Indexed with IIJIF
Impact Factor : 1.021
ISSN: 2456 - 608X
International Journal of Legal Research and Studies
A Peer-Reviewed Refereed Online Law Journal

AN OVERVIEW OF CYBER SECURITY LAWS IN INDIA

Pooja[1], Dr. Raj Kumar[2]
[1]Research Scholar, [2]Associate Professor and Head & Dean,
[1,2]Faculty of Law, Baba Mastnath University, Asthal Bohar, Rohtak

Abstract-- **Today, human activities as directly or indirectly are influenced by science and technology in many ways. The invention of radio, television, telephone, super computers etc. all are the indispensable outcomes of science and technology. Today is era of technology which grossly affects our day-to-day life. It is the age of computers. along with that it has negative aspects also. Criminals are using this technology to commit many crimes as it is very easy to get access of information in very less time and almost for free. Legislators have enacted many laws to deal with cybercrimes. Government has also approved many policies and programs to deal with the crimes in cyberspace. This study aims to discuss various laws and government policies to combat cybercrimes in India.**

Key words: **Cybercrime, Cyber law, Cyber security, Information Technology Act.**

INTRODUCTION

Human beings are privileged with a sharp mind and special brainpower gifted by the nature which distinguishes them from other creatures of the universe and makes him superior than others. The progress of civilization leads to created more needs which eventually leads to more and more inventions and discoveries to fulfill the luxuries of modern life. Human mind generated the knowledge and reasoning capacity within him which results into the growth of modern science and technology[1]. Science is a branch of knowledge and the study of natural phenomenon which includes observation, description, identification, experimentation and systematic investigation and a thrust for reasoning to find out truth beyond usual concepts. Science and technology have substantially contributed to the overall development of mind kind. It has given new dimensions to human capabilities to improve his way of living. Development of science and technology provides all comfort of life benefitting the mankind worldwide. Today, human activities as directly or indirectly are influenced by science and technology in many ways. The invention of radio, television, telephone, super computers etc. all are the indispensable outcomes of science and technology. Today is era of technology which grossly affects our day-to-day life. It is the age of computers.

CYBER CRIMES

Crimes occurring in cyberspace are known as cybercrimes. It is the most emerging and spread worldwide now a days. They are different from conventional crimes in their mode of commission of the crime. Earlier, they were called as computer crime, computer-related crime or crime by computer. Others forms also include digital, electronic, virtual, IT, high-tech and technology-enabled crime. In general, cybercrime may be committed by three ways:

1. Target cybercrime: It is the crime in which a computer system is the target of the offender to commit a crime.
2. Tool cybercrime: It is the crime where a computer system is used as a tool by the offender in commission of a crime.
3. Computer incidental: It is the crime in which the computer system plays a minor role in the commission of the offense.

[1] Technology refers to the creation, gathering, processing, storage, retrieval. Presentation and dissemination of information and includes the processes and devices that enables all this to be done.

Indexed with IIJIF
Impact Factor : 1.021
ISSN: 2456 - 608X
International Journal of Legal Research and Studies
A Peer-Reviewed Refereed Online Law Journal

TYPES OF CYBERCRIMES

Some of the main cybercrimes prevailing in the society are as follows:

1) Hacking: Hacking in simple words is an act committed by an intruder by accessing the computer system without the owner's permission. They alter and modify system's data to execute tasks at their whims.
2) Logic Bombs: A Logic bomb, also known as 'slag code', is a malignant bit of code which is purposefully embedded into programming to execute a noxious undertaking when set off by a particular occasion. It is subtly embedded into the program where it lies lethargic until indicated conditions are met.
3) Virus Dissemination: A Virus is a computer program that attaches itself to or infect a system or files. It has a tendency to circulate itself to other computers connected on a network. They disturb the computer operation and grossly affect the data stored in it, either by modifying it or by deleting it altogether. Nonetheless, "Worms" not at all like viruses needn't bother with a host to stick on to. They simply recreate until they gobble up all accessible memory in the framework.
4) Denial of Service Attack: A Denial-of-Service attack is an express endeavor by attackers to refuse service to planned clients of that program. It includes flooding a PC resource with a larger number of solicitations than it can deal with available bandwidth through its accessible data transfer capacity which brings about server overload. This makes the resource to crash or slower down so nobody can get access to it.
5) Phishing: This is a technique of get the confidential information of a person such as credit card numbers and username & password by accessing it as a legitimate authority. Phishing is done by email spoofing. The specific malware tends to install itself on the computer and stolen private information.
6) Email Bombing and Spamming: Email bombing is sending numerous emails to a target address resulting in crashing the victim's email account or mail servers. These messages are meaningless and very long in order to consume network resources.
7) Web jacking: Web jacking drives its name form 'hijacking'. Here, the hacker fraudulently takes control of a web site and changes the original content of the web-site or tends to redirect the user to another fraudulent similar looking site maintained by him. The owner of the original web site now has no control over it.
8) Cyber Stalking: Cyber stalking is an online crime in our society when a person is stalked or followed by online medium. A cyber stalker doesn't physically follow his target, rather he does it virtually through cell phones or computer system, by following his online activity to get his information and then harass him or her. It's an invasion of one's online privacy.
9) Data Diddling: This involves altering a computer's raw data just before the processing of a particular data and converting that after the processing of the data. This is done for the purpose of committing monetary scam in the organization without even leaving the evidence to find out the mistake or the lost data.[2]
10) Identity Theft and Credit Card Fraud: The offence of Identity theft committed when someone steals others identity and pretends to be that person to get the access of the resources like credit cards, bank accounts and other benefits in victim's name. The imposter may also use others identity to commit other crimes. 'Credit card fraud' is a wide-ranging term for crimes that includes identity theft in which the offender uses

