Incompetence of Cyber Law Still a Major Threat to Cyber Privacy

Abstract

As we all know, this is the era in which most things are usually done through the Internet, from online trading to online transactions. Since the web is considered a global stage, anyone can access Internet resources from anywhere. Few people have used Internet technology for criminal activities such as unauthorized access to other people's networks, scams, etc. These criminal activities or internet-related crime are called computer crimes. To stop or punish cyber criminals, the term "cyber law" was introduced. Computer crime occurs in the world of computers and the Internet. This type of crime has a serious impact on our economy, on our lives and on our society, because our society is becoming an information society, full of exchanges of information that is happening in cyberspace. Computer crimes always involve some degree of violation of another's privacy or damage to computer properties, such as files, web pages or software. This document is completely focused on the topic of cybercrime, on trends and problems faced by users and on how cybercrime can be minimized by formulating effective cybercrime laws in India.

Chandni
Research Scholar,
National Law University,
Jodhpur, Rajasthan,
India

Keywords: Cyberspace, Cyber Crime, Cyber Privacy, Cyber Law, Loopholes of the Law.

Introduction

In the era of the cyber world, with greater use of computers, there has also been an expansion in the growth of technology, and the term "Cyber" has become more popular. The evolution of information technology (IT) has given rise to cyberspace that offers everyone equal opportunity to access any information, data storage, analysis, etc. with the use of high technology. The rapid growth of the Internet and information technology has led to the growth of new forms of cyber crime and has become a major concern worldwide.

While it opens door to many useful applications and provide great opportunities for information sharing, most private networks contain some information that should not be shared with outside users on the internet, not all internet users are involved in lawful activities. Thus, the major concern is protecting confidential information.

Cyber crime is a crime whose kind is conventional crime, where crime is committed using the computer as a tool or means. It can be easily compromised, but it is difficult to identify and is also very difficult to trace in jurisdictional terms. It is true that technology has offered a global opportunity to promote and progress in human society. But unfortunately it provided fertile ground for the criminal enterprise. New technologies, such as e-commerce, social networks, online bank accounts, etc., have given rise to many new emerging trends in cybercrime. The need to introduce a cyber law to govern cybercrime and protect the privacy of Internet users in cyberspace has given rise to the Information Technology Act, 2000, but it still does not reach many aspects. The cyber world is vulnerable in the current era due to the lack of adequate preventive measures and results in a disaster, not only in the banking and commercial sector, but also in natural social life.

Review of Literature

Animesh Sarmah, Roshmi Sarmah, Amlan Jyoti Baruah, in their article “A brief study on Cyber Crime and Cyber Law’s of India,” in International Research Journal of Engineering and Technology Vol. 04 Issue 02, (2017), asserted that the invention of the computer has made the life of human beings easier, has been used for various purposes, from individuals to large organizations around the world. In a simple term, we can define the computer as the machine that can store and manipulate / process information or instructions that are provided by the user. Most computer users use the computer for incorrect purposes, either for their personal benefits or for the benefit of others for decades. This gave birth to "cyber crime". This led to participation in illegal activities for the company. We can define cybercrime as crimes committed with computers or computer networks and usually occur in the cyber space, especially on the Internet.

Shubham Kumar and Uday Kumar, in their article “Present scenario of cybercrime in India and its preventions,” in International Journal of Scientific & Engineering Research, Vol. 6 Issue 4, (2015), disused that cyber law must change and evolve at the same rate as hackers if it has any hope of controlling cybercrime. The law must also strike a balance between protecting citizens from crime and violating their rights. The good thing about the internet is how large and free it is. There will always be new and unexpected challenges to keep up with cyber criminals and cyber terrorists, but we can only win through collaboration and collaboration between individuals and the government. There is much we can do to ensure a safe and reliable IT environment. It is crucial not only for our national sense of well-being, but also for our national security and our economy. However, India has taken many steps to stop cyber crime, but the cyber law cannot afford to be static, it has to change over time.

Dr. B. Muthukumaran, in his article, “Cyber Crime Scenario in India,” in Criminal Investigation Department Review, January2008, found that the global anti-malware market is driven by cyber threats. The commercialization of cyber crime is stimulating malware writing activity and is causing more such threats. In the consumer space, this results in identity theft and stolen passwords. Growth opportunities have led to greater competition in the consumer and business segments. On the other hand, the loss of intellectual property and customer data, along with extortion with the threat of removing websites or revealing confidential information, is increasing in the business space.

