Available online @ www.iaraindia.com
RESEARCH EXPLORER-A Blind Review & Refereed Quarterly International Journal
ISSN: 2250-1940 (P) 2349-1647 (O)
Impact Factor: 3.655(CIF), 2.78(IRJIF), 2.77(NAAS)
Volume XIII, Issue 43
July- 2024
Formally UGC Approved Journal (63185), © Author

NEWLY EMERGED CYBER CRIMES AND ITS LEGISLATIVE MEASURES IN INDIA

B.DHANAVEL
5th year B.A.LL.B, Government Law College, Dharmapuri
K.JEEVA
5th year B.A.LL.B, Government Law College, Dharmapuri
A. SRISABARINATHAN
5th year B.A.LL.B, Government Law College, Dharmapuri

Abstract

In this modern era, Human society has several high-level technological advancements; two such advancements are the creation of high-speed processing machines called computers and the internet. Both inventions converted the entire world into a global village. Due to speedy transfer of data, easy communication across the world, effective computer networking, and the entire world has been shrunk down as a village. Virtual world has been created by mankind. This is also known as cyberworld. People may live in the virtual world; all day-to-day activities will be conducted in the virtual world. It is already happening in the world. Physical activities of people have been reduced due to the influence of computers and the internet. Entire human life has been infused with hardware and software of the modern technological devices. We are influenced by the new technological advancements daily. But the statutes for penalising cybercrimes are not fully evolved in India. It should take a quick step to penalise the new cybercrimes. Artificial Intelligence aided crimes, cyber terrorism, cyber child pornography, cyber stalking, and cyber grooming are the newly evolved cybercrimes in India. Even those cybercrimes are newly emerged but they have very high capabilities to make a huge impact. Everyday new criminal incidents take place in India but penal statutes of India are not fully evolved to penalise those crimes. In this background this study provides a clear view about newly emerged cybercrimes and legislative measures in India.

***Keywords**: Cyberspace, Cybercrimes, Artificial Intelligence, Cyber terrorism, Cyber Child Pornography, Cyber Stalking, Cyber Grooming, Indian penal code, Information Technology Act.*

Introduction

Our natural world has been changed into the cyber world. Now-a-days, humans cannot survive without using the internet. The environment of the cyber world is known as cyber space. It has been defined by United States's National Institute of Standards and Technology as "the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form". Cyber space is the easy place to gather the information for committing crimes and easy place to execute criminal plans. It is very easy to commit cybercrimes through cyber space. Any person can commit it if he has internet connection and device for using internet connection. So effective penalising laws are much needed to prevent and punish cybercrimes.

Object of the Study

1. To identify, the cybercrimes which are newly emerged in India?
2. To focuses, the impacts which were done by such cybercrimes in the past and what are their capabilities.
3. To study about how the legislative measures are working to penalise such cybercrimes.

1. Cybercrimes aiding by Artificial Intelligence (A.I.):

Artificial Intelligence means an intelligence possessed by a computer source for making suitable decisions in difficult circumstances based on human thinking and reactions. AI is one of the best innovations of human beings, because it can analyse the circumstances and make decisions where humans cannot. Like critical functions of scientific and medical research, space research and so on. Human beings are unique creatures in the world because they have the ability of complex reasoning, introspection and very evolved cognitive thinking. These three functions can be done by the AI tool that is why AI is very dangerous. AI make the decisions based on artificial neural network which is mimics the human brain neural network. The tons of data with the description of what is what will feed in neural network. Artificial intelligence can do what is learnt from such data. Taking example of deepfake AI, it can replace faces, voices and facial expressions of persons based on task given by the user. because this AI already have the hundreds or thousands of images, videos and audios as data. Undress AI is also using this kind of working module.

Now-a-days, the threats of AI are significantly high. Many innocents are suffered by the misuse of AI by cybercriminals. Recently the Uttar Pradesh State Police filed a FIR for India's first cyber fraud case which is aided by AI. In that case, fraudsters made a nude video call to an innocent senior citizen for few seconds. After he cut the call, he received a video message in WhatsApp from the fraudsters. In that video message, Former Uttar Pradesh Additional Director General of Police Prem Prakash threated him and demanded him money for not taking legal actions against him. After the investigation, the nude video call and video message are artificially generated by Deepfake AI. Many AI tools can entirely

shake the safety of the country. Subscriptions for such kind tools are being sold on the dark web.

