal infrastructure that develops with less sophisticated technical skills. Now a days, hacking is not only associated with Windows Computer but the Android system have also attracted and invited the hackers.

In the case of **S. Sekar v The Principal General Manager (Telecom) (B.S.N.L.),**[18] the petitioner was an employee of the respondent, BSNL, working as a telecom technical Assistant. It so happened that while he was working in SIPCOT MBM Main Exchange, Keeranur, the B.S.N.L. higher officials suspected him and others for having committed offences in manipulating the computer system and thereby causing loss to B.S.N.L. The FIR in Crime No. 1 of 2004 was came to be registered on 06.01.2004 by the Police, Pudukkottai, for the offences under Section 406, 420 and 468 I.P.C. and 43(g) of the Information Technology Act, 2000.

The main thrust of the grievance of the petitioner in this case is that when there is a special enactment namely, the Information Technology Act, 2000, which is in operation relating to the alleged misconduct attributed as against the petitioner, there is no question of invoking the penal sections under the Indian Penal Code. The Second respondent filed that the FIR registered was proper and the Police is investigating into the matter properly. The Madras High Court stated that The Section 43(g) of the Information Technology Act, 2000, invoked by the police and specified in the FIR is declared void.[19]

4. **Child Pornography:** It involves the use of computer to circulate or distribute, that sexually exploit the children. Federal Law defines Child pornography as depiction of sexually explicit conduct involving minor. Images related and used in such child pornography is also termed as child sexual abuse image. When these images are placed on the Internet and disseminated online, the victimization of the children continues in perpetuity.[20] Victims of such sexual abuse generally suffers a lifetime of such victimization again as they have the knowledge of their sexual abuse being

[17] https://economictimes.indiatimes.com/definition/hacking, accessed on 1st June,2020

[18] W.P.(MD) No.10208 of 2005

[19] http://www.prashantmali.com/cyber-law-cases, accessed on 1st June,2020

[20] https://www.icsi.edu/media/webmodules/aboutus/courses/CS_Course_01042014.htm, accessed on 1st June,2020

on the internet forever. Such kind of abuse can create an everlasting psychological damage to the child. The US department of justice have reported an increase in the number of people for child pornography.

The **Arzika Case,**[21] Pornography and obscene content sent electronically has continued to grab the attention of liberals. Cases relating to such pornography and obscene materials thought reported in media, often goes unregistered. The Arzika Case was the first case relating to pornography.

Janhit Manch and Ors V. The Union of India,[22] was a case to put a ban on the Child Pornography. The petitioner solicited a total ban on such websites. The NGO urged that these websites create a negative impact leading the youth on a criminal path.

5. **Phishing:** Phishing is that kind of fraud which tries to fool people and make them part with their money. The increase in E-commerce has also evolved the new regime of paying online and making payment online. This has led to increase in the no. of cases of phishing. Phishing is the receipt of unauthorised e-mails by a customer by their financial institutions, calling them from their username, password or other personal information about their bank account for some banking or other reason. Customers do as direct in the mails as it this fraudulent site is just replica of the original website of that institution, so they remain unaware about the fraud that has occurred. Then the person committing the fraud can access the bank account of the customer and even to the funds available in that particular account.

The first phishing lawsuit was filed in the year 2004. The case of against a Californian teenager who created the replica of the actual website named "America Online". Due to the creation of this fake website, he was able to get access to some very sensitive information of the customers relating to their credit cards and other bank account details. He was able to withdraw money unlawfully.[23]

In another landmark case of **National Association of Software and Service Companies V. Ajay Sood and ors,**[24] the High Court of Delhi in this case declared that 'phishing' on the internet is an illegal activity. Emphasizing on the concept of 'phishing' that court stated that it that form of internet fraud where a person pretends to be in a legitimate association with banks or an insurance company, so that they can extract the data from the customers. The court also stated that typical phishing cases involves

[21] Southwark [Crown Court, 30/6/1999]
[22] 2008 (1) Bom.C.R 670. Bench: P J.N., S A.A
[23] https://www.phishing.org/what-is-phishing, accessed on 1st June,2020
[24] 2005 (30) PTC 437 Del

person who pretend to represent the bank online, i.e., E-banking and move the cash illegally from one account to another after the customers hand them with their banking details.

The High Court of Delhi stated that there is no specific legislation in India regarding 'phishing'. The court held 'phishing illegal by defining it under the Indian Law as 'a misrepresentation made in the course of trade creating confusion as to the origin of the E-mail causing harm to the consumer.' The plaintiff was an India's one of the premier software association and the defendants, on the other hand, was a placement agency which was involved in the recruitment. In order to get the personal information of the customers, the defendant companies used send fake E-mails to various persons in the name of the software company. These offending E-mails were downloaded and presented in the court of Delhi as evidence.

