A CRITICAL EXAMINATION OF CYBER CRIMES IN CENTRAL INDIA, WITH PARTICULAR REFERENCE TO SOCIAL MEDIA

Vijay*

INTRODUCTION

Men have always fought for advancement, seeking out new techniques and tools in an effort to improve their chances of surviving. arguably the most remarkable accomplishment, the computer is not only responsible for making human life more convenient and comfortable, but it also serves as an alternative for the human brain when it comes to the storing and retrieval of information. As a repository for information and knowledge, the computer has even surpassed the capabilities of the human intellect, at least from a purely functional standpoint. Thus, human innovation is an action that entails decades of knowledge to increase individual capacity or to meet evolving human desires. Consequently, there is no denying the fact that technology influences the natural environment with the help of the practical application of scientific understanding to human convenience. As a result, the advancement of science and technology has provided all comforts of life to the entire globe.

The use of the internet pervades almost every aspect of existence. The prevalence of the internet and its benefits increased along with the idea of cybercrime. The nature of cybercrime rarely stays the same for long. Opportunities emerge on a consistent basis as a result of advancements in both technology and society[1]. Hackers are always discovering new ways to exploit the newest browsers, e-commerce websites, or mobile computing devices. It is the same case with social media.

The power of social media lies in their capability to bring people together in novel settings and provide them with an expanded range of communication options. They make it easier for individuals, businesses, and governments to find new ways to promote a product, reach an audience, and create groups of people interested in that product[2]. Social networking websites are also of interest to online offenders. However, there is still a lack of information regarding the growing number of criminal dangers that are associated with social media. The purpose of

*MAHARISHI UNIVERSITY OF INFORMATION TECHNOLOGY, NOIDA.
[1] Heena Keshwani, "Cyber Stalking: A Critical Study", Bharti Law Journal, Page 3.
[2] Supra.

this research is to explain how the buying and selling of services, tools, and data on social media platforms, in addition to the sharing of malware, are making it easier for cybercriminals to carry out their illicit activities and contributing to the spread of traditional crime[3].

Any illegal activity that is carried out using a computer, a computer network or a gadget that is connected to a network is referred to as cybercrime. The act of computer cracking is predominantly carried out by individuals who identify as hackers or cybercriminals, with the primary motivation being financial gain. Nevertheless, it is important to note that there exist diverse rationales for engaging in cybercrime.

AN OVERVIEW OF CYBERCRIME

Any illegal behavior that takes place on the internet or makes use of the internet as a platform is referred to as cybercrime. These involve engaging in a wide variety of unlawful pursuits. The word "cybercrime" is an umbrella term that can be used to group together a variety of different types of illegal activities. Cybercrimes are done with technology, so the people who do them are usually very good with computers and the internet. Some regular crimes can also be cybercrimes if they are done on the internet or through it. The utilisation of social media platforms on portable devices such as smartphones and laptops is commonly referred to as mobile social media. The significance of mobile social media in mobile marketing lies in its ability to facilitate the production, sharing, and dissemination of user-generated content, which can aid companies in conducting marketing research, fostering communication, and cultivating relationships.

CYBER CRIMES USING SOCIAL MEDIA

Social media sites give people a new way to be seen and heard, so speakers and protesters can't be found at street protests and gatherings. For example, you can't say enough about how important social media was in the Gang Rape case in Delhi, India's capital, in December 2012. Millions of people were asked to join the movement against the people who did this on Facebook. It gave a lot of people in India a chance to talk about how angry they were about the horrible crime.

Using social media sites to communicate in a way that is annoying, dangerous, or aggressive. It has changed from making sexually explicit phone calls to sending repeated messages to

[3] Supra Note 1 at 5.

someone who does not want to receive them[4]. This is called "cyberstalking." Cybercriminals look for personal information about users on social media sites. When people share personal information on websites, like their name, delivery information, address, process details, e-mail addresses, and phone numbers, cybercriminals can use that information to get into their accounts and steal their information.