Liability:

The civil and criminal liability of AI is not determined by Indian statutes. AI is neither a natural person nor an artificial person. For deciding civil liability, AI just acts like a web search engine. It gives a result what it is inputted by the programmer. So civil liability should give to him but it is too difficult to define the criminal liability of AI. Criminal state of mind and criminal conduct are the two factors for attracting criminal liability. AI can do or can be used to do criminal activities but it cannot possess a criminal state of mind because it does not have a mind. Then who takes such liability. It is a burning question to decide now. According to Dr. Gabriel Hallevy, the criminal liability shall be decided by two aspects. First one, liability should be given either to the programmer or last user. Second one, liability is vast to AI itself along with the programmer or last user. But AI is a tool, dangerous activities only done by the evil mind of the last user or programmer. So, legislation should make a functional framework and penal provisions against them.

Legislative measures:

India has well-constructed penal statutes. Several Provisions are criminalizing various cybercrimes. Especially, Information Technology Act, 2000 is enacted specifically for technology related crimes. But none of the statutes of India penalise AI related offences. Cybercriminals can be punished for their crimes which are already criminalised by the statutes. But those criminals cannot be punished for using AI as the sources for their crimes. It is now very important to create separate enactments to penalise the last users and programmers for AI cybercrimes.

2. Cyber Grooming

The word grooming is defined in oxford dictionary as, "The process in which an adult develops a friendship with a child, particularly through the internet, with the intention of having a sexual relationship". Cyber grooming takes place in the internet. In this cybercrime, offenders show he as the child friendly person to children in online. After attracting the attention of children, they start sexual abuse, sexual interaction and trafficking. Most of the children are easily exploited in it because they did not know about the offender's demands. Cyber Grooming impact the feelings of children and it leads to self-harm, embarrassment and traumatic stress.

Cyber world is the playground for offenders who can easily hide their identity and they can easily attract children towards them. Those are the worst sexual predators in the world, they can now groom any child within their grasp with a few clicks of a mouse's button.. Especially In United Kingdom, reports of National Society for the Prevention of Cruelty to Children (NSPCC) stated totally 34,000 online grooming crimes had been recorded by UK police forces over the last six years and 1 in 4 online grooming crimes were against primary school children in the last 5 years. India is also facing this cybercrime now, the National Crime Records Bureau (NCRB) published statistical data on

crimes. As per data, totally 305 cases of cybercrime against children were registered in the year of 2019. The number of cases increased as 1102 in the year of 2020. Most of the cybercrimes against the children are started by cyber grooming. It leads to child harassments, child abuse, and child pornography and so on.

Legislative Measures

India does not have any dedicated penal statutes against cyber grooming, it does not have a statutory definition for cyber grooming. None of provisions penalise the cyber grooming now. Statutes penalise the outcome crimes related with cyber grooming but cyber grooming is not penalised yet. So, now separate penal provisions are needed to curb this cybercrime.

3. Cyber Terrorism

Cyber terrorism is the combination of two greatest fears of 20th century; Cyber and Terrorism. Berry Collin coined this term and defined it as the convergence of cybernetics and terrorism in 1997. As early as 1990, the report of the US National Academy of Science started as "Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb." The terrorists are using cyber technology for making, anonymously carrying, executing and covering the terror attacks. The twins tower attack by Al-Qaeda, 2008 Mumbai Taj Hotel attack, 2010 Varanasi blast are the examples of cyber terrorism. Cyber space is very easy to access and it has very wide information in it. Anyone can use it. It is already reported that most of the captured files of Al-Qaeda are either not encrypted or poorly encrypted. Encryption is one of the ways to carry information secretly. The person who wants to know such information, first he needs to decrypt the encrypted files. For decryption, he needs to know what the key is for it. So, the encryption method is very secure to carry terror plans and attacks.