[2] Paranjape N.N. (Dr.): Criminology and Penology (13th Ed., 2007) p.139.

Indexed with IIJIF
Impact Factor : 1.021
ISSN: 2456 - 608X
International Journal of Legal Research and Studies
A Peer-Reviewed Refereed Online Law Journal

other's credit card to fund own transactions.

11) Salami Slicing Attack: A 'salami slicing attack' is also called as 'salami fraud'. it is a technique through which cyber-criminals draw money or resources in a very small amount at a time so that it is hard to notice the difference in overall size. The offender gets away with these little pieces from a large number of resources and thus receives an appropriate amount with passage of time.
12) Software Piracy: Software piracy is the unauthorized use and distribution of computer software. Software developers put immense hard work to develop these programs, and pirates snatch their ability to generate enough money to maintain application development.
13) Child Pornography: It is a form of pornography showing children which is against the law in many countries. Child pornography is typically done by clicking pictures or videos, or sometimes sound recordings of children, wearing less clothing than usual, wearing no clothing, or being raped.
14) Cyber Terrorism: cyberterrorism is a form of terrorism activities, where the "place" or "medium" through which it is carried out in is cyberspace. In current era, Cyberspace is a worldwide interconnected network of the internet and computer networks.[3]

LAWS TO DEAL WITH CYBERCRIMES IN INDIA

The following Act, Rules and Regulations are covered under cyber laws to combat the problems of cyberspace:

- The Information Technology Act, 2000.
- The Information Technology (Certifying Authorities) Rules, 2000.
- The Information Technology (Security Procedure) Rules, 2004.
- The Information Technology (Certifying Authority) Regulations, 2001.
- Indian Contract Act, 1872.
- Indian Penal Code, 1860.
- Information Technology Act, 2000 (as amended in 2008) Information Technology (Intermediately Guideline) Rules, 2011.
- The Juvenile Justice (Care and Protection of Children) Act, 2000(as amended in 2006 & 2010).
- The Constitution of India.
- The Commissions for Protection of Child Rights Act, 2005.
- The Criminal Procedure Code, 1973.
- The Protection of Children from Sexual Offences Act, 2012.
- The Young Persons (Harmful Publications) Act, 1956.

Information Technology Act, 2000

Cyber laws in India, basically are contained in the Information Technology Act, 2000. Information Technology Act, 2000 is India's mother legislation regulating the use of computers, computer systems and computer networks as also data and information in the electronic format. This legislation has covered varied aspects related to electronic authentication, digital (electronic) signatures, cyber-crimes and liability of network service providers. The IT Act of 2000 was initially enacted to promote the IT industry, regulate e-

[3] https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0719-25842018000200005

Indexed with IIJIF
Impact Factor : 1.021
ISSN: 2456 - 608X
International Journal of Legal Research and Studies
A Peer-Reviewed Refereed Online Law Journal

commerce activities, facilitate e-governance and prevent cybercrime. This Act also sought to foster security practices within the jurisdiction of India that would tends to serve the nation in a global context.