Most of the time, fake profiles are made on the following websites or apps:

1) Facebook, and
2) Instagram
3) Twitter
4) WhatsApp
5) Snapchat

There is a risk that the user or their friends could be subjected to physical or verbal violence if personal information is made public. The more information that is shared, the greater the likelihood that another person will be able to impersonate the user and also persuade one of their friends into sharing their confidential information, such as downloading malicious software or gaining access to websites that are normally off-limits[5].

1. Fraud

Even though it might be appropriate among friends to use a friend's social media account in order to publish a humiliating status update, it is a serious crime. Also, based on what the person behind the fake or impersonation account does, making fake accounts to trick people may also be considered fraud.

2. Cyber Stalking, Online Threats

Most crimes that are recorded and seen to happen on social media involve people making bullying, harassing, and threats, or following other people. Even though many of these crimes aren't punished or taken seriously, the people who are victims of them often have no knowledge

[4] P.D Singh & D. Loura, "Cyber Security in Civil Aviation: Current Trends", Dehradun Law Review, 13(1), Page 20.
[5] I.T Vakul Sharma, "Information Technology Law and Practice", Universal Law Publications, Page 12.

of when to call the police. If someone says something about you online that makes you feel threatened or if you think the threat is real, you should probably think about calling the police[6].

3. Illegal Transactions

It is possible that using social media platforms to establish business connections or to purchase legitimate goods or services is a perfectly acceptable practice. However, establishing a connection through social media with the intent of purchasing illegal substances or other products subject to regulation, control, or prohibition is definitely against the law[7].

CYBERCRIME LAWS IN INDIA

There are a significant number of laws and regulations that have been implemented by a variety of authorities to punish criminal activity committed online. It should come as no surprise that many of the provisions of the Indian Penal Code, 1860 (IPC), and the Information Technology Act, 2000 (IT Act), which both have provisions criminalising various forms of online misconduct, intersect one another.

Important Provisions are as follows:

1) *Section 67A* of the IT Act says that the person can spend up to five years in jail and pay a fine[8].
2) *Section 66E* of the IT Act makes it illegal to send pictures of a person's private area, and even taking such a picture without the person's permission is against the law[9].
3) *Section 43* Penalty and compensation for damage to the computer, computer system, etc. - If another individual causes damage to it or uses it in a way that is harmful to the other individual without the authorization of the owner or any other person, the other individual is obligated to pay a particular sum of compensation[10].
4) *Section 69A* goes into detail about who has the power to order that the public can't access any information through any computer tools. A person who breaks this law could get up to 7 years in prison and a fine[11].

[6] Abhiraj Thakur, Cyberstalking: A Crime or A Tort, Page 14.
[7] Ibid.
[8] The Information Technology Act, 2000 (Act 21 of 2000), s. 67A.
[9] The Information Technology Act, 2000 (Act 21 of 2000), s. 66E.
[10] The Information Technology Act, 2000 (Act 21 of 2000), s. 43.
[11] The Information Technology Act, 2000 (Act 21 of 2000), s. 69A.

5) *Section 71:* It applies to anyone who knowingly gives false information or hides Requisite information from a regulatory body or an entity responsible for authentication, for the purpose of obtaining a license or a digital signature certificate. The individual in question may face a maximum penalty of two years of imprisonment or a fine of 1 lakh rupees, or both, depending on the length of the sentence and the amount of the fine[12].
6) *Section 292* of the IPC states that it is against the law to spread any kind of sexually explicit information[13].
7) *Section 419 and Section 420:* Since both of these sections deal with theft, their rules are grouped together. These two parts of the IPC have a lot to say about crimes like stealing a password to get money by being dishonest, making fake websites, and committing online scams[14]. In contrast, email phishing is associated solely with Section 419 of the IPC due to its deceptive nature of impersonating another individual and soliciting their password. According to Section 419, a penalty of a maximum of three years of imprisonment or a monetary fine may be imposed. Section 420 of the law stipulates a punitive measure that entails a maximum prison sentence of seven years or a fine[15].
8) *Section 354C* of the IPC says that it is necessary to obtain authorization from the subject, to get a picture like this. However, authorized permission is not needed to share the picture. But one thing you should know is that this rule doesn't apply to morphed or photo-shopped pictures, even though they might have the same effect[16].
9) *Section 504:* Section 504 of the IPC says that it is against the law to use email or any other method of digital or electronic communication to threaten, insult, or try to start a fight with someone in order to bring peace. If you break this law, you could get up to two years in jail, a fine, or both[17].
10) *Section 506:* The present section delineates that in the event of an individual attempting to issue a criminal threat towards another individual with respect to the endangerment of their life, destruction of property by means of fire, or violation of a woman's chastity, the individual in question will be prosecuted under Section 506 of the Indian Penal

