Journal of Advances and Scholarly Researches in Allied Education
Vol. 20, Issue No. 2, April-2023, ISSN 2230-7540

Challenges and Solutions of Cyber Crime in Indian Jurisprudence

Dr. Anil Kumar Jeph[1]*, Renu Vijaywargia[2]

[1] Supervisor, Professor, Govt. Law College, Raj Rishi Bhartrihari Matsya University, Alwar-301001, Rajasthan

[2] Research Scholar, Raj Rishi Bhartrihari Matsya University, Alwar-301001, Rajasthan

Abstract - There is a balance of good and evil in life. The web is, too. Cyberspace has many positive uses, but it also has some negative ones. However, since there are no police officers monitoring the Internet as there are in traditional neighborhoods, anything from Trojan horses and viruses to cyber stalking, trademark counterfeiting, and cyber terrorism may flourish online. If we want to avoid becoming victims of online crime, now is the moment to educate ourselves on the dangers posed by both deliberate and careless actions. Cybercrime is a product of technology, and without it, its investigation and regulation would be impossible. Although India's legal system is inadequate at the present, it may serve as a powerful deterrence against such acts..

Keywords - Cyber Space, Cyber Crime, Hacking, Intellectual Property Rights, Information Technology Act,2000.

----------X----------

INTRODUCTION

One of the most credible Indian administrative treatises is Kautilya's Arthashastra, which dates back to about 350 B.C. and details the numerous crimes committed by society, the security efforts that rulers may take to prevent these crimes, the different types of crimes that can occur inside a state, etc. It also supports the use of differential sanctions for the various offenses specified. The issue of compensation for victims' losses is also examined.

According to his thesis of likely crime, criminal behavior evolves with civilization. To emphasize women's precarious social standing, it predicts an uptick in crimes targeting them; conversely, a dominant group's misuse of its power will lead to an increase in crimes targeting other powerful groups.

It's undeniable that the rise of ICT has spawned a new kind of criminal activity known as Cyber Crime. In order to fully understand what we mean when we term "Cyber,"

To truly understand Cyber Crime, one must first understand what is meant by the term "crime."

Blackstone a breach of a public law that either prohibits or commands the conduct to be done is defined as a Crime.

Stephen A criminal act is "a violation of a right considered in reference to the evil tendency of such violation as regards the community at large," as described by one source.

In general, there are three ways to define a Cyber Crime:

1. ***Target Cyber Crime***: An offense in which a computer is used as the instrument of commission.

2. ***Tool Cyber Crime*:** When a computer is used to aid in the commission of a crime, that crime is called "computer crime."

3. ***Computer incidental***: It's a crime in which the computer is used in a very minimal way.

Statutory Provisions in India and its Analysis[1]

An email-borne virus infected approximately 45 million computers across the globe in the late 1990s, marking the first widely publicized case of cybercrime.

The Information Technology Act of 2000 is India's primary statute governing the conduct of business through the Internet and other electronic means of communication ("electronic commerce"). validity in law.'[xxxv] The Act also aimed to change the

[1] Justice K. S. Puttaswamy(Retd) vs Union Of India And Ors. on 24 August, 2017.Available at https://indiankanoon.org/doc/91938676/.

Reserve Bank of India Act of 1934 and the Banker's Book Evidence Act to make them consistent with this Act, as well as the Indian Penal Code and the Indian Evidence Act. Cyberspace in India was mostly ungoverned until the year 2000. Users of the internet [xxxvi] should rest easy however, for many of their concerns have been addressed by the Information Technology (Amendment) Act, 2009. The legislation effectively regulated online business in India. It's also a defense mechanism against cybercrimes, but with some caveats. Important provisions of the I.T. Act addressing cybercrime may be found in chapters IX and XI, including sections 43, 65, 66, and 67. We will focus our discussion of the law only on the aforementioned sections.