Neelesh Jain and Vibhash Shrivastava, in their article “Cyber Crime Changing Everything – An Empirical Study,” in International Journal of Computer Application Vol. 1 Issue 4, (2014), stated that law enforcement agencies around the world are working together to develop new partnerships, new forensic methodologies and new responses to cybercrime to ensure Internet security. New skills, technologies and research techniques, applied in a global context, will be needed to detect, prevent and respond to computer crimes. This "new enterprise" will be characterized by new forms of crime, a much broader scope and scope of crime and victimization, the need to respond in a much timelier manner and the complex technical and legal complexities. Eventually innovative responses might be needed, such as the creation of cyber-police, cyber-courts and IT judges to overcome important jurisdictional problems.

Cyber Crime

The term "cyber" has been derived from the term "cybernetics", which means the science of communication and control of the machine and man. Cyberspace is the new machine-controlled horizon for information and communication between human beings throughout the world. The term "cybercrime" is an inappropriate name. The concept of cyber crime is no different from the concept of conventional crime. Both include conduct, or act or omission, which causes non-compliance with the rules of the law and is neutralized by the sanction of the state.

Cyber crime is the most complicated problem in the cyber world. It can be said that cybercrime is a type, which is a conventional crime, and in which the computer is an object or subject to behavior that constitutes a crime. In this crime, the computer is used as a tool or objective or both such as in the cases of financial crimes, crimes against intellectual property, cyber-defamation, etc.

The Internet is rapidly becoming a lifestyle for millions of people. However, it is also becoming a haven for criminals[1]. The "Internet Security Threat" report released by Norton (Symantec) states that India has 42 million computer crimes every year. He also said that 52% of victims suffered attacks such as malware, viruses, piracy, fraud, fraud and theft.[2]

There have been several types of computer crimes and the Internet. The most common of these is the use of viruses to corrupt or destroy data stored in the computer system. These viruses can be attached to e-mails, etc. There are also other forms of fraud, theft and forgery. The false plans have already robbed many people of a large amount of money. The growth of internet crime is directly proportional to the growth of the Internet itself, as is the variety of crimes committed.

The Indian Penal Code of 1860 does not have a definition of cyber crime; but it is understandable because at the time of his framing there was nothing that could be said to be a computer. Before the enactment of the law on computer science, 2000, this was the law applicable to all computer crimes. Furthermore, the IPC still applies to all these circumstances, since Article 77[3] of the IT Act states that compensation, sanctions or confiscation under the IT Act does not release the author from the responsibilities of any other law. Therefore, the substantive provisions of the IPC continue to apply these crimes. Therefore, it is worth examining the cyber crimes in the context of the ICC.

Essentials Ingredients of Cybercrime

It is a general principle of criminal law that a person cannot be convicted of a crime unless the prosecution has proven beyond reasonable doubt. According to criminal law, a crime consists essentially of two elements, namely, actus reus and mens rea.

A well-known definition of *actus reus* is *“such result of human conduct as the law seeks to prevent.”*[4]

The second essential component of a crime is "a guilty mind", also known as Mens rea. It can include a range of different mental attitudes, including intension, recklessness and negligence.[5]

Thus, in the same way, the theory of criminal law can be applied to computer crimes, since *actus* *reus* and *mens rea* together constitute a crime, that is a cyber crime.

Few of the illustrations that amount to *Actus reus* in cybercrimes are:

When a person is-

1. Without the authority tries to make a computer function;[6]
2. Without the authority tries to access information stored on or from a computer.
3. If someone uses the Internet to try to log in, the signals go through different computers. Each of these computers is designed to perform a function in the instructions that the person gave to the first computer in the chain. Each such function can be said to constitute *actus reus.*
4. Tries to login, although those attempts fail.[7]

Some of the examples that constitute *Mens rea* in cybercrimes are:

1. The person who intends to access, alter, damage, delete, destroy information, network security, the computer system, etc., or the intention to defraud or simulate a false representation, etc.
   In the case of a hacker[8]:
2. The access intended to be secure must have been unauthorized;
3. The hacker should been aware of the same at the time he or she tried to secure the access.