[12] The Information Technology Act, 2000 (Act 21 of 2000), s. 71.
[13] Indian Penal Code, (1860), s. 292.
[14] Indian Penal Code, (1860), s. 419.
[15] Indian Penal Code, (1860), s. 420.
[16] Indian Penal Code, (1860), s. 354C.
[17] Indian Penal Code, (1860), s. 504.

Code. The aforementioned section entails a maximum imprisonment term of seven years and a monetary penalty, or both[18].

The judgements that follow are considered to be important judgements on the subject of cybercrime in India. When the first polymorphic malware was made public in 1992, this marked the beginning of the first instance of cybercrime. One of the very first instances of cybercrime in India was the case of ***Yahoo v. Akash Arora***[19], which took place in that country. The plaintiff in this case, Akash Arora, was accused of making unauthorised use of the trademark or domain name "yahooindia.com," and the defendant requested a permanent injunction against Akash Arora.

The remark in question was made in a Yahoo discussion group, and it was obscene, defamatory, and harassing to a woman who had recently divorced. The accused also used a bogus email account in the victim's identity to send emails to the victim requesting information. The accused forwarded these texts to the victim. Because the message became public, the woman has been given a barrage of harassing phone calls from people who mistook her actions for those of a salesperson. The defendant was taken to Chennai's Central Prison after making the necessary payment. Section 67[20] has been effectively applied to a case in India for the first time.

In the ***Shreya Singhal v. Union of India***[21] case, Mr. Tushar Mehta, the learned Additional Solicitor General for the defendant, argued that anything posted on the internet or made available to netizens is more accessible to everyone than any other media because it is not limited to a certain area. In the well-known case Shreya Singhal v. Union of India, this point of view was brought up. Because of this, it shouldn't be a surprise that this calls for more rules. With the current legal structures, it's getting harder and harder to stop the rising rate of crime[22].

CONFLICT BETWEEN IT ACT AND IPC REGARDING CYBERCRIME

At the moment, a number of crimes are punished by both the IPC and the IT Act, even though the same things are involved in both crimes. There are small changes between the punishments in these laws, such as whether the crime can be bailed out, fixed, or brought to court. Obscenity

[18] Indian Penal Code, (1860), s. 506.
[19] 78 (1999) DLT 285.
[20] The Information Technology Act, 2000 (Act 21 of 2000), s. 67.
[21] (2013) 12 SCC 73.
[22] Available at <<https://www.scconline.com/blog/post/tag/shreya-singhal-case/>>, accessed on 23rd March 2023.

is a crime that can happen through different kinds of media, both online and off. But it could be unfair if two different laws are used to punish the same crime based on the type of media used.

In ***Gagan Harsh Sharma v. The State of Maharashtra***[23] case, some individuals have been alleged to have appropriated both data and software from their respective places of employment. The individuals in question have been charged with theft under sections 408 and 420 of the Indian Penal Code, as well as violations of sections 43, 65, and 66 of the IT, Act. Except for section 408, all of these parts of the IPC have already been talked about in other parts. Section 408 of the IPC talks about a clerk or helper who breaks the law by betraying a trust. This part of the law says, "Whoever, being a clerk or servant or working as a clerk or servant, and being given property or control over the property in any way, commits criminal breach of trust with respect to that property, shall be punished with imprisonment of either kind for a term that may last up to seven years, and shall also be fined." If the judge does not give authorization, it is impossible to combine the offences described in sections 408 and 420 of the Indian Penal Code because neither of these offences is bailable. Offenses that are eligible for parole and compounding are created by the Information Technology Act sections 43[24], 65[25], and 66[26]. As a direct consequence of this, the petitioners requested that the charges brought against them under the IPC be withdrawn and that the charges brought under the IT Act be investigated and brought to justice[27]. It was also stated that in the event that the judgement made by the SC in ***Sharat Babu Digumarti***[28] was implemented, the petitioners could only be charged for their actions under the Information Technology Act and not the Indian Penal Code. Therefore, the respondents' arguments were accepted by the Bombay High Court, which then issued an order to have the IPC charges brought against them dropped.

