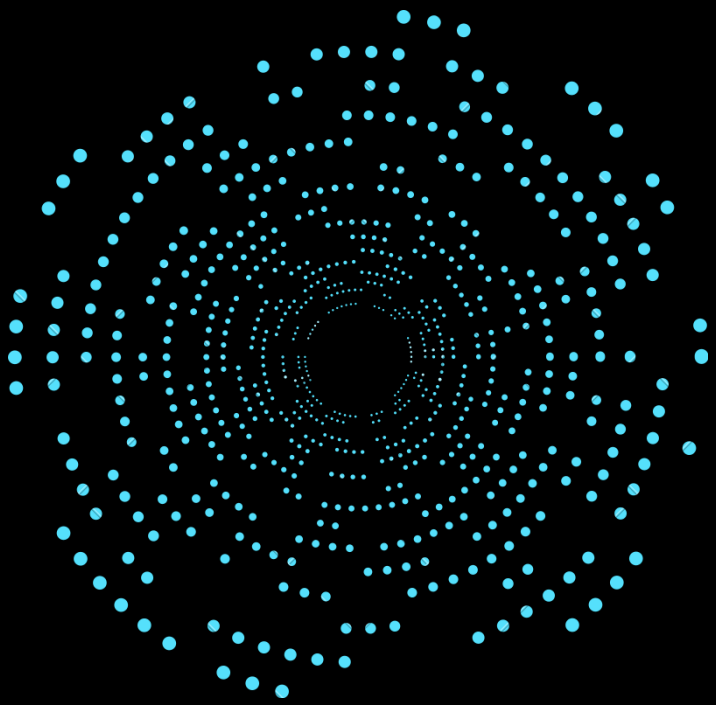
INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY



VOLUME 1 AND ISSUE 1 OF 2023

INSTITUTE OF LEGAL EDUCATION

International Journal on Cyberspace Law and Policy

(Free Publication and Open Access Journal)

Journal's Home Page – https://ijclp.iledu.in/

Journal's Editorial Page - https://ijclp.iledu.in/editorial-board/

Volume 1 and Issue 1 (Access Full Issue on - https://ijclp.iledu.in/category/volume-1-and-issue-1-of-2023/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education (Established by I.L.E. Educational Trust)

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY

Volume I and Issue I of 2023

ISBN - 978-81-960677-4-8

Published by

Institute of Legal Education

https://iledu.in

Need of Cyber Law in the Era Of Technology

Author - Utsav Biswas, Student Of Gujarat National University Of Law, Silvassa

Best Citation - Utsav Biswas, Need of Cyber Law in the Era Of Technology, *International Journal on Cyberspace Law and Policy,* 1 (1) of 2023, Pg. 43-47, ISBN - 978-81-960677-4-8.

Abstract

Today the 21st century is also known as the era of technology it's a place that is connected by digitalization, networking which brings benefits in various fields such as science and technology, commerce, communication, and so on but with these, it also gives rise to a new criminal methodology which is known as cybercrime which is spreading like a wildfire in today's time. Preventive measures have been taken to combat this crime such as "The IT Act of 2000", "National Cyber Security Policy" etc but still, there are some loopholes that are preventing these laws to work efficiently. Given the serious nature of cybercrime and its worldwide character and repercussions, It becomes clear that to combat this we need to have a common understanding of this criminal conduct. This article focuses on the challenges to cyberspace and cybercrime which needs to be reformed and the current legislation of cyberlaw in India and how can it be made efficient to combat cybercrime.

Keywords: Cyber Law, Cyber Crime, Need for Reforms, Era of Technology, Preventive Measures.

Introduction

On January 1, 1983, the internet celebrated its first official birthday since then it has come a long way to the 21st century when everyone is dependent on it. The scenario of technological development is booming positively but every coin has two sides. The Internet also brought with it a place called cyberspace which had few loopholes and through these loopholes, selected individuals started exploiting it and introduced to the world a new crime haven called "CyberCrime".Since then the pace of cybercrime has continued to rise. As cybercrime neither has reference nor origin in the law the more significant it becomes to take action regarding this. Cybercrime has become a common occurrence in modern India criminals not only cause significant harm to society but are also able to disguise their identities. A variety of crimes such as unauthorized access and hacking, Trojan attack, Virus attack, etc. Are being carried out by them. In a broader sense, cybercrime can be defined as any illicit conduct in which a technological device such as computers, mobile phones, etc, or the internet is used as a tool or target to cause harm. In some cases "Cybercrime" has been construed by Indian courts but the same is not present in any Indian Act or Statute. Cybercrime is an evil that is rooted in people's dependence on technology for their convenience. According to the tactical aspect attacks on digital networks for seizing control or destroying infrastructures which are crucial for governments are also being targeted by these lawbreakers. In July 2013 the government published a national cyber security policy and just after that it was reported that government officials' emails had been hacked. In this steady increase in the number of cyber crimes, it is expected that all the stakeholders will come together in a forum to discuss this issue and find an adequate solution regarding these evil deeds.

