AN ANALYSIS ON LEGAL REGULATION OF CYBER CRIME TO PROVIDE CYBER SECURITY IN INDIA

Mrs. Shubhalakshmi P.

Abstract

The world has become so small and come closer because of the influence of globalisation and innovative technological progress. Software Technology has reached its zenith but crimes that involves and uses computer devices and Internet, became rampant which has threatened cyber security. This is nothing but Cyber Crime without using physical force one can be commit against an individual or a group. Cyber Crime can also be committed against Government Departments, Private organizations and Non-Government Organisations as well. It may be in the form of hacking, phishing, virus attack, online fraud, electronic fraud, email bombing, spamming, cyber stalking, web jacking etc. It is difficult to trace the criminals in case of cyber-crimes as crime scene is not fixed to get evidence on it. To overcome from this risk of cyber-crimes, one should be aware about cyber security and data protection along with legal remedies for it. Cyber-crimes are dealt under few provisions of Indian Penal Code and criminal law. The Information Technology Act 2000, as well as its amended provisions in 2008, sanctions legal remedy to the cyber-crimes. It also narrates offences and punishment for the same. So, combating cyber-crime in any means is the need of the hour.

Introduction

Cyber Crime is not defined anywhere in the legislation but impact of cybercrime is severe and it is difficult to find the where abouts of the person committed crime. Cyber-crime is just a combination of crime and computer technology. Any kind of crime or offence in which a computer is used is considered as cyber-crime. In cyber-crime, fraudster steals information or data stored in the computer or destroys them for ever.Sometimes they steal intellectual property and utilize them in unauthorised manner too.

Different Kinds of Cyber Crimes

Cybercrime is a kind of criminal activity which takes place in the cyberspace. Even though cyber-crimes are crimes done by using computers, it can be inflicted against a person, property as well as against the Government.Cyber space has lots of components which includes computers, networks, software, data storage devices, the internet, websites, emails and even it includes electronic devices such as mobile phones, Automated Teller Machines etc.Cyber-crime against a person can be done through cyber stalking, impersonation, loss of privacy, transmission of obscene material etc.Cyber-crime against property can be done through unauthorized computer trespassing, by computer vandalism, transmission of harmful programmes, siphoning or tapping of funds from financial institutions, stealing secret information & data, copyright violation etc. Even against Government cyber-crimes can happen. They are in the form of hacking of Government websites, cyber extortion, cyber terrorism, infliction of computer viruses and so on.Other than these, there are certain other crimes like logic bombs, spamming, virus, worms, trojan horse, e-mail bombing, e-mail abuse etc.

Hacking

Hacking is an act committed by a fraudster by accessing computer of any other person without his prior permission. It is nothing but intruding privacy of an individual which is considered as an offence. Hackers usually gain an advanced understanding of computers and

* Assistant Professor, SDM Law College, Mangaluru

they commonly misuse this knowledge for deceitful reasons. They are technologically advanced and have skills and expertise in software programs and language.

Computer Fraud

Fraud is a kind of cybercrime that intends to deceive a person with the reason to gain important data or information. Computer fraud can be done by stealing, altering, destroying or suppressing any useful information to secure unlawful or unfair gain.

Identity Theft

In identify theft, cyber criminals steal personal data, especially passwords, data of banking, details of bank account, credit cards, debit cards, matters of social security and other sensitive information. Through this kind of cyber-crime, criminals can steal money.

Scamming

Scamming is done through different forms in cyber space such as by offering computer repair, network troubleshooting, and Information Technology support services, by forcing the users by posing some issues in computer but in reality, such issues do not exist.

Computer Viruses

The criminals can gain unauthorized access to systems and steal important data through infliction of computer virus. Mostly, highly-skilled programs send viruses, malware and Trojan, among others to infect and destroy computers, networks, and systems. Viruses can spread through removable devices and the internet.

Ransomware

Ransomware is a kind of malware from crypto virology wherein the victim is threatened from publishing or perpetually block access to data unless certain said amount is paid to the person committing this offence. Ransomware enters computer network and encrypts files and information through public-key encryption.

Distributed Denial of Service attack

This kind of attack is one of the most popular methods of hacking. There will be interruption on temporary or permanent basis, in servers and networks that are successfully running. Hackerswill manage to make the website unavailable for users when the system is offline.