According to the Supreme Court's ruling in the ***Sharat Babu Digumarti***[29] case, no one can be charged with a crime under the Indian Penal Code for actions or omissions that could also be

[23] (2017) 2 SCC 18.
[24] The Information Technology Act, 2000 (Act 21 of 2000), s. 43.
[25] The Information Technology Act, 2000 (Act 21 of 2000), s. 65.
[26] The Information Technology Act, 2000 (Act 21 of 2000), s. 66.
[27] Available at << https://www.scconline.com/blog/post/2022/11/21/tenability-of-successive-complaints-based-on-similar-facts-for-dishonour-of-cheque-under-the-negotiable-instruments-act-1881-and-cheating-under-section-420-ipc/>>, accessed on 22nd March 2023.
[28] SCC OnLine SC 1464.

[29] Ibid.

punished under the IT Act. This is what the court's ruling comes down to[30]. Even though we agree with the Supreme Court's ruling on every point, we still believe that the Information Technology Act shouldn't be the place where all cybercrimes are kept. Just because a crime was done online doesn't mean that the different types of that crime should be handled differently in the justice system. The Sharat Babu Digumarti case ruling by the Supreme Court of India stipulates that the Indian Penal Code cannot be invoked to charge an individual for an offence that arises from specific acts or omissions if the Indian Information Technology Act can be applied to the same acts or omissions. However, it is noteworthy that crimes such as theft and obscenity will be subject to distinct punitive measures if they involve any form of cyber activity. At the moment, someone who gives away an obscene book in hard copy will be punished according to the Indian Penal Code (IPC), while someone who gives away obscene materials over the internet will be punished according to the Information Technology Act (IT Act), even though the basic crime hasn't changed. If someone takes a car, they will be punished according to the IPC, and if they steal information online, they will be punished according to the IT Act. No matter if the stolen property was digital or physical, it is still called theft. The same rules should apply to profanity that is sent in person or online. The same rules should apply to obscenity that is sent over the Internet.

CONCLUSION

The legal framework for cyberspace is regulated by the Information Technology Act and its corresponding regulations. One may also refer to the IPC when the IT Act is unable to cover a specific category of offence or when it does not contain all applicable provisions. The vast array of cybercrimes, however, cannot be adequately addressed by the present cyber law system. This research paper tries to put some light on how crime has changed on social media sites. It talks about how the growth and development of social media have changed the manner in which individuals communicate with one another and engage in social interaction, but it has also made its users more vulnerable. Without a doubt, the impact and influence of social media websites on personal and professional life are diminishing. Before falling victim to these snares, it is prudent to be aware of the drawbacks and flaws of every benefit. One such issue is cybercrime security, which is inextricably linked to the use and impact of social media networks.

REFERENCES

1) Articles

1.1) Keshwani Heena, "Cyber Stalking: A Critical Study", Bharti Law Journal.

1.2) Singh P.D & Loura D, "Cyber Security in Civil Aviation: Current Trends", Dehradun Law Review.

1.3) Sharma Vakul I.T, "Information Technology Law and Practice", Universal Law Publications.

1.4) Thakur Abhiraj, Cyberstalking: A Crime or A Tort.

2) Statutes and Legislation

2.1) Indian Penal Code, 1860.

2.2) The Information Technology Act, 2000.

3) Web sources

3.1) <https://www.scconline.com/blog/post/2022/11/21/tenability-of-successive-complaints-based-on-similar-facts-for-dishonour-of-cheque-under-the-negotiable-instruments-act-1881-and-cheating-under-section-420-ipc>

3.2) https://www.scconline.com/blog/post/tag/shreya-singhal-case/