Classifications of Cyber Crime

Unauthorised Access

Use or access knowingly or intentionally without the authorization or consent of the owner or possessor, in whole or in part of a computer, computer system or computer network to commit computer crimes.

Cyber Fraud

Fraud committed through a computer, an IT system, a computer network or Internet-related communications should be considered computer fraud.

Cracking

Crackers are malicious hackers who normally "eliminate" network security. Secretly enter the security system causing intentional damage.

Hacking

Unauthorized use of other computers, the computer database system, the network is a crime. Piracy is a crime in which hackers advance to sabotage, espionage and credit card theft after obtaining unauthorized control of victims' computers.

Cyber Theft

Theft of information or identity in cyber space.

Flowing of Virus

Programs that flow through the computer network from human agents, such as viruses, Trojans, logic bombs, worms to cause damage, alter, eliminate and destroy equipment, computer systems, computer networks and databases.

Cyber Pornography

Pornography on the net may include hosting a website that contains these prohibited materials and using computers to produce these obscene materials, which are downloaded through the Internet, obscene materials.

Cyber terrorism

It is a kind of cyber threat that uses new technology or turns it into a terrorist target. It is a national and international challenge.

Phishing

It is an act of acquiring personal information and confidential financial information from customers such as passwords, details of online bank accounts, credit card details, etc. stealing e-mail that contains spyware or malware codes or when customers visit a malicious website that is a replica of the original institution's website to enter their information. The offender therefore abuses this acquired information and causes an undue loss of the owner's funds.

Skimming

It involves the use of an electronic device called a skimmer to maliciously copy the customer's details and credit card data stored in a credit card's magnetic strip. Then, when the credit card slips through the skimmer, the credit card details are captured and the criminals use them to create a cloned card that they use for malicious transactions. Since the card is not stolen, the owner discovers this fraud when he uses the cloned card.

Hacking

Unauthorized use of other computers, the computer database system, the network is a crime. Piracy is a crime in which hackers advance to sabotage, espionage and credit card theft after obtaining unauthorized control of victims' computers.

Corporate espionage

Increased competition and the increase in new technology platforms have led companies to seize the opportunity to position their brand through personal websites and social networks. This has made corporate espionage evolve and become digital. It is a major concern for organizations, since most CEOs have started using the services of investigators and surveillance agencies to spy on their former employees and their lifestyle.

Cloud computing

Cloud computing involves transfer of data and information to third parties for storage, processing or support. This involves risks, such as the place where confidential data resides, such as information on security and data privacy. It becomes difficult to govern and regulate information. Since there is no law covering cloud computing, the problems related to it are not solved in India. Many organizations in India do not have the infrastructure to reduce risks. Organizations need to be aware of cloud computing vulnerabilities.

Emergence of IT Act 2000

The law on evidence is traditionally based on paper documents and oral testimonies, which bear the signatures. It was necessary to introduce a new law to facilitate electronic commerce and give legal recognition to electronic records and digital signatures that gave rise to Information Technology Act, 2000.

The IT Act 2000 was mainly aimed at ensuring the legal recognition of electronic commerce in India. For this reason, most of the provisions are mainly related to the creation of digital certification processes in the country. Computer crime as a term was not defined in the act. It only developed with the case laws dealing with cyber crimes.

The IT Act 2000

The purpose of this Act is to grant legal recognition to transactions carried out through the exchange of electronic data and other electronic means of communication, commonly referred to as "electronic commerce", which also involve the use of alternatives to paper communication and archiving methods of information, to facilitate the electronic presentation of documents to government agencies and to modify the Indian penal code, the Evidence Act of India, 1872, Banker Book Proof Act, 1891 and the Reserve Bank Act of India, 1934 and for matters related to it.

Objectives of the Act are

1. To stop computer crimes and protect the privacy of Internet users.
2. To grant the legal recognition of transactions made through the electronic exchange of data and other electronic means of communication commonly known as "electronic commerce" instead of paper-based communication methods.
3. To make required amendments to Indian Penal Code 1860, Indian Evidence Act, 1872, Banker's Book Evidence Act, 1891, and Reserve Bank of India Act, 1934.
4. To guarantee legal recognition of digital signatures for authentication of any information or subject, this requires authentication based on any law.
5. To facilitate electronic data archiving and electronic transmission of documents to government departments.
6. To provide legal recognition for the maintenance of account books by bankers in electronic format.
7. To facilitate and legally sanction electronic funds transfers between banks and financial institutions.