Botnets

By sending spams or malware, computers are attacked by remote attackers called bot herders is called as botnets. Botnets specifically attack the information technology infrastructure of business and Government sector.

Spamming

In spamming, electronic message system is used, commonly through sending email messages that host malware, fake website links and other malicious programs. Email spamming is a popular kind of cyber-crime.

Phishing

Phishing is an activity wherein phishers act like a legitimate company or organization. By email spoofing they extract confidential informationlike credit card numbers, social security number, passwords, code words etc. They also send thousands of phishing emails which carry links to fake websites. Users will enter their personal information by believing that these are genuine sites to upload personal information.

Social Engineering

Sometimes criminals in cyber space, can contact through phone calls, emails or even in person is called personal engineering. Basically, they will depict themselves as legitimate companies and gain the confidence of the people first and later extract personal data as well.

Malvertising

Malvertising is a kind of attack in which perpetrators inject malicious code into any legitimate online advertising networks which redirects users to malicious websites.When the usersclick these advertisements, thinking they are legitimate then they will be redirected to fake websites or a file carrying viruses and malware will automatically be downloaded. And they will destroy data and create problems in cyber space.

Cyberstalking

Cyberstalking is a kind of cyber-crime in which a person is followed online anonymously. The stalker will follow the victim, mostly women and children including their activities.

E-mail Bombing

By sending large amount of emails to a victim account, the email account, the mail server or email account could be crashed.

Salami Attack

The financial institutions will be attacked by this kind of cyber crime wherein a very small amount of money will disappear from customers account while the employee of the Bank inserts a program.

Software Piracy

The original contents including songs, books, movies, albums, and software will be copied in duplicates and which leads to copyright infringement. This software piracy will result in illegal production of goods by fraudulent where the real owner's business gets affected.

Child Pornography

Because of the internet, pornography of children made available everywhere which is considered as an offence under law. Child pornography is a kind of cybercrime which involves the exploitation of innocent children in the porn industry.

Cyberbullying

Cyberbullying is a kind of harassment that takes place through digital devices such as cell phones, computers and other gadgets. Cyberbullying usually occurs through messages, text and applications which can also be done through online in social media where people can participate and share content. Through cyberbullying sending, posting, or sharing of negative, harmful, false content about someone else is done which causes humiliation to the victim.

Data Diddling

Data Diddling is a method of cyber-crime which involves altering raw data just beforeprocessing by a computer and later changing it back after completion of processing.

Legislations Governing Cyber Crimes

Cyber law incorporates various aspects mainly laws relating to cyber-crimes, electronic and digital signatures, intellectual property issues, data protection, privacy matters and so on.

Information Technology Act 2000

The Government of India enacted Information Technology Act and it got President's assent on 9th June 2000 and became effective from 17th October 2000. The main objective of this Act was to provide legal recognition for e-commerce that is electronic data interchange and other means of electronic communication, which are mainly alternatives to paper-based methods of communication and methods of storing information, to facilitate electronic filing of documents etc. Further, IT Act 2000 had an objective to amend certain legislations like Indian Penal Code1890, the Indian Evidence Act 1872, the Bankers' Books Evidence Act 1891 and the Reserve Bank of India Act1934.

The legislations like the Indian Penal Code, Indian Evidence Act etc contained certain provisions to identify and administer crimes of varied nature by they could not address the issues of cyber space directly. So, the need to amend these legislations along with formulation of new technological oriented legislation arose. It was Information Technology Act which consists of all the provisions to look in to the issues on cyber-crimes and cyber security matters under same umbrella. The main objective of the IT Act is to give legal recognition to electronic documents, digital signatures and to identify various offences along with redressal methods.

Information Technology Amendment Act 2008 focuses on legal recognition of electronic documents, digital signatures, data protection, data privacy, information security etc. The IT Amendment Act also focus on additional cyber-crimes like child pornography and cyber terrorism. The Information Technology Act consists of 13 chapters and 90sections.

Cases on cyber crime

There are plenty number of cases reported and sorted out by the cyber crime police department in relation to cyber-attack.