It came to the limelight that the defendants who were sending E-mails were a fictitious person which was created by the employees of the defendant company itself in order to avoid legal issues. The defendant arrested there claim and admitted their illegal act and they agreed to pay Rs. 1.6 million to the plaintiff as damages.

This case is a landmark judgement as it brings the act of 'phishing' into the purview of the Indian legislation in the absence of any law relating to 'phishing'.

2) Cybercrimes against the Government

1. **Use of Internet and Computer by the Terrorist:** Use of internet and the computer network by the terrorist is rapidly increasing. Most of the terrorists are using virtual and also physical storage for hiding information for their illegal crime. The terrorist also uses E-mails and other chat ways to communicate with their sleeper cells all over the world. They keep all that information in a password protected file which cannot be hacked easily. They E-mail one another using such code word which cannot be encrypted. Sometimes they compose a mail and save it in draft folder, and the other terrorist, they open the same E-mail id and read the message as saved in the draft.[25]

3) Crimes against Property

[25] https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

1. **Cyber Squatting:** Cyber Squatting implies where two persons come together and claim for the same Domain Name either by saying that they had registered their name first or claiming to use something similar to that previously. For example, there can be two similar website and two person claiming for it, i.e., www.yahoo.in and www.yahoo.in. Cyber Squatting may be defined as the practice of registering an internet domain name which is very likely that it would be wanted by another person or a business in the hope that it can be sold for profit. It implies registration of trade names as the domain names by the third parties, who do not have the rights in such names. Precisely, Cyber squatters register trade names or business name and so on which belongs to the third party with the motive of trading on reputation of such third party by confusing the customers to sell the domain name to the owner at a profit.

Like many developed countries, India doesn't have any specific legislations for domain name protection law and thus all the Cyber Squatting cases are to be dealt with the existing legislations relating to Trade Mark under Trade Marks Act, 1999. In the case of **Satyam Infoway Ltd. V. Sifynet Solutions Pvt Ltd.,**[26] The Supreme Court observed the difference between the terms trade mark and domain name. the court held that the difference lies in the way the two operates. A trade mark is protected by the trademark mark Act of that particular country. A trade mark can have multiple registrations in various countries throughput the globe. But, on the other hand, a domain name is potentially accessible irrespective of the location of the customer. The outcome is that not only a domain name would require worldwide exclusivity and also that no national law would be adequate to protect domain name. The Supreme Court could feel the backdrop in the law. However, in the absence of such law, provisions of the Trade Mark Act would be applied to solve the disputes.

In another case of **Travel.IndiaTimes V. IndiaTimesTravel,** The plaintiff in this case sought an injunction to restraint the defendants from cybersquatting, i.e., using similar name and to transfer the domain name 'Indiatimestravel.com' to the plaintiff.

The court referred to the judgement of Satyam Infoway, it was held that plaintiff owned the mark "indiatimes.com" way before the defendant created the mark "indiatimestravel.com". Further, "indiatimes" which was the essential component of the domain name, was used by the defendant without any explanation. The use of impugned web portal by the defendant may also jeopardise the reputation of the plaintiff if the products and services which are advertised through the website lack quality. The instant dispute was held to be a clear case of "passing off". As the plaintiff was

[26] AIR 2004SC3540

held to have the sole right to use the words "Indiatimes", defendant was directed to transfer "indiatimestravel.com" to plaintiff.[27]

CYBERCRIMES AND SOME LANDMARK OCCURRENCES

1) **India's First ATM Card Fraud Case**: The Chennai Police arrested an International gang which was involved in the Cybercrime. This was the 1st ever such ATM fraud. When the Chennai Police arrested Deepak Prem Manwani, who was just 22 years old, was caught red handed while breaking into an ATM in the city of Chennai in June Last. The proportions of the police achievement could be gauged from the fact that they netted a man who was on the wated list of the FBI of the US. At the time of he being under detention, the accused had with him Rs. 7.5 Lakhs knocked from two of the ATM'S of the city. And prior to this, he had also knocked off Rs. 50,000 from an ATM in Mumbai. While dealing in this case in details, the police noticed upon the Cybercrime which involved people from all over the globe. Deepak Prem Manwani was an MBA drop-out from a college in Pune and had served as a marketing executive in a firm in Chennai for quite a sometime. His crime career began in an internet café. While scrolling through the net, he got attracted to one of the sites offered him assistance of how to break the ATM's. His contacts, who were sitting somewhere in Europe, were ready to give him a no. of credit cards of some American Banks for $ 5 per card. They also offered him some magnetic code for those cards but they charged $200 for those codes. The operators of the site, floated a new site that resembled the website of a reputed telecom company. The company had millions of customers and subscribers. This fake site offered the visitors to return $11.75 per head which the operators said that it was collected excess from them by mistake. Seeing this and believing it to the original website of the telecom company, the subscribers logged on to the site to get back their money but while doing so, they had to part with their PINs. Having all the necessary data's, the gang started with systematic looting of the bank's ATM. In the mean time, Manwani somehow managed to get 30 plastic cards that contained necessary data so that he could break into an ATM. He also sold a few of such plastic cards to his contacts in Mumbai. On the receipt of such large-scale complaints from the billed credit cards, the FBI started investigations and also alarmed CBI in New Delhi that the international gang had some contacts in India too. This is now believed by the state's police that the beginning of a major cybercrime in the world.[28]