Cyber privacy

Communication, speech and expression are undoubtedly some of the most elementary freedoms of individuals and to a large extent, can be considered inalienable. In the Indian context, these rights are legally recognized in Part III of the Indian Constitution.[9]

No freedom, however inalienable, can exist without restrictions. It is necessary that circumstances arise when freedoms can be reasonably limited if they are not suspended. The right to privacy under the Constitution of India can also be regulated for certain specific purposes contained therein.[10] One of the conditions, when such a restriction can be imposed, is national security. The problem, however, is to ensure that retraction is legitimate and solely in the interests of national security.

Therefore, in today's context it would not be sufficient to state that the violation of privacy would be justified by law; Furthermore, it must be shown that the law under which the violation occurred is fair, reasonable and reasonable.

As in the case of prejudice to constitutional rights, the validity, or alternatively, the invalidity of the restriction of the practice of such conduct, is pure speculation. Not surprisingly, this right contains conditions expressed when they can be private.

We have the right to privacy that the most confidential and private information must be kept secret and not disclosed, as we do not want to disclose it to third parties. The moment they are disclosed, they will lose secrecy, privacy and privacy. The right to privacy derives directly from Article 21 of the Indian Constitution.

In this context, it can be stated that privacy implies the right to control one's personal information and the ability to determine if and how such information should be obtained and used.[11]

With regard to the question of privacy and deprivation of privacy according to a procedure established by law, the answer lies in a solid and complete set of safeguards to ensure that state interference is allowed only when absolutely essential.

It may not be unreasonable to incorporate procedural safeguards into the IT Act of 2000. This safeguard should include procedures to declare when a problem has arisen concerning national security issues on which basis the same should be determined. In this scenario, the government or authority in question must be allowed to intercept in someone's privacy. This proclamation is not invoked at the absolute discretion of the authority; It will have to be done by the legislator in question. Furthermore, by making a proclamation of this kind public, a provision providing that during the emergency or security period may also be included. This would have the dual effect of avoiding unnecessary privacy violations and would substantially reduce the task of the government, intercepting and maintaining records.

Lacuna in IT Act

Some of the loopholes of it are:

1. Cyber crime is a global phenomenon and therefore the initiative to combat it must come from the same level so that the law lacks uniformity.
2. Because cyberspace is universal in nature, there are many jurisdiction problems. As cyberspace grows in a larger space, the territorial concept seems to disappear. There is a great need for new methods for this dispute resolution and should be replaced by conventional methods.
3. Section 43 of IT Act 2000[12], deals with 'sensitive personal data' but fall short in defining what it meant by this.
4. With regard to pornography, Article 67 of the IT Act establishes that obscenity is a crime when it is published, transmitted or published in any electronic form. But the expressions, "publication" or "transmission" have not been specifically defined in the IT Act.
5. According to Article 66[13] of the IT Act, the definition of piracy is very broad and can be poorly implemented. Furthermore, Article 67[14] of the IT Act is also vaguely to some extent. It is difficult to define the term lascivious information or obscene pornographic information. Therefore,

it can be stated that there are some ambiguities and inaccuracies in some of the definitions provided by the IT Act.

6. The lack of awareness amongst the people regarding their rights is the foremost reason that why IT Act is not attaining absolute success.
7. The IT Act does not address the problem of identity theft. This is a major problem, as most of India's subcontract work requires companies in India to ensure that there is no identity theft. This was the main reason for a great nuance and tone in an accident related to the personal information of UK customers and an Indian web marketing company. [15]

The country is becoming a healthier economy and the use of computers becomes ubiquitous, it is urgent that our laws are updated to respond to an evolving scenario. Due to rapid changes in the use of technology and in advanced society, smarter IT Act has an urgent need to be revised and should be reviewed in a much more regular way, mainly.

Conclusion

We have the right to privacy so that confidential and private information is kept secret and not disclosed because we do not want to disclose it. The right to privacy derives from Article 21 of the Indian Constitution. In the event of violation of these rights, we obtain legal redress. But in the current scenario, there is a great need to set up electronic courts and an electronic learning process so that people in India can prevent and control cybercrime related to privacy.

But in India, the prohibitive costs of litigation, along with the enormous delay that could occur at a very stage, make litigation an alternative that must be categorized as a last resort. Therefore, some defined principles must evolve to ensure that disputes are prevented rather than resolved.