There aren't many exceptions or stipulations in the law,

1. There are a total of 94 sections throughout 13 chapters in the Act. Nonetheless, the document's primary focus is on facilitating online trade. The definition of cybercrime and the punishment for it may be found in just two chapters (9 and 11). Because of this, it seems that the major goal of legislation was not to prevent and punish cybercrimes, but rather to encourage and control e-commerce.

2. Section 79 of the Act exempts "Intermediaries" from liability for certain cybercrimes. Because of its status as a "Intermediary," cyber cafes are already subject to the regulations established in Section 79, which outline the duties and conduct expected of such businesses. More comprehensive regulations for internet cafés are needed from each states.[xxxvii]

3. The legislation prohibits pornography on Indian websites but allows it on international sites with little to no discussion. This allows Indian cybercriminals the option of hosting pornographic websites outside of India, where they won't face legal repercussions.

4. The CrPC prohibits warrantless searches of residences. No enhanced search warrant authority is granted to law enforcement agencies under this statute. Most cybercriminals work from private residences, which law enforcement is unable to raid.

Criminal Liabilities under Information Technology Act, 2000[2] [2]

- Sec.65: Modifying original computer-based records.

- Sec.66: Computer hacking, data modification, and various forms of computer-related espionage.

- Sec. 66A: Consequences for Disturbing Others through Electronic Means.

- Sec. 66B: Consequences for the dishonest acquisition of a stolen computer, network component, or mobile device.

- Sec. 66C: Theft of personal information penalties.

- Sec. 66D: The Consequences of Using a Computer to Commit Identity Theft.

- Sec. 66E: Privacy Invasion Penalties.

- Sec. 66F: Cyberterrorism Consequences.

- Sec.67: Distributing sexually explicit material.

- Sec. 67A: Consequences of disseminating or sharing digital content that depicts or describes sexually explicit acts, etc.

- Sec. 67B: Punishment for Child Pornography

- Sec. 67C: Preservation and Retention of Information by Intermediaries

- Sec.70: Un-authorized access to protected system

- Sec. 70A: National Nodal Agency

- Sec. 70B: CERT-in

- Sec. 71: Penalty for Misrepresentation

- Sec.72: Breach of Confidentiality and Privacy

- Sec.73: Publishing false digital signature certificates

- Sec. 74: Publication for fraudulent purposes

The criminal provisions of the IT Act and those dealing with cognizable of fences and criminal acts follow from Chapter IX titled “Offences”

Impact of Information and Communication Technology on Society

The Internet is the most massive anarchist experiment ever run, and it's also the first thing that humans have built that they can't fully understand. The development of the Internet and the proliferation of other information technologies have had profound effects on society. It's levelling the playing field for business and making it simpler for people all around

[2] The Information Technology Act, 2000

the globe to communicate and collaborate, regardless of their economic standing, physical location, or the length of time that has passed since they last saw each other. A new international marketplace has emerged thanks to cyberspace, the merging of computers, networks, and people. Technologies based on cyberspace are increasingly being used by governments, businesses, and communities everywhere. It's altering people's views on security and economic growth, and it's creating new opportunities for both. It has also increased availability of tools for enhancing government and public welfare on a worldwide scale. Indeed, the rise of the internet has allowed for more R&D&I possibilities, which has resulted in tremendous economic development and prosperity, and has also enabled educated communities to spread rapidly around the world. (WEF, 2014).

Organizations will need to review and update their data protection policies and codes based on the type of personal data being processed, as the revised principles call for the appointment of a Data Protection Officer by the Significant Data Fiduciary and the implementation of appropriate technical and organizational measures to prevent data misuse. On August 23, 2017, in the seminal case Justice K.S. Puttaswamy (Ret.) v. Union of India (Case NO- WP (C) 494/2012), a 9-judge panel of the Hon'ble Supreme Court of India decided that people have a fundamental right to privacy.The Supreme Court decided that everyone has the right to choose who sees what information about them online, how far it is spread, and other aspects of how their personal data is used for commercial reasons. The Supreme Court's decision is the first time that individuals have been given legal title to their personal identifier records.