A. What is a Cyber Crime And Its Types

Cybercrime is generally defined as crimes that are committed through the usage of technological devices for personal profit or causing harm.

B. Types of Cyber Crimes

- Cyberbullying: When a person harasses or bullies others through the medium of electronic devices like computers, mobile

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY
Volume I and Issue I of 2023
ISBN - 978-81-960677-4-8
Published by
Institute of Legal Education
https://iledu.in

phones, laptops, etc is called a cyber bully. Generally speaking, cyberbullying refers to bullying through the means of technology such as social media, online messaging platforms, gaming platforms, etc, cyberbullying is used to scare, humiliate or anger the victim.

- Child Pornography: Children are the easiest target of these lawbreakers as they can be lured and manipulated easily by them. They lure the children into secret chat rooms where they befriend them and sexually exploit them for pornography videos and images.
- Cyberstalking: It is an act of harassing or stalking another person online. Cyberstalker does not pursue their victims physically, after online interaction the cyberstalker utilizes vital information to intimidate the victim.
- Phishing: This fraud involves the appearance of mail from a legitimate source but contains malicious attachments that when opened steal personal information like bank account details, IPIN, ID, etc.
- Vishing: In vishing, the victim's vulnerable information is stolen from smartphones by calling the victims and impersonating them as government officials, bank clerks, etc.
- Smishing: It's a fraud where a text message is used to trick its victims into visiting malicious websites, emails, etc.
- Identity Theft: When a person impersonates someone else to get vital information about the person is called Identity theft.
- Hacking: It's a technique where the hacker hacks someone else technological property such as mobile phones, computers, laptops, etc to gain access to their information without the consent of the owners.
- Cyber Defamation: When someone commits slander or Libel through electronic means it's called cyber defamation.

C. Preventive Measures Against Cyber Crimes

- Refrain from sharing vulnerable details: It's one of the simplest tasks we can use to prevent scammers from duping us. We need to make sure that we are not indulging in sharing our personal and vulnerable details like banking details etc to anonymous sources or strangers.
- Sharing of OTP: One of the common mistake people makes is sharing their OTP with anyone which makes them an easy target for scammers. Hence, we need to make sure we just don't share our OTP with anyone as OTP can lead them to access our vulnerable information.
- Legal Actions: As discussed above there are various provisions in IPC and IT Act regarding cyber crime like section 66, section 43, section 65, section 379, and section 417 hence reporting them to the responsible authority is the best way to catch these scammers.
- Updating Passwords: Make sure to update your password as the same and constant password can be easily hacked and used to steal vulnerable details hence updating the password does not give rise to this grim occasion.
- Use of AI and Machine Learning: AI and Machine Learning – driven technologies can be used for scams

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY
Volume I and Issue I of 2023
ISBN - 978-81-960677-4-8
Published by
Institute of Legal Education
https://iledu.in

and fraud detection which can help in finding and preventing fraud by analyzing customer data these technologies detecting accuracy can be increased.

D. Cyber Crimes Laws In India

With such harmful nature of cyber crimes happening in India, the government launched some cyber laws to combat this crime. These strict laws govern the use of cyberspace and supervise the spread of information in the sectors of software, Information Technology, E-commerce, and Financial Transactions. One such important act is the "Information Technology Act of 2000" which states "To provide Legal Recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as electronic methods of communication and storage of information, to facilitate electronic filing of documents with the government agencies and further amend the Indian penal code, the Indian Evidence Act 1872, the Banker's Book Evidence Act 1891 and the Reserve Bank of India Act 1934 and for matters connected therewith or incidental thereto". However, with each passing time, several amendments have been made to the legislation.

1. Important Sections of the IT Act

- Section 43- When someone destroys the computer of another, without the consent of the owner he/she is charged with sec. 43
- Section 66- If someone fraudulently or dishonestly does any act mentioned in section 43, he shall be imprisoned for a term that can extend to 3 years or with a fine which may extend to five lakh rupees or both.
- Section 66B- If someone fraudulently receives stolen technological devices or computers. He shall be imprisoned for a term that can extend to 3 years or a fine which may extend to 1 lakh rupees.
- Section 66C- If someone commits the crime of digital signatures forgery, hacking, and identity theft he shall be imprisoned which may extend to 3 years or a fine which may extend to 1 lakh rupees.
- Section 66D- if someone cheats the victim by personation using computer resources he will be charged with sec. 66D and shall be imprisoned which may extend to 3 years or a fine upto 1 lakh rupees
- Section 66E- Clicking pictures of someone's private areas and publishing or transmitting them without the person's consent will be punishable under this section and shall be imprisoned for three years or a fine up to 2 lakh rupees.
- Section 66F- If someone commits cyberterrorism he shall be punishable under this section and can be imprisoned for a lifetime.
- Section 67- If someone publishes obscenities electronically he shall be convicted under section 67 and shall be imprisoned which can extend up to five years and the fine is up to 10 lakh rupees.

