International Journal of Enhanced Research in Educational Development (IJERED)
ISSN: 2320-8708, Vol. 12 Issue 2, Mar.-Apr, 2024, Impact Factor: 8.376

The Role of Indian Government in the Prevention of Cyber Crime

Vaidehi Sharma

Bharati Vidyapeeth Deemed To Be University, New Law College Pune

ABSTRACT

The purpose of the paper is to analyse the increasing cases of cybercrime and also how the government delas with the increasing cases cybercrimes, i.e. the prevention taken by Indian government to deal with the ongoing cybercrimes. Between March and April 2020, India has witnessed a staggering 86% increase in cyber-attacks. According to the UN Special Reporter, women are both disproportionately targeted by online violence and suffer disproportionately serious consequences as a result. Cybercrime has real consequences and costs. It undermines women's wellbeing, their rights, and their progress in all aspects of life. Cyber violence results in psychological, physical, sexual or economic harm to women. Given the push towards digitisation, amongst the ongoing pandemic, more women and girls are using the internet for varied purposes including education, work, and financial transactions, amongst others. Many of these women and girls could be first-time users and/or may have a limited understanding of good practices when interacting with others in cyberspace and could be subjected to cybercrimes. Online frauds have seen an advancement.This working from home has now become an opportunity for cybercriminals to exploit the people through e-mail scams, hacking passwords, phishing, ransom attacks, online sexual harassment, etc. Thus, it makes government intervention very necessary to stop the ongoing cybercrimes. Several measures have been taken by the government so as to stop these crimes. Many sites have been created by the government so that the people suffering from cybercrimes can visit those sites and seek help from them.

INTRODUCTION

Cybercrime is any criminal act that involves a computer, network or networked devices.
Cybercrimes are increasing rapidly and because of the rapid increase in cybercrime, government intervention is necessary to ensure the safety and security of individuals and organizations. Cybercrime impacts various sectors such as finance, healthcare centres and even national security. As in today's time everyone is going digital i.e. almost all people are on computers, laptops or on their mobile phones. Almost all the work can be done digitally without much efforts. Thus, people prefer being digital. And there is nothing wrong in using the technology as the technology is developed for helping human beings. But people need to take precautions while being digital as cybercrimes are growing rapidly. Government has taken many precautions to help people who are suffering from cybercrime. Many people are facing the challenges that comes from cybercrime. This research paper aims to explore the different measures that are undertaken by the Indian government to protect people from cybercrime. Government has even launched a cybercrime portal. The Ministry of Home Affairs has also launched www.cybercrime.gov.in the national cybercrime reporting portal(NCRP) which allows 24*7 reporting of all types of cybercrime, with special focus on cybercrime against women and children. People tend to provide and/or give permissions to access their personal information readily available on their phones, laptops and/or social media accounts in order to use the services provided by the applications. Also, during the time of lockdown people are accessing social media websites such as Instagram, Facebook, Twitter, etc.

These cybercrime activities have opened the door for spyware and ransom ware attacks. A spyware steals sensitive personal data of the user while, ransom ware takes control over the login and other vital credentials of a person. These attacks may result into huge losses to people not only financially but also otherwise. All these crimes are caused by computers. Computer crime alternatively referred to as cybercrime, e-crime, electronic crime, or hi-tech crime. Computer crime is an act performed by a knowledgeable computer user, sometimes referred to as a hacker that illegally browses or steals a company's or individuals' private information. Computer crime describes a very broad category of offenses.

Understanding cyber crime
Cybercrime refers to criminal activities that are conducted through digital means, typically involving the use of computers or networks. It consists of a wide range of illegal activities such as hacking, identify theft, online fraud and

some other malicious software. The advancement of cybercrime has helped people a lot but has also provided cybercriminals with new tools and techniques to carry out illegal activities. Understanding the motivations and mindset of cybercriminals can help in the development of effective prevention and intervention strategies. Thus, it is essential to gain insights into the psychological and sociological factors that drive individuals to engage in cyber-criminal behaviour.

Cybercrime is also taking place with the teenagers who did not pay attention to the precautions that can be taken against the cybercrime. And it's not just the problem with the teenagers but with everyone. Many times, these criminals take peoples photos from various social media platforms and use them illegally with wrong intention which can cause a lot of trouble in someone's life. As said technology has helped us with many things but has also provided cybercriminals a platform where they illegally disturb other people's life by using their information that is posted by them on various social media platforms and sometimes, they even use pictures that are posted by people on various social media platforms.