[27] https://spicyip.com/2010/11/travelindiatimes-v-indiatimestravel.html, accessed on 2nd June,2020
[28] https://indiaforensic.com/atmfraud.htm., accessed on 2nd June,2020

2) **CBI Website Hacked**: In the biggest embarrassment to the country's security, the website of the investigating agency named CBI was hacked on 03th of December,2010. It was hacked by a programmer identified as "Pakistani Cyber Army". CBI website, before the hacking, had received a warning from the Pakistani cyber army that the Indian Cyber Army should not attack their website. The hacker by infiltrating into the CBI website and hacking the countries more secure website have scorned at the country's cyber security. The CBI is 24 * 7 connected to the world police organisation-Interpol. The message from the hackers also spoke about the various controls given by the National Informatics Centre. National Informatics Centre or NIC is a body that controls the computer servers all across the country. CBI and many other Intelligent agencies operating in the country have often told and warned the Government about the lack of proper security being provided in these government offices and that cyber security audit was not being carrying out. The Pakistani Cyber Army had also warned the CBI that they could carry 'mass defacement' of other sites as well.[29]

3) **Official Website of IRCTC Hacked:** On 4th May 2016, IRCTC website was hacked. IRCTC is a ticket booking platform provided by the Indian Railways. Personal information of around 1 Crore people were feared to be stolen from the E-ticketing portal. IRCTC feared that personal information like date of birth, phone no., and other such information were being sold in a CD for Rs. 15,000. The state government of Delhi had reported to have identify those hackers. IRCTC has urged the government to provide more safety to such website as its customers give their personal information while filling the reservation form and if such information is leaked can cause harm to the customer.

Recently on 21st January,2020, A software developer from Jharkhand named Ghulam Mustafa was arrested for the charges of illegal ticketing in the Indian Railways. Using 563 different IRCTC id's, he used to run an illegal software racket to generate ticket. He was suspected bank accounts in 2,400 SBI branches and 600 regional rural banks. The main aim of such rackets is to generate money. Once they have collected the money, they then turn toward financing terror.[30]

CONCLUSION

[29] https://timesofindia.indiatimes.com/india/CBI-website-hacked-by-Pakistani-Cyber Army/articleshow/7038524.cms, accessed on 2nd June,2020
[30] https://www.livemint.com/, accessed on 2nd June 2020

The Information Technology Act,2000 is the most significant development in the legal field. Going through the timeline of the country, firstly, it was an agrarian based country. Its economic activities included only agriculture. Then the economy had a shift from agriculture to industrial and looking to our economy now, we have a totally different kind of economy, i.e., information-based economy. The fast development in the field of communication and information technology have brought about a good deal of change in the way of communication. And transfer of information. Now a day's business transactions have also started to take place online through electronical means since the business transaction can be accessed and can be taken place from any part of the world.

It is very clear that with the advancement of such technology, the rate as well as the frequency of the Cybercrimes have increased and is increase day by day. From E-mail spoofing to software piracy, from cyber stalking to child pornography, there are no such stones remained untouched by the offender to commit a crime. It has been reported that there is an increase of approx. 1.4% in the rate of Cybercrimes committed every year and it is even more surprising to know that most of the crimes are committed by qualified people. From the first bank fraud case to the first cyber defamation case, the offenders are qualified engineers committing such crimes. As the issues discussed in various case laws by the Indian courts, the Information Technology Act,2000 is found to have some loopholes and there are doubts left in the provisions which becomes the reason for the escape of the offenders. It was only after the amendment in the year 2008 which has brought few more specific Cybercrimes in the provision.

India, is one of such nations in the world to have a separate legal framework for E-Commerce and other technological services. The Information Technology Act,2000 is comprehensive in nature, yet their area various provisions that could be added and are left uncovered. Never the less, it can be said that the legislatures have put in a great effort to bring forth such kind of an Act. As this is open for amendment at any point of time, the law makers can amend it according to the situations and the need of the society at that time.

Thus, it can be concluded by saying that the Information Technology Act,2000 have tried to address to an extent all kind of legal questions and problems relating to Cybercrimes and E-commerce.