INTERNATIONAL JOURNAL OF LAW

MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 7 | Issue 4

2024

Follow this and additional works at: https://www.ijlmh.com/

Under the aegis of VidhiAagaz – Inking Your Brain (https://www.vidhiaagaz.com/)

In case of **any suggestions or complaints**, kindly contact **Gyan@vidhiaagaz.com.**

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to **submission@ijlmh.com.**

An Epistemological Analysis of Cybercrimes Relating to Digital Property

S. VIDYA[1]

ABSTRACT

The online ecosystem has become an integral part of human lives, in which Cybercrime has become an intolerable threat to all the users of cyberspace. It emerges in numerous forms with the development in the discipline of information technology. Cybercrimes can be majorly categorized as crimes against person, property, Government and society. Cyber Citizens are being vulnerable to be victimized under any one of the above forms of Cybercrime. This article aims to give a clear understanding about the Cybercrimes relating to digital property.

Keywords*: Cybercrime, Digital property, Cybersquatting, Cybervandalism, Cyber Trespass, Cyber intellectual property crimes.*

I. INTRODUCTION

Today the online ecosystem has become an integral part of our lives with a lot of dependence on the digital space. The development in the discipline of information technology provides equal opportunity to all humans and they get a chance of access to any information, stored data, its analysis and so on, with the help of technological development. In the recent decades, the internet has tremendously changed in the field of education, entertainment mediums, social media platforms, sports sectors and wherever there is a need for frequent use of the internet. For any person having little knowledge about accessing the web browsers or mobile devices, the internet acts as the knowledge hub to them. The internet usage has its own pros and cons, but the worst part of it is cyber-crime. Thus, cybercrime has become an alarming threat to all the internet users and also to the general public. So it has become the need of the hour by every government to take stringent initiative to eliminate cyber crime of all kinds.

II. CYBERCRIMES

Cybercrime is a criminal activity that either targets or uses a computer, a computer network or a networked device. The computer may have been used in committing the crime or it may have been the target. Cybercrime may harm someone's security or finances.[2] The term cyber crime

---

[1] Author is an Assistant Professor at Government Law College Madurai, India.
[2] Cyber crime against property, https://www.slideshare.net/slideshow/cyber-crime-against-property/258816454

can be stated as any illegal activities, which are not permissible by any state of law, when carried out by any individual person or a team with the help of information technology enabled services and devices. Here the word cyber crime has not been restricted within the means of the word computer but it is used here to describe all forms of electronic means.

Computers are used as a tool to commit various cybercrimes like cyberdefamation, sexual harassment, child pornography, phishing, identity theft, assuming someone's identity, etc whereas computer itself has become the target in some form of cybercrimes like espionage ,hacking, software piracy, viruses, worms and so on.

(A) Various forms of Cybercrime

1. Cybercrime against person

2. Cybercrime against property

3. Cybercrime against government/ organizations

4. Cybercrime against society

III. DIGITAL PROPERTY

Digital property is the electronic information someone creates or owns. Digital property refers to digital information such as database, internet accounts, cloud storage, etc. it also covers the necessary files, codes or informations required in order to gain access to a specific digital file of value.[3]

If someone has money in a safe or vault, the key or the digital code of the vault is of the same value as the safe itself. Similarly the password to a cloud account where valuable items are stored is essentially a digital property.

(A) Cybercrimes against Digital property

Cyber crime against digital property are the criminal activities in which the computers, internet and technological devices are used in an illegal manner to deprive a person of their digital property . Cyber crimes against property have become a significant concern in India with the advanced digitalisation in various sectors. Everyone under cybercrime is vulnerable as it can lead to financial loss, identity theft, data theft and reputational damages.

After the development of modern networking and communication technologies, people began to rely more on soft copies than on manual records that are to be protected and safeguarded which has led to the replacement of hard copies into computer databases. Therefore the

---

[3] Casey Schmidt, The unique power of digital property, https://www.canto.com/blog/digital-property/

occurrence of cybercrime has also increased.