Some important provisions of the Information Technology Act, 2000:

- Section 65: Provisions for tamper with computer resources
- Section 66: Provisions for hack the data/ information stored in the computer.
- Section 66B: Provisions for misappropriation of information/ data which is stolen from computer system or any other electronic gadget.
- Section 66C: Provision of penalties for stealing someone's identity.
- Section 66D: Provision for access to personal data of someone by concealing their original identity with the help of computer system.
- Section 66E: Provision of penalties for breach of privacy.
- Section 66F: Provision of penalties for cyber terrorism.
- Section 67: Provisions related to the publication of offensive information.
- Section 67A: Provision for publishing or circulating pornographic information through electronic means.
- Section 67B: Provisions for publication or broadcast of some objectionable material by digital means, where children are shown in obscene mode.
- Section 67C: Provision for disrupting or blocking information by mediators.
- Section 70: Provision for making objectionable access to a secured computer.
- Section 71**:** Delivering data or data incorrectly.
- Section 72**:** Provisions related to mutual trust and privacy.
- Section 72 - Provisions for revealing the information violation of the terms of the Protocol in public.
- Section 73 - Publication of Ezra Digital Signature
- Section 78 - Inspector level police officer has the right to investigate these cases in the Information Technology Act,

Indian Penal Code, 1860

Cybercrimes in India has reared its ugly head in many ways and it is getting worse with passage of each day. Indian Penal Code is the main legislation to deal with different forms of crimes in India. Some main sections of IPC which cover cybercrimes are as follows:

- Sec. 354 C- Voyeurism.
- Sec. 354 D- Stalking.
- Sec.499 IPC – Sending defamatory messages through email.
- Sec .500 IPC – Email Abuse.
- Sec.503 Indian Penal Code (IPC) – Sending threatening messages through email.
- Sec.509 IPC – Word, gesture or act intended to insult the modesty of a woman.

DIGITAL EXPLOITATION OF CHILDREN

States/UTs are initially responsible for prevention, investigation, detection, and prosecution of crimes including crimes related to exploitation of children; by their law enforcement machinery. The law enforcement agencies take legal action as per provisions of law against persons involved in digital sexual exploitation/abuse of children. The Information Technology (IT) Act, 2000 contains sufficient provisions to deal with emerging cybercrimes. Section 67B of the IT Act provides adequate punishment for publishing, browsing or

Indexed with IIJIF
Impact Factor : 1.021
ISSN: 2456 - 608X
International Journal of Legal Research and Studies
A Peer-Reviewed Refereed Online Law Journal

transmitting child pornography in electronic form. Additionally, sections 354A and 354D of Indian Penal Code also provide appropriate punishment for cyber stalking cyber bullying against women. [4]

Government policies for preventing digital exploitation of children:

- Ministry of Home Affairs has initiated a scheme namely 'Cyber Crime Prevention against Women and Children (CCPWC)'. In this scheme an online Cyber Crime reporting portal (www.cybercrime.gov.in) has been started to allow people to report complaints related to Child Pornography/Child Sexual Abuse Material, imageries or sexually explicit content. This portal allows the public to lodge complaints without revealing his identity. Steps have likewise been taken to spread awareness, issue of alarms/warnings, training of law implementation offices, improving cyber forensic facilities and so forth. A handbook with guidelines on Cyber Safety for Adolescents/Students has been delivered (Copy accessible on www.cybercrime.gov.in and www.mha.gov.in) and shipped off all States/Union Territories for wide course. Cybercrime awareness campaign has been dispatched through twitter handle (@CyberDost) and radio the nation over.
- The Ministry of Women and Child Development had approved the Protection of Children from Sexual Offences Act, 2012 (POCSO Act), which will work as a specific law to protect children from offences like sexual assault, sexual harassment and pornography. Section 13-15 deals with the issue of child pornography. Further Section 28 of the same act provides for establishment of Special Courts to provide speedy trial of offences under the Act. In accordance with this act, MWCD has taken numerous steps to spread awareness about the provisions of the POCSO Act through digital and print media, workshops, consultations and training programs with stakeholders concerned from time to time. Further, State Commission for Protection of Child Rights (SCPCRs) and The National Commission for Protection of Child Rights (NCPCR) are also obliged to monitor the implementation of the POCSO Act, 2012.
- Government has provided various steps to be taken by Internet Service Providers (ISPs) to secure children from sexual abuse done online. These include blocking the websites which contains extreme Child sexual Abuse Material (CSAM) based on INTERPOL's "Worst-of-list" shared periodically by Central Bureau of Investigation (CBI). The list is sent to the Department of Telecommunications (DoT) to direct major ISPs to block such websites. Government ordered major Internet Service Providers (ISPs) in India to adopt and disable/remove the online CSAM persistently based on Internet Watch Foundation (IWF), UK list.
- Ministry of Electronics and Information Technology (MeitY) has launched a major program on Information Security Education and Awareness (ISEA). A particular website for information security awareness (https://www.infosecawareness.in) has also been initiated.