Various terrorist Organisations are planning to utilise the internet for the advancements of their illegal activities. Reports also say that Osama Bin Laden has taken steps to improve organisational secrecy and to make clever use of technology. Cyber space is an easily available source to terrorists, anyone can learn hacking and encryption in cyber space. If the terrorists manage to break the government cyber system, terrors will be unimaginable. So, the implementation of strict control over online usage is very important. Cyber Terrorism is a world widely threatening problem. India is also not exceptional for it. Many incidents have already taken place. Particularly, taking example of Indian Mujahideen Delhi bomb blasts case, A terrorist group called as carried a serial of bomb blasts at several places in Delhi which killed 26 persons and injured 135 persons. After the bomb blasts, terrorists sent the mail to various Electric and Print Media taking responsibility for the blasts from the unsecured Wi-Fi connection of an innocent person.

Legislative Measures:

India did not have a dedicated penal provision for penalising cyber-Terrorism long ago. Even the Information technology Act, 2000 did not cover cyber terrorism before. but now, this criticism has been completely changed. There was

no provision in the original Information Technology Act, 2000 which dealt with cyber terrorism. But later the Indian Government addressed cyber-terrorism and amended the Information Technology Act, 2000 in 2008 after the Mumbai 26/11 terror attacks. Sections 66F, 70, 70A and 70B of Information technology Act, 2000 are introduced to deal with cyber terrorism. Cyber terrorism addressed as threat to unity, integrity, security or sovereignty of India. And whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

4. Cyber Child Pornography

Children are the easy targets for the offenders. They are voiceless and defenceless. They require special attention for protection of their rights. Even they cannot understand what is happening against their body. In child pornography, offenders sexually abuse children; they record such abuse and make it as a permanent record either in image or video format. The viewers of child pornography make a demand in the cyber world by way of watching that for that demand; children are abused, injured, even died in the real world.

Article 2 of the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child prostitution and Child Pornography defines child pornography as "any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes." Child pornography is a worldwide grievous problem. India also suffering from it. As per the latest published report of National Crime Records Bureau (NCRB) which is published in the year of 2020, the total number of child pornography/rape and gang rape complaints lodged in the National Cybercrime Reporting Portal (NCRP) is 13244 in 2020. A Child line India Foundation (CIF) reported that it received 3941 calls regarding child sexual cases in 2020, in most of the calls children are not able to express what happened to them but they know a wrong has been committed against their body.

Legislative Measures:

India being a signatory to the convention on the Rights of the child and having ratified the "Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography" introduced section 67B to the Information Technology Act, 2000. It is a penal provision to punish that offence. This provision also states children means – a person not completed the age of 18. As per section 67B, such offence is punishable with imprisonment of five years and fine extends to ten lakhs on first conviction. On subsequent conviction, it is punishable with imprisonment of seven years and fine extends to ten lakhs. Additionally, Sections 13, 14 and 15 of The Protection of Children from Sexual Offences Act, 2012 penalise cyber child pornography in several aspects.

5. Cyber Stalking

Cyber stalking is a crime in which someone stalks or harasses a victim using electronic devices such as email, social media, Internet and so on. Stalking means

"the act of threatening, harassing, or annoying someone through multiple e-mail address, as through the internet, especially with the intent of placing the recipient in fear that an illegal act or an injury will be inflicted on the recipient or a member of the recipient's family or household." Cyber space makes stalking easy and anonymous. Cyber stalkers can track the victim's locations and follow them online, monitor the victim's online activities and plan to commit serious offences. Stalkers can plan to commit serious offences against the victims because they completely know about such victims. So, stalking should not be ignored by the victims. Inexperienced web users, emotionally weak persons and young children are the usual victims.