Challenges of Fighting Cyber Crime[3]

New forms of cybercrime emerge with the development of IT. Cybercriminals are becoming more and more creative with their strategies to avoid being caught and foil investigations. The non-figurative and abstract nature of cybercrime makes it challenging to assess and prevent. We may categorize the issues at hand into two broad categories: general issues and legal issues.

The term "cybercrime" comes from the combination of "cyber," which represents the pinnacle of human intellect, and "crime," which represents its lowest point. This occurrence is giving people nightmares.Threats are only going to increase, and our weak laws won't do anything to stop them.

[3] http://assets.vmou.ac.in/PGDCL01.pdf page 39

CONCLUSION

Cybercrime can't be wiped off of the internet entirely, but it can be stopped. To yet, no law has been totally effective in eliminating crime, although several have been in reducing its incidence. Like physical crime, cybercrime cannot be eradicated by legislation alone, but it may be thwarted with the help of people, machines, and the law. If we want to avoid becoming victims of online crime, now is the moment to educate ourselves on the dangers posed by both deliberate and careless actions. Cybercrime has its roots in technology, and without it, it would be difficult to investigate and regulate. Law though currently not well equipped today in India; but can act as a strong deterrent to avoid suchcrimes[4].

REFERENCES

1. Cyber Space Jurisdiction: Issues and Challenges. Avialable at https://www.legalbites.in/cyber-spacejurisdiction-issues-challenges/

2. Cybercrime and cyber security strategies in the Eastern Partnership region. Avialable at https://rm.coe.int/eap-cybercrime-and-cybersecurity-strategies/168093b89c.

3. New Generation of angry & Youthful hackers join the hacktivism wave, adding to cyber-security woes. Available at https://economictimes.indiatimes.com/magazines/panache/new- generation-of-angryyouthful-hackers-join-the-hacktivism-wave-adding-to-cyber-security-woes/articleshow/81707844.cms.

4. Call for Special Courts to try Cyber Crimes, The Hindu, August 30, 2006, p5 (Writer is DR K. JAYANTH MURALI Additional Director General of Police and Director, DVAC, Chennai. The views expressed in this article are that of the author and not of the government) - Link - https://www.deccanchronicle.com/nation/crime/200718/indias-cybercrime-scenario-ground- situation-alarming.html)

5. Report on Cyber Security & Right to Privacy submitted by the Parliamentary Standing Committee on Information Technology Act presented on Feb 12th 2014, under the chairmanship of Rao Inderjit Singh to the fifteenth of the Lok Sabha.

6. The categories of the crimes have been adapted from the article found in https://www.lawctopus.com/academike/cybe

[4] http://www.lawctopus.com/academike/cyber-space-and-cyber-crime/

r-crimes-other-liabilities/

7. Cyber space available at: https://www.britannica.com/topic/cyberspace.

8. Barkha, Rama Mohan, U. (2011) Cyber Law and Crimes, IT Act 2000 & Computer Crime analysis. (3rd ed.), ISBN: 978-93-81113-23-3.

9. India: Key Features Of The Personal Data Protection Bill, 2019 available at https://www.mondaq.com/india/data-protection/904330/key-features-of-the-personal-data- protectionbill-2019.

10. Examining the importance of Stenography information technology essay. Available at https://www.ukessays.com/essays/information-technology/examining-the-importance-of-steganographyinformation-technology-essay.php.

11. Introduction to Cyber Crime, Available at: http://cybercrime.planetindia.net/cybercrime_cell.htm.

12. Legal Service India < http://legalservicesindia.com/article/article/offences-&-penalties- under-the-it-act2000-439-1.html>

13. Cyber Space Jurisprudence, Available at https://www.coursehero.com/file/p6qh84m/2-Cyberspace-hascomplete-disrespect-for-jurisdictional-boundaries-A-person-in/

Corresponding Author

Dr. Anil Kumar Jeph*

Supervisor, Professor, Govt. Law College, Raj Rishi Bhartrihari Matsya University, Alwar-301001, Rajasthan