Cybercrime needs to be stopped and for that government intervention is necessary.These kinds of online crimes can lead to harassment, defamation, suicide, etc. Online frauds are conducted by people who can destroy some ones life by doing these kinds of crimes.

Indian Governments Initiatives in cybercrime prevention: -
The Indian government has taken several initiatives to address the issue of cybercrime and enhance cyber security in the country. One of the significant steps taken in this regard is the establishment of Cyber Coordinate Centre (CCC), under the Ministry of Home Affairs. The CCC serves as a central hub for receiving, analysing, and disseminating information relating to cyber threats and incidents. It collaborates with various law enforcement agencies, including the Central Bureau of Investigation and the National Crime Record Bureau, to investigate and prosecute cyber criminals. Additionally, the government has introduced the National Cyber Crime Reporting Portal, where citizens can report cybercrimes and seek assistance (Ministry of Electronics and Information Technology, Government of India). This platform not only ensures easy reporting of cyber incidents but also provides valuable data for analysis and policy making. Moreover, the government has initiated capacity building programs and workshops to enhance the skills and knowledge of law enforcement and agencies dealing with cybercrimes. These initiatives collectively aim to strengthen the cyber security infrastructure in India and effectively combat cybercrime.

Government is still in the process of developing these kinds of cells which can help people to get rid of cybercrimes especially the youth. As the youth is so into the social media, that they forget to take precautionsregardingcybercrimes. Thus, it makes government to make them understand or transfer them some knowledge about the cybercrimes taking place.

And also in the rural areas, where most of the people are not aware of the cybercrime taking place. There the government should take initiative to make them understand about the crimes that can take place through the internet. Government can use projectors to make people understand in large.

Legislative measures and Cyber Crime Prevention
Legislative measures play a crucial role in the prevention of cybercrime in India. The government has enacted several laws and regulations to protect individuals and organizations from cyber threats. The Information Technology Act, 2000 is the primary legislation governing cybercrimes in the country. It provides legal recognition for electronic transactions and lays down penalties for offences such as hacking, identity theft, and online fraud. Additionally, the government has established the Cyber Appellate Tribunal to adjudicate cybercrime cases and ensure speedy justice. Furthermore, the national cyber security policy, launched in 2013, aims to create a secure cyberspace for citizens and promote collaborative efforts between the government, industry. These legislatives measures demonstrate the Indian government's commitment to combating cybercrime and safeguarding its citizens digital life.

Law Enforcement and Cyber Crime Prevention: -
Law enforcement agencies play a crucial role in the prevention and investigation of cybercrimes. They are responsible for identifying and apprehending cyber criminals, as well as gathering evidence to support legal proceedings. In India, the Information Technology Act,200 provides the legal framework for addressing cybercrime (Ministry of Electronics and Information Technology, Government of India). The act empowers law enforcementagencies with the authority to investigate and prosecute cybercrimes. Additionally, the establishment of specialized cybercrimecells within police departments has enhancedthe capabilities of law enforcement in dealing with cybercrime. These units are equipped with the necessary expertise and resources to investigate cyberattacks and track down offenders. Effective collaboration between law enforcement agencies and other stakeholders, suchas private sector organisations and international counterparts, is also essential for maximized cybercrime prevention. By working together, these entities can share information, exchange best practices, and coordinate efforts to combat cybercrime on a global scale.

Law enforcement can help help a lot to stop these crimes that are taking place on daily basis. Several acts have been enforced by the government to protect people from cybercrime. As cybercrimes is a very harmful crime that can make a person commit suicide, or do such acts that are not good for the person or the near and dear ones. Or sometimes these cybercrimes are conducted ona person to defame the person that can lead to a huge loss.

Public Awareness and Cybercrime Prevention

Public awareness plays a crucial role in preventing cybercrime. Educatingthe public about the various types of cyber threats and their potential impacts can help in reducing the number of victims fallingprey to cybercriminals. Government agencies, educational institutions, and cybersecurity organisations can collaborate to conduct awareness campaigns, workshops and training programs to disseminate information about cybercrime prevention strategies. Additionally, the government should invest in creating user friendly and accessible resources such as websites, brochures, and mobile applications that provide information on best practices for online safety. Thes initiatives can empower individuals to protect themselves and their personal information from cyber threats. Increased public awareness can also contribute to a safe digital environment by fostering a sense of responsibility and encouraging the reporting of cybercrimes to relevant authorities.