Four call centre employees, in 2004, who were working at an outsourcing facility operated by Mphasis, obtained PIN Codes from the customers of Citi Group, who were the customers of Mphasis. But they were not authorized to receive the Personal Index Numbers from the customers but after obtaining number they joined with other few employees and opened new accounts in Bank with false Identity Proof.They have transferred money from the bank accounts of CitiGroup customers to the new accounts at Indian banks. But in 2005 the Indian police had identified the individuals involved in the scam and arrested them and recovered the amounts too.

In 2009, Bomb Hoax mail was dropped to a private news channel by a teenager from Bangalore who was arrested by the cyber-crime investigation cell of to a private news

channel. He has challenged to search five bombs which are kept in Bombay within two hours. Police identified him and handled the situation.In another case, in 2010 the fake profile of then PresidentPratibha Devi Patil, created and was posted the fake profile in the name of the President.

Pornographic scandal took place in Jawaharlal Nehru University wherein two accused students initially tried to extract money from a girl who is caught in the videobut they could not receive money from her. But later, they uploaded it in mobile phones, internet and sold through Compact Disk as well in the blue film market.

SIM Swap Fraud was identified in August 2018 at Bombay wherein, two men from Navi Mumbai were in fraudulent money transferfrom the bank accounts of numerous individuals through obtaining their SIM card information through illegally.

The Canara Bank ATM servers at Kolkata were hacked by fraudsters in July 2018 in which around 20 lakh rupees from different bank accounts were swindled. The fraudsters were holding the account details of numerous ATM users across India.

National Cyber Security Policy 2013

The Cyber Security Policy 2013 provides a strong vision to secure the critical infrastructure and build a strong cyberspace for citizens, business, and government. The policy also intends to evade any resultant economic instability arising due to cyber-attacks.

Section 3, 3A, 4 and 5 of Information Technology Act mainly consists of electronic records and electronic signature related matters like their legal recognition and authentication. Section6,7 and 8 denotes as not to confer right to insist document should be accepted in electronic form and section 10-A deals with electronic contract. Chapter IX of Information Technology Act gives details on penalties, compensation and adjudication matters. Section 43 of the Act deals with penalty and compensation for damage to computer, computer system, etc. and 43A, 44, about compensation for failure to protect data and penalty for failure to furnish information, returns, etc. Residuary penalty also discussed under Section 45 of the Act. There are Cyber Appellate Tribunal established under section 48and 49 of the Act.

There are certain offences dealt under different sections of IT Act 2000 like section 65, tampering with computer source documents, section 66 hacking with computer systems, section 73 publishing of false digital signature etc.Sending threat messages through e-mail is a punishable offence under section 503 of Indian Penal Code. Forgery of electronic records also discussed under section 463 of IPC, E-mail spoofing, web jacking, E-mail abuse also considered as an offence under section 463, 383 and 500 of IPC.

Penalties for Computer Crimes

Section 65 to 78 of the Information Technology Act discuss about various penalties relating to computer crimes. As per the Act, civil liability and stringent criminal penalties may be imposed on any person who causes damage to a computer or computer system. The offender would be liable to pay compensation for gaining unauthorized access to a computer or computer system, introducing a virus in the system, damaging the system, denying access to an authorized person or assisting any person in any of the above activities.For the violation of its provisions there are specific penalties are imposed.If any person contravenes any rules or regulations framed under the Act for which no specific penalty is prescribed, he will be liable to pay compensation not exceeding Rs. 25,000.

Any person who intentionally or knowingly tampers with computer source documents would be penalized with imprisonment up to three years or a fine of up to Rs. 2 lakhs or both. In simpler terminology, hacking is made punishable.

The Act also disallows the publishing and dissemination of obscene information and material. The introduction of this provision should curtail pornography over the net. Any person who disobeys this provision will be punishable with imprisonment of two years and a fine of Rs. 25,000 for the first conviction. In the event of a subsequent conviction, the imprisonment is five years and the fine doubles to Rs. 50,000. Section 79A of the Act depicts notification by Central Government forexamination of Electronic Evidence.

Cyber Security

As the world has become digitally sophisticated, even the offences are also done in such a manner that offenders are not traced easily. Because of technological growth and accessibility for internet, most of the transactions and activities are done through internet and there arose a need to formulate law to govern this system of transactions

and business along with finding solutions to the problems which may occur in cyber space. Security and protection for all data and information and privacy matters are required as they are the basic things of any individual to be maintained. To protect ourselves from cyber-crimes, one should be well equipped with suitable law to handle the issues which are happening in cyber space. So, legal issues relating to internet are dealt through cyber law in India.

