Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2023 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rishikesh Dave; Publisher – Ayush Pandey

Criminal use of Social Media Platforms

Arsheya Chaudhry[a]

[a]Vivekananda Institute of Professional Studies, New Delhi, India

Received 30 January 2023; *Accepted* 18 February 2023; *Published* 24 February 2023

Cybercrime has breached social media networks, thanks to both the increased number of users and the increased usage. No statute specifically defines cybercrime. Cyber refers to anything having to do with computers, the internet, and virtual reality. The social media sites that we all adore and spend countless hours on serve as a gateway for cybercriminals to take advantage of us. In order to boost their chances of connecting with their victims, cybercriminals have set up numerous social media accounts and joined numerous social media platforms as a result of the extensive usage of social networking websites in the digital age. Social media is a platform that paves the way for various cyber-crimes such as stalking, identity theft, or fraud, and the most committed crime of the century is Trolling. The meaning of trolling is very much similar to defamation, but there is a thin line of difference between the two. In this article, the author discusses such cyber-crimes which are abundantly committed on social media.

Keywords: *social media, cybercrime, stalking, trolling, morphing, identity theft.*

INTRODUCTION

Facebook, Instagram, WhatsApp, and LinkedIn are examples of social media platforms that have been successful in the twenty-first century. Social Media is a phenomenal platform to form relationships, connect with people, share ideas, and expand businesses. Apart from these wonderful benefits, it is also a haven for cybercriminals who are hunting for gullible and ignorant victims. The nature of social networking sites is such that it means sharing of data

which is the inherent part of these applications. The social media engine also depends heavily on trust. A flawless cyber-storm is produced by the combination of these two factors.

Any digital technology that enables users to instantly generate material and share it with the world is referred to as social media. It is easily accessible with a computer, smartphone, iPad, or another internet-connected device. The most well-known social media platforms included Facebook, WhatsApp, Twitter, Instagram, and LinkedIn. No statute specifically defines cybercrime. Cyber refers to anything having to do with computers, the internet, and virtual reality. In simple terms, Cybercrime refers to any criminal activity which is done by the perpetrator through the usage of a computer or the internet. The most prevalent types of cyber crimes are cyberbullying, cyber-stalking, identity theft, etc.

To boost their chances of connecting with their victims, cybercriminals have set up numerous social media accounts and joined numerous social media platforms as a result of the extensive usage of social networking websites in the digital age. In the year 2020, India registered 50,035 occurrences of cybercrime, an increase of 11.8 percent over the previous year, with 578 incidents of "false news on social media" being documented[1]. As per the National Crime Records Bureau data, the rate of cybercrime also increased to 3.3 percent[2].

SOCIAL MEDIA TROLLING

The meaning of trolling is very much similar to defamation, but it is not the same as defamation. Defamation is the act of damaging a person's reputation through words spoken or written. Trolling on social media, on the other hand, is the circulation of pictures, videos, or messages on famous and most-surfed social media platforms such as WhatsApp, Facebook, Instagram, Snapchat, etc. which offends any individual, any group, or any organization. The objective of social media trolling is to make the victim feel uncomfortable or put them under severe

[1] Siddhartha Kaikinia et al., 'Statics on Cyber Crimes and Cyber Laws in India: A Study' (2022) 13 Journal of Algebraic Statistics https://publishoa.com/index.php/journal/article/view/533/462 (Last visited on 22 January 2023).

[2] 'India reported 11.8% rise in cyber crime in 2020; 578 incidents of 'fake news on social media' (*The Hindu*, 15 September 2021) <https://www.thehindu.com/news/national/india-reported-118-rise-in-cyber-crime-in-2020-578-incidents-of-fake-news-on-social-media-data/article36480525.ece> accessed 22 January 2023

depression. This is known as social media trolling. Trolling also includes writing some texts which are controversial and insulting to start an unwanted debate and the result of such a debate is always disputes between religions, genders, etc. In addition, these disputes cross all limits and become a spot for crimes.