And in rural areas government with help of the projectors can spread information about the cybercrimes that are taking place and how can they get rid of the crimes that are taking place as it is very important to make people aware about all these things that are taking place. As they can prove to be dangerous for people.

As many cases of cybercrime have been seen where people commit suicide because of shame, that is they feel defamed. Thus, public awareness is very necessary amongst people,people need to be educated about every small thing as it is rightly said, “Education is notpreparation for life; education is life itself.” Educating people can help a lot in the growth of the society and can lead to a better future. Educated people can fight against cybercrimes too. As they are aware that what should be done if someday that have to face such a situation. Government should take the initiatives of spreading awareness about education and should make education free for the people who are unable to afford it.

CASE LAWS RELATING TO CYBER CRIME

State of Tamil Nadu v. Suhas Katti

The instant case is a landmark case in the Cyber Law regime for its efficient handling made the conviction possible within 7 months from the date of filing the FIR.

Facts: The accused was a family friend of the victim and wanted to marry her but she married another man which resulted in a Divorce. After her divorce, the accused persuaded her again and, on her reluctance, to marrying him, he took the course of harassment through the Internet. The accused opened a false e-mail account in the name of the victim and posted defamatory, obscene, and annoying information about the victim.

A charge-sheet was filed against the accused person under Section 67 of the IT Act and Section 469 and 509 of the Indian Penal Code, 1860.

Decision: The Additional Chief Metropolitan Magistrate, Egmore convicted the accused person under Section 469 and 509 of the Indian Penal Code, 1860 and Section 67 of the IT Act. The accused was subjected to the Rigorous Imprisonment of 2 years along with a fine of Rs. 500 under Section 469 of the IPC, Simple Imprisonment of 1 year along with a fine of Rs. 500 under Section 509 of the IPC, and Rigorous Imprisonment of 2 years along with a fine of Rs. 4,000 under Section 67 of the IT Act.

CBI v. Arif Azim (Sony Sambandh case)

A website called www.sony-sambandh.com enabled NRIs to send Sony products to their Indian friends and relatives after online payment for the same.

In May 2002, someone logged into the website under the name of Barbara Campa and ordered a Sony Colour TV set along with a cordless telephone for one Arif Azim in Noida. She paid through her credit card and the said order was delivered to Arif Azim. However, the credit card agency informed the company that it was an unauthorized payment as the real owner denied any such purchase.

A complaint was therefore lodged with CBI and further, a case under Sections 418, 419, and 420 of the Indian Penal Code, 1860 was registered. The investigations concluded that Arif Azim while working at a call centre in Noida, got access to the credit card details of Barbara Campa which he misused.

The Court convicted Arif Azim but being a young boy and a first-time convict, the Court’s approach was lenient towards him. The Court released the convicted person on probation for 1 year. This was one among the landmark cases

of Cyber Law because it displayed that theIndian Penal Code, 1860 can be an effective legislation to rely on when the IT Act is not exhaustive.

CONCLUSION

In conclusion, the Indian government plays a crucial role in the prevention of cybercrime. Through the implementation of various cybersecurity measures and legislation, it has made significant strides in creating a safer digital environment for citizens. The establishment of CERT-IN has been instrumental in coordinating efforts to detect, prevent, and respond to cyber threats. Additionally, the government has collaborated with international organisations and agencies to enhance its cybersecurity capacity and knowledge sharing. However, there is still much work to be done to address the ever-evolving nature of cybercrime. The government should continue to invest in research and development, forge stronger partnerships and industry experts, and educate the public about online safety. With sustained efforts the Indian government can effectively combat cybercrime and ensure the protection of its citizens in the digital era.

REFERENCES

[1]. https://www.researchgate.net/publication/351902133_CYBER_CRIMES_IN_INDIA_TRENDS_AND_PREVENTION
[2]. https://enhelion.com/blogs/2021/03/01/landmark-cyber-law-cases-in-india/
[3]. Cybersecurity Laws and Regulations Report 2024 India (iclg.com)
[4]. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india
[5]. Cybersecurity and Infrastructure Security Agency – Wikipedia
[6]. Steps Taken to Deal with Cyber Crime and Cyber Security (pib.gov.in)
[7]. Indian government initiatives on cyberbullying: A case study on cyberbullying in Indian higher education institutions - PMC (nih.gov)