CHILD BULLYING ON INTERNET

The Government has taken various steps in this regard which include[5]:

- Ministry of Home Affairs has issued an Advisory on Preventing & combating Cyber

[4] 18.07.2019 - PIB : MANU/PIBU/1177/2019
[5] MANU/PIBU/0481/2014

Crime against Children dated 4th Jan., 2012, wherein it was advised to States / Union Territories to specifically combat the crimes in the forms of cyber stalking, cyber bullying, child pornography and exposure to sexually explicit material etc.

- The Information Technology Act, 2000 has provision for dealing with cybercrimes targeting children.
- Government has implemented Information Security Education Awareness (ISEA) program including the programs conducted by Confederation of Indian Industry (CII), Internet & Mobile Association of India (IMAI) and Data Security Council of India (DSCI) to provide awareness and training in the area of information security. Specific workshops have been organized for school children to make them aware about risks pertaining on internet and adopting safe internet browsing practices. A dedicated website for information security awareness (www.infosecawareness.in) has also been developed and content is available in English and Hindi language.
- A website (secureyourpc.in) for children, home users and elderly are launched for safeguarding their computer systems and learning the risks on internet.

NATIONAL CYBER SECURITY POLICY, 2013

Cyber Security has slowly emerged as a location of main concern for Indian lawmakers to follow repeated security lapses inside current info constructions in addition to a policy agenda of quickly improving digitization and increasing a chance to access the web. Nevertheless, while the emphasis on acquiring cyber security institutions has grown and also spending has grown exponentially, there's simply no long-range financial allocation for cyber safety steps, and then many stakeholders propose that present financial allocation has been insufficient. India's cyber security policy has goals in securing cyberspace, though it lacks in conditions of determining physical ways to accomplish the objectives. The policy paperwork that cyberspace has been a very common resource utilized by actors that have been diverse, among who it's tough to bring borders, which cyber security has to draw the perspective into consideration. The policy has been cognizant of the wide techniques associated with making sure cyber security identification of risks, info sharing between people, exploration and synchronized replies. The goals of the 2013 Policy spotlight the economic and social significance of safeguard individual details and also guard against cybercrime, in addition to the benefits of saving critical infrastructure, which may hinder the performance of the national economic climate. Even though the policy has been actually informative inasmuch as the different features of cyber safety steps have been recognized by it, the policy in unhelpful within demarcating various techniques to national cyber security and spelling away the way the federal government seeks to address these various features, for instance, exactly how replies to cyber terrorism or even attacks from vital infrastructure will be distinct from cybercrimes as information crime. Additionally, it fails to offer concrete steps or objectives to attaining cyber security. As the National Cyber Security Policy, but as vague, has been the XII 5 Year Plan report28 on Cyber Security, for 2012 to 2017, that concentrates on potential methods to attain cyber protection in a systemic way with the program time. The Plan Report additionally identifies several distinct steps that may be considered as goal deliverables for cyber security; however, few of their but functional. Cybercrime has been labeled as a high priority in the 5 Year Plan also the Cyber Security Policy. Additionally, hacking, a crime of information, 28Ministry of Communication & Technology (2018) Department of Information Technology, 12th Five Years Plan (2012-17) Report of the Working Group on Information Technology Sector, Government of India, New Delhi, p-95-109 31 computer-related crimes,

and cyber terrorism have been crimes that have been prosecuted under different as of the IT Act or maybe the IPC and functional zed through police agencies. There's very little difference between cyber-dependent and cyber-enabled crimes and no particular policy procedure for the latter. There's no law on information protection applied to governmental authorities. In reality, you will find minimal importance in-laws on securing unique private details kept by individual people as an issue of cyber security. Incidences of the individual as well as customer information safety via online services have been mainly remaining to the world of individual law, which includes contractual cures. The main umbrella application for information safety has been still a single provision for sensible protection habits needed by' body corporate' under Section 43A of the IT Act, hear together with the Reasonable Security Practices Guidelines, that involve conformity with sensible protection requirements recommended underneath the suggestions, like ISO 27001 Information Security Management Standard or maybe some additional standard with federal endorsement. Cyber protection has been clearly an expanding concern for India - each for federal policy and also for the private industry along with a culture progressively more dependent on a protected online. While India's cyber security framework signifies a definite should secure economically and socially great sectors as financial and banking, power cyber security has been labeled as simply being especially important to India's foreign policy safeguard goals. Likewise, while cyber security policy recognizes the assortment of variables which may create risks cyber security, which includes overseas American states, criminals, disasters policy or mishaps has been basically centered on dealing with structured cyber risks including foreign states or terrorist organizations, which may present a risk to security that has been national, and as that cyber protection has been viewed as an objective to attain by way of a multilateral strategy, with a huge predilection for satisfying national goals and statist through policy. Additionally, policy in India has been concentrated upon boosting the cyber of its protective methods rather compromised to its cyber unpleasant abilities.