There are certain reasonable security practices to be followed for cyber security like site certification, security initiatives, awareness training, conformance to Standards, certification and adherence to policies like password, access control, email related policies etc.

Other than these, there is also requirement for periodic monitoring and review of our computers and related aspects of cyber space. The ATM card must have security featuresenhanced along with ATM monitoring systems which can prevent any misuse of data.

Sometimes, people receive even unsolicited text messages from an unknown number. But one should not respond to such messages. While downloading to mobile phones, one should download from a trustworthy source only. Those emails or calls which will ask for personal information and other details who are totally unconnected Persons To Us Not To Be Responded.

Conclusion

To prevent cyber-crime there are different provisions under law but they are not sufficient and effective to combat crimes in cyber space as it is borderless. The Government of India planned to formulate projects which need to be implemented effectively to serve its basic purpose. They are National Cyber Coordination Centre, Cyber Attacks crisis Management plan Internet Spy System Network, Crime and Criminal Tracking Network Systems etc. So, there is requirement of cooperation and coordination between various departments in the Government to handle cyber crime issues.

References

[1] AnandBhushan, TejasKaria and Sahana Chatterjee, India-Cyber Security 2020, accessed from, https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india on 19th February 2020.

[2] Dr. Farooq Ahmad (2012), Cyber Law in India(Law on Internet), 4th Edition, New Delhi: New Era Law Publications.

[3] Jayashankar K.K. and Philip Johnson, (2011), Cyber Law, New Delhi: Pacific Books International Publishers.

[4] Krishna Kumar (2011), Intellectual Property and E-Commerce Security, New Delhi: Dominant Publishers and Distributors.

[5] Mani K. (2012), A Practical Approach to Cyber Law, 2nd Edition, New Delhi: Kamal Publishers

[6] Naavi (2006), Cyber Law Demystified, Bangalore: Ujvala Consultants Pvt. Ltd.

[7] Paul Brennan (2007), Law for Information Technology Professionals, New Delhi: Universal Law Publishing Company.

[8] Prof. Bansali P.R. (2003), Information Technology and Cyber Law, 1st Edition, Jaipur: University Book House Pvt. Ltd.

[9] Pro. Randhir Singh and Dr. Ghanshyam Singh (2004), Cyber Space and the Law-Issues and Challenges, 1st Edition, Hyderabad: NALSAR University.

[10] Prof. Shilpa S. Dongre (2010), Cyber Law and its Implications, Mumbai: Current Publications.

[11] Rohit Anand (2015), Internet Education, 1st Edition, New Delhi: International Scientific Publishing Academy.

[12] Rowland D. and Elizabeth Macdonald (1997), Information Technology Law, London: Cavendish Publishing Ltd.

[13] Suri R.K. and Chhabra T.N. (2002), Cyber Crime, New Delhi: Pentagon Press.

[14] Swaroop K. Das, Bhattacharjee S, Srivastava R.K., Gautam Sarkar, Krishna Kumar and Nayak A.K. (2007), Encyclopaedia of Information Technology, Computer Sciences and Cyber Laws, 1st Edition, New Delhi: Dominant Publishers and Distributors.

[15] Talat Fatima (2016), Cyber Crimes, 2nd Edition, Lucknow: Eastern Book Company.

[16] Vakul Sharma (2011), Information Technology, Law and Practice, 3rd Edition, New Delhi: Universal Law Publishing Company.

[17] VanitVerma, Importance of Cyber Law in India, accessed from, http://www.legalserviceindia.com/legal/article-1019-importance-of-cyber-law-in-india.html on 20th February 2020

[18] Varun Bharadwaj (2014), Global Security and Cyber Crime, Jaipur: Neel Prakashan.

[19] Yatindra Singh J. (2012), Cyber Laws, 5th Edition, New Delhi: Universal Law Publishing Company.

[20] Cyber Crime-A Menace to India, by lawnn.com, September 26th 2016, accessed from https://www.lawnn.com/article-cybercrime-menace-india/ on 29th February 2020.