2. Indian Penal Code, 1860

If the IT Act is not sufficient to cover specific cyber crimes, Governments can use the IPC,1860 following sections-

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY
Volume I and Issue I of 2023
ISBN - 978-81-960677-4-8
Published by
Institute of Legal Education
https://iledu.in

- Section 292: If someone publicly published or transmitted obscene material, sexually explicit acts, or exploits of children he shall be punishable under this section the penalty is imprisonment for two years and a fine of 2000 rupees, and for second-time offenders imprisonment upto five years and a fine of five thousand rupees.
- Section 354C: If someone takes pictures of private parts or sexual actions of a woman without her consent and if someone commits voyeurism he shall be punished under this section the punishment for first-time offenders is three years imprisonment and for second-time offenders, it is seven years imprisonment.
- Section 354D: If someone tracks a female using social media, email, or any other electronic means and attempts to contact her without her consent he commits the crime of cyberstalking. First-time offenders are punished with imprisonment for up to three years and a fine and second-time offenders face imprisonment of five years and a fine.
- Section 379: If someone hijacks electronic devices with the motive of stealing someone's data they are punished under this section with imprisonment of three years in addition to a fine.
- Section 420: If someone creates fake websites and uses them to commit cyber fraud and steals the victim's data using it he is charged under this section with imprisonment of seven years along with a fine.
- Section 463: If someone falsifies some documents electronically such as spoofing emails he is charged under this section with imprisonment of up to seven years and a fine.
- Section 465: If someone commits forgery along with spoofing email and prepares false documents he is charged under this section with imprisonment of two years and a fine.

E. Budapest Convention on Cyber Crime

The Budapest Convention on Cybercrime was the first international treaty on cybercrime which was signed on 23 November 2001. It aimed to address the growing issue of cybercrime around the globe and harmonize international and national laws by improving investigative techniques and increasing cooperation among different nations. It was drawn up by the "Council of Europe" in Strasbourg along with its observer parties such as Canada, Japan, etc. And finally, on 1 July 2004, it was entered into force. Since then 67 countries have ratified it. India has declined to ratify it by stating the reason that India was not involved in the drafting process.

3. Objectives Of the Convention

The objectives of the Budapest Convention are as follows:

- It deals with the issue of copyrights, computer fraud, child pornography, hate crimes, hacking, etc.
- It pursues a common policy against cybercrime to protect society by adopting efficient legislation and fostering it.
- It connects the provisions regarding cybercrime along with other substantive criminal elements by synchronizing domestic laws.
- Providing procedural criminal law under the domestic system for the investigation and prosecution of cybercrime offenses and collecting evidence for the same.
- Setting up a forum for international cooperation regarding cybercrime.

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY
Volume I and Issue I of 2023
ISBN - 978-81-960677-4-8
Published by
Institute of Legal Education
https://iledu.in

- The convention also ascertained the provision of safeguarding human rights and liberties.

Conclusion

As we move forward with time so will the development of technology and the internet and with that new mediums or new cybercrime will emerge as the internet is a worldwide phenomenon. Cybercrime has the capacity to destroy every aspect of life as it is easy to commit but difficult to detect. Our lawmakers when making the law didn't envision the advent of the internet and how it can be misused not only that it has also led to sensitive legal issues in our country and other nations which necessitate the ratification of efficient cyber laws which will go under constant up-gradation and refinement to keep pace with technological development. It's impossible to completely eradicate cybercrime but what we can do is examine them and enact better legislation to combat it that can only happen when all the stakeholders including common people, businesses, and governments work together synchronously also we need to make sure that legislation becomes so strict and severe for cyber law that it stifles the growth of various industries and infringes the right of citizens.

References

(i) Ipleaders, https://blog.ipleaders.in/cyber-crime-laws-in-india (5th Feb 2023).
(ii) Legal Service India E-journal, https://www.legalserviceindia.com/legal/article-1019-importance-of-cyber-law-in-india.html (5th Feb 2023).
(iii) IndianKanoon, https://indiankanoon.org/doc/1965344/ (6th Feb 2023).
(iv) IndianKanoon, https://indiankanoon.org/doc/1569253/ (6th Feb 2023).
(v) Ruchi Nehra, *Cybercrimes and Cyber Laws in India*, Probono India (6th Feb 2023, 7:27 PM), https://probono-india.in/blog-detail.php?id=218.
(vi) Meity, https://www.meity.gov.in/content/cyber-laws (6th Feb 2023).
(vii) Lexology, https://www.lexology.com/library/detail.aspx?g=4af6c044-dc77-4b1a-9288-986395eff8d1 (7th Feb 2023).
(viii) InsightsIAS, https://www.insightsonindia.com/2019/11/22/budapest-convention-on-cyber-security/ (7th Feb 2023).
(ix) Vijay Pal Dalmia, *Data Protection Law In India- Everything You Must Know*, Mondaq(7th Feb 2023, 8:30 PM), https://www.mondaq.com/india/data-protection/655034/.