There is also a question of jurisdiction. The nature of the Internet is such that geographical and political boundaries become irrelevant. A person with access to a computer and the Internet could participate, attempt or plan a criminal act anywhere in the world. Internet is analogous to *"High Sea".* People of all nationalities use it but nobody owns it. This makes cybercrime an international problem.

This would require that any policy, to be effective, be accepted and applied uniformly in different parts of the world. Partial efforts would not serve as an adequate solution. One suggestion was to try to commit cyber crimes in international crimes, similar to the crime of piracy under the law of the sea, which can be proven in any country.

However, the formulation of an international model law on cybercrime (on the basis of which different countries could legislate and guarantee harmony between the different territorial laws) could be one of the most practical approaches. The success of this initiative would control cyber crimes around the world.

The cyber world must be such that there is no fear and this can be achieved by implementing strict security measures and creating awareness of the laws, so that you can enjoy your own cyberspace.

Reference

A.H. Robertson *Privacy and Human Rights, Manchester University Press,* Manchester, 1st Edn., (1973).

Animesh Sarmah, Roshmi Sarmah , Amlan Jyoti Baruah, *"A brief study on Cyber Crime and Cyber Law's of India,"* International Research Journal of Engineering and Technology Vol. 04 Issue 02, (2017)

D.L. Shinder, *Scene of the Cyber crime: Computer Forensics Handbook*, Syngress Publishing Inc. 88 Hingham Street, USA, (2002).

Dr. B. Muthukumaran, *"Cyber Crime Scenario in India,"* Criminal Investigation Department Review, January2008

J.C. Smith and B. Hogan, *Criminal law, Butterworth and Company Publishers Ltd*., London, 6th Edn., pp. 31-36 (1988).

J.W. Cecil Turner (ed.), *Kenny's Outlines of Criminal Law*, *Cambridge University Press,*Cambridge, 18th Edn., pp. 31-36 (1962).

Karnika Seth, *Cyber Laws in the Information Technology Age*, Jain Book Depot, New Delhi, India, (2009).

Neelesh Jain and Vibhash Shrivastava, *"Cyber Crime Changing Everything – An Empirical Study,"* International Journal of Computer Application Vol. 1 Issue 4, (2014)

Nina Godbole and Sunil Belapure, *Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives,* Wiley India Pvt. Ltd, New Delhi, India, (2012).

Shubham Kumar and Uday Kumar, *"Present scenario of cybercrime in India and its preventions,"* International Journal of Scientific & Engineering Research, Vol. 6 Issue 4, (2015)

Footnotes

[1] Cybercrime cases in the country registered under the ITA 2000 last year rose by about 61% to 2,876 with Maharashtra recording the most number of cases.

[2] See<http://www.indiainfoline.com>. accessed on 9 September 2018.

[3] Compensation, penalties or confiscation not to interfere with other punishment.

[4] J.C. Smith and B. Hogan, Criminal law, Butterworth and Company Publishers Ltd., London, 6th Edn., 1988, pp. 31-36.

[5] J.W. Cecil Turner (ed.), Kenny's Outlines of Criminal Law, Cambridge University Press,Cambridge, 18th Edn., 1962, pp. 31-36.

[6] This is done by using input devices like the keyboard, mouse, etc.

[7] This is because most hackers have an authorized system of trying passwords, the very running of which can be considered to be a function being performed.

[8] Hackers are intellectual programmers who have special study and knowledge about computer system and they use their skills to cause troubles, steal credit card numbers, flow viruses etc. of

those hackers who are involved in illegal act to break into others computer system and network security they are crackers.

9. *Article 19(1)(a) of the Constitution of India, 1950.*
10. *In article 21 of the Constitution of India, 1950 which deals with the 'right to privacy' are provided the conditions when the right can be curtailed.*
11. *For broader definition see generally, A.H. Robertson Privacy and Human Rights, Manchester University Press, Manchester, 1st Edn., 1973.*
12. *Penalty and compensation for damage to computer, computer system, etc.*
13. *Computer related offences.*
14. *Punishment for publishing or transmitting obscene material in electronic form.*
15. *Horror of outsourcing to India - Indian call centers are illegally selling personal information of Australian customers. See < http://www.indiadaily.com/editorial/4198.asp>. accessed on 18 November 2018.*