In most of the cases the cyber-stalker and the victim have a prior relationship and the cyber-stalking begins when the victim attempts to break off the relationship. Mrs. Ritu Kohli's Case was one of the cases which attained the focus of India about cyber stalking . In this case cyber-stalker Manish Kathuria, chatted Mrs. Ritu Kohli under the username of her name in micr online chatting platform and continuously sending obscene messages and he posted her telephone number in internet, she received several obscene phone calls from India and abroad, the Delhi police arrested him under section 509 of the Indian Penal Code. This case was registered before the enforcement of Information Technology Act, 2000. Such incidents frequently take place. Notably, online harassment of Sharmistha Mukherjee who is the daughter of Former President Pranab Mukherjee attracted national attention. A Cyber stalker sent a sexually explicit messages to her Facebook profile, first she decided to ignore that message and block him, but later she decided silence is not a solution for this problem so she publicly shares the screenshots of that message in Face book and tag him in that post. This sensational incident denotes no one is safe in the cyberspace. Cyber stalking is one of the offences which is aiding other offences. Once cyber stalkers collect personal information of the victim successfully, they are able to commit any offences against him.

Legislative Measures:

India did not have the provisions for penalising Stalking before 2013. But, after the Nirbhaya incident in December 2012. Justice J.S. Verma committee was set up for strengthening the laws for curbing crimes against women. Based on the recommendation of this committee, section 354D was inserted in Indian Penal Code. As per this section, physical stalking and cyber stalking are penalised, which shall be punished with imprisonment which may extend to three year and fine on first conviction. And on subsequent conviction, imprisonment which may extend to five year and fine. But this provision is not gender neutral it only covers cyber stalking against women by men, it is silent in other cases like cyber stalking against women by women and men by men.

Conclusion

Now, we have technologically advanced lifestyle, every day the new technologies are innovated and infused with our life. Criminals also utilise such

technological advancements. A clear view has been given over newly emerged cybercrimes and its legislative measures in India. As earlier explained, India does not have fully evolved penal statutes for penalising some cybercrimes. Especially AI aided crimes and cyber grooming did not effectively penalise by any statutes of India. Committees should be constituted by the government. Such committees should consist of expert members from the field of law and technology. Legislation should enact dedicated penal statutes to penalise those newly emerged cybercrimes effectively.

References

1. Avishek Kumar, (2023, November 30), Sextortionists target senior citizen with retd IPS officer's deepfake, The Times of India, https://timesofindia.indiatimes.com/city/ghaziabad/retired-ips-officers-deepfake-used-to-blackmail-senior-citizen/articleshow/105603283.cms

2. Collin, B. C. (1996), "The Future of cyber terrorism", Proceedings of 11th Annual International Symposium on Criminal Justice Issues, The University of Chicage, IL.

3. Kaplan, D. (2003, June 2), "Playing Offense: The Inside Story of How US Terrorist Hunters are Going After Al-Qaeda", US News and World Report, p 19-29,42.

4. Verma, A. (2012), "Cyber Crimes in India", Central Law Publication, 1st Edn., p.138.

5. Hallevy, G. (2015), "Liability for Crimes Involving Artificial Intelligence Systems", Springer Publication, p.118.

6. HT Correspondent, (2016, August 15), Police register FIR against Sharmistha's online stalker, Hindustan Times, https://www.hindustantimes.com/nation-newspaper/police-register-fir-against-sharmistha-s-online-stalker/story-jUULxFJJuSIV9AYMPrOn9I.html

7. National Society for the Prevention of Cruelty to Children, (2023, August 15), 82% rise in online grooming crimes against children in the last 5 years, NSPCC of U.K., https://www.nspcc.org.uk/about-us/news-opinion/2023/2023-08-14-82-rise-in-online-grooming-crimes-against-children-in-the-last-5-years/

8. Press Information Bureau, (2020, September 22), Sexual Abuse Cases of Children Reported Online (Release ID: 1657679), Ministry of Women and Child Development India, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1657679

9. Press Information Bureau, (2022, March 16), Online Cyber Grooming of Women and Young Children (Release ID: 1806602), Ministry of Women and Child Development India, https://pib.gov.in/PressReleasePage.aspx?PRID=1806602

10. Bendrath, R. (2001, January), "The cyberwar debate: Perception and politics in US Critical Infrastructure Protection," Information & Security An International Journal. Volume 7, p. 80-103.

11. Tech Desk, (2023, July 29), What is FraudGPT, dark web's dangerous AI for cybercrime?.The Indian Express, https://indianexpress.com/article/technology/artificial-intelligence/what-is-fraudgpt-dark-webs-dangerous-ai-for-cybercrime-8866138/