There occurs various forms of cyber crimes against property among which the following four forms of cybercrimes against property are considered to be the most common form of criminal activities against property in cyberspace

- Cyber squatting

- Cyber vandalism

- Cyber trespass

- Cyber intellectual property crimes

a. Cyber squatting

Cybersquatting means registering a domain name with the names of third parties' trademarks or trade names, with the intent of selling it for profit to any other person, company or an organization.

A domain name is a string of characters, consisting of letters, numbers, and dashes, that is part of a uniform resource locator URL which is used to access web pages. Each website has a unique domain name through which it is accessed. They begin with 'WWW' followed by the unique name or the name of the registered trademark and ending with domain name extensions like '.com', '.org' , '.edu', ' .net', '.ac', 'in', etc.[4]

Here the cybersquatters register the domain name with the names of third parties' trademark, trade names and other similarly spelled names with an intention of profiting from the reputation and prestige of such third parties either for confusing the consumers or for selling the domain name to the rightful owners for huge some of money. By this unethical and illegal act of cyber squatters, The trademark holders or the company or an organization are pushed to use their required domain name by buying it from the cybersquatters for a huge sum of money because two similar domain names cannot be registered and used at the same time.

b. Cyber vandalism

Cyber vandalism refers to the intentional or unauthorized act of causing damage or disruption to digital systems, websites or on online platforms. Sometimes it is even used to threaten individuals or institutions. In simple cyber vandalism is the deliberate act of destruction of digital property. Cyber vandals employ an array of means to correct internet sites, erase

---

[4] Nikhil Mishra and Damini sharma, Cybersquatting and Trademark Issues: An analysis with reference to India, https://articles.manupatra.com/article-details/Cybersquatting-and-Trademark-Issues-An-analysis-with-reference-to-India

documents, compromise user profiles and disseminate spam mail and malware.[5]

Cyber vandalism can be majorly categorized into three forms , such as disruptive cyber vandalism, destructive cybervandalism and defamatory cyber vandalism. Disruptive cybervandalism is designed to disrupt the normal functioning of a computer resource, destructive cybervandalism vandalism aims at damaging or destroying the computer and defamatory cyber vandalism involves posting false information or derogatory information about an individual or organization to damage their reputation.

c. Cyber Trespass

In general, a trespass is a legal wrong. In specific it can also be stated as a property wrong. Cyber Trespass is a cyber crime which involves accessing someone's computer without authorisation and permission. It is similar to the traditional form of trespass which involves entering someone's property without their consent and permission. Cyber Trespass occurs through unauthorized wireless internet connections. It involves hacking, website defacement but does not involve altering, misusing, disturbing, damaging data or systems.

d. Cyber Intellectual property crimes

A bunch of rights are available with the intellectual property online. Any illegal or unlawful activity against cyber intellectual property amounts to the offense of cyber intellectual property crimes. Various forms of violations occur in intellectual property rights but the most common forms of it are software piracy, infringement of copyright, trademark, patents, design and theft of computer source code etc.[6]

IV. CONCLUSION

Thus India is in an urge to enhance the capacities of users of cyberspace by sensitizing them about newly emerging cyber crimes relating to persons, property, Government and society and also there is a need to enhance the practical strategies that the users need to adopt in order to protect themselves from becoming the victims of cybercrimes. An energetic increase in digital awareness will ensure knowledge about the increasing threats of cyber crime and how to safeguard oneself against such crimes.

Before parting with, it is being concluded with a hope that this article have kindled the interest of the readers with knowledge and awareness about tremendously emerging cybercrime,

---

[5] Cyber Vandalism in Cyber Crime, https://www.geeksforgeeks.org/cyber-vandalism-in-cyber-crime/
[6] Nidhi Narnolia, Cyber Crime In India: An Overview, https://www.legalserviceindia.com/legal/article-4998-cyber-crime-in-india-an-overview.html

specifically relating to digital properties.

*****