CONCLUSION

Today due to high rate of internet usage, cybersecurity is one of the biggest needs of the hour globally. Cybersecurity threats and cybercrimes are very dangerous for the security, justice and peace of the nation. It is the duty of the government as well as the citizens to spread awareness among the people to deal with cybercrimes and always update the system, network security settings and to the use proper anti-virus so that the system and network security settings stay virus and malware-free. The victim should report the cybercrime at time and ignore being involved in a cybercrime cycle. By taking proper care and security measures individuals can deal with cybercrimes and protect the fair use of information technology for the growth of the nation.

As our investments in ICT infrastructure grow our vulnerability to damage by natural disasters or through

attacks by insurgents/terrorists with objective to immobilize and paralyze day-to-day activities of the nation is becoming real. Such damage would cause short and long term setback to economy. We have many lessons from US initiative to secure our cyber system, while planning and implementing India’s ICT infrastructure. Natural or insurgency/terrorist induced disaster increases pressure on available ICT systems exponentially to facilitate coordination between various agencies like fire brigade, medical services, police, media and civil administration. It is proposed that the existing and planned ICT infrastructure of the nation, both in public and private domain be analyzed by a group of experts under aegis of NDMA to suggest suitable operational arrangements to minimize their vulnerability to

perceived attacks by inimical elements and natural disasters. This would entail rigorous technical analysis of current and emerging wireless and wired ICT systems. The expert group should find and recommend suitable mix of redundancies in the critical ICT systems supporting the governance structure of the nation. The focused analysis of the vulnerabilities and their protection, would lead to recommendations that would avoid duplication of effort and, therefore, economical at national level. The notion that disasters can be completely brought under control by technological and scientific capabilities alone would be too presumptuous. The most sacrosanct component in any such venture is participation from all stakeholders to ensure an appropriate solution for the welfare of humanity.

As our investments in ICT infrastructure grow our vulnerability to damage by natural disasters or through

attacks by insurgents/terrorists with objective to immobilize and paralyze day-to-day activities of the nation is becoming real. Such damage would cause short and long term setback to economy. We have many lessons from US initiative to secure our cyber system, while planning and implementing India's ICT infrastructure. Natural or insurgency/terrorist induced disaster increases pressure on available ICT systems exponentially to facilitate coordination between various agencies like fire brigade, medical services, police, media and civil administration. It is proposed that the existing and planned ICT infrastructure of the nation, both in public and private domain be analyzed by a group of experts under aegis of NDMA to suggest suitable operational arrangements to minimize their vulnerability to perceived attacks by inimical elements and natural disasters. This would entail rigorous technical analysis of current and emerging wireless and wired ICT systems. The expert group should find and recommend suitable mix of redundancies in the critical ICT systems supporting the governance structure of the nation. The focused analysis of the vulnerabilities and their protection, would lead to recommendations that would avoid duplication of effort and, therefore, economical at national level. The notion that disasters can be completely brought under control by technological and scientific capabilities alone would be too presumptuous. The most sacrosanct component in any such venture is participation from all stakeholders to ensure an appropriate solution for the welfare of humanity

REFERENCES

[1] https://www.scconline.com/blog/post/2019/07/25/digital-exploitation-of-children/
[2] http://www.madhuvridhi.com/blog/cyber-frauds-types-controls/
[3] https://www.srdlawnotes.com/2020/08/use-of-child-for-pornographic-purposes.html
[4] http://www.legalserviceindia.com/legal/article-807-important-sections-from-information-technology-act-2000.html
[5] https://vajiramias.com/current-affairs/2019/7/?page=2
[6] http://www.legalserviceindia.com/legal/article-2379-dynamics-of-internet-child-pornography-menace-to-legal-and-societal-perceptions.html
[7] https://blog.ipleaders.in/introduction-to-cyber-crime-and-cyber-law/
[8] http://informationtechnologyprograms.org/information-technology-act-2000-in-marathi-pdf/
[9] https://www.indiacode.nic.in/handle/123456789/2056?view_type=browse&sam_handle=123456789/1362