To summarize, it can be said that trolling is a direct character assassination of an individual, any group, or any organization because it harms the reputation of that person or group. They feel insulted and get so much destroyed inside that they feel embarrassed to even stand in that group or a public place. In India, there are no specific laws prohibiting online trolling. Trolling is not defined under the Indian Penal Code of 1860. However, cyber bullies and trolls can be combated by combining several articles of the Code with the Information Technology Act of 2000 ("IT Act").

SOCIAL MEDIA MORPHING

Morphing is the process of altering or changing images of people using online morphing tools. Morphing was previously reserved for the film and animation industries, but it is now widely available to the general public. Criminals take advantage of this and use it to harass people online. Such criminals take out pictures of victims from online platforms, alter them and post them or threaten to circulate them. They many times, even blackmail the victims. Young girls and women are frequently targets of cyber criminals who use their photographs posted online and misappropriate them by changing the images[3].

CYBERSTALKING

Stalking in layman's terms means a pattern of unwanted behaviour which involves monitoring, harassing, repeatedly contacting, or following another person. Cyberstalking, on the other hand, is a crime that involves the internet or any other electronic media. The stalkers use the internet and various other media to follow people. Cyberstalking is generally understood as the usage

[3] Aashank Dwivedi, 'Crime against women through social media' (*Times of India*, 18 December 2022) <https://timesofindia.indiatimes.com/readersblog/aashank-dwivedi/crime-against-women-through-social-media-48132/> accessed 22 January 2023

of the internet or computers to stalk or harass an individual. In this, the stalker does not physically follow the victim but keeps a tap on the victim using the internet and other forms of social media. Cyberstalking is not easily predictable since there is no physical confrontation. The stalker hides behind the internet which makes it very difficult for the police to track down the offender. Some examples of Cyberstalking are –

- Posting rude, offensive, or suggestive comments online.
- Following the target online by joining the same groups and forums.
- Sending threatening, controlling, or lewd messages or emails to the target.
- Using technology or social networking sites to threaten or blackmail the target.

There are various reasons behind stalking such as hatred, jealousy, envy, obsession, internet deviation, or power and control. Cyberstalking is proven to be a grave offence. It has a very far-reaching impact on the mental and physical health of the victim.

IDENTITY THEFT

Identity theft or identity fraud are terms used to describe the act of stealing someone's identity. From the name itself, we can make out that it means a person's identity is being stolen. This term is made from two words which are identity and theft. Here, identity means who or what a person is and theft refers to stealing. It is about stealing the identity of some person. Identity theft is a common crime these days, but it is a serious one because it involves someone stealing an individual's identity and then misusing it. The true name and account takeover are two of the most common types. True name identity theft means that the thief can use the name or identity of another person and can obtain a SIM card or open a bank account or get a debit card in his/her name. In case of account takeover, the offender will steal things such as debit cards, credit cards, etc that have already been issued. In both cases, it does not cost him anything since the identity is of that another person, and in case the perpetrator commits any subsequent crime, that person whose identity was originally used will be the accused one.

Cases of Identity theft are increasing continuously on social media. People create phoney accounts in the name of someone else. This is frequently done to avenge someone, extract

retribution, or make fun of the other person. Because they have all information about the person whose account they are making, such as date of birth, place of residence, religion, and so on, the person who creates such accounts is highly familiar with the person whose account they are creating which is accurate, so that it looks as real as it can be. This is an absolute invasion of the privacy of the person involved.

OBSCENITY ON SOCIAL MEDIA

Obscenity is becoming increasingly prevalent in our country. This is posing a threat, and it is past time for us to take appropriate action. Obscenity on social media is defined as any image, photograph, figure, article, write-up, video, or other content that depraves or corrupts people's minds. This violates acceptable social and moral standards. There has been a lot of debate regarding obscenity on social media with the recent case of Ranveer Singh's obscene pictures being posted on social media. It has sparked a heated debate in India about what constitutes 'obscene' and what is an obscenity[4].

CYBERBULLYING

Cyberbullying, also known as online bullying, is the deliberate and repetitive use of technology by an individual or a group of individuals to upset someone else. Cyberbullying, like other forms of bullying, has an impact on self-esteem and self-confidence, as well as mental health and well-being, and can lead to self-harm and death in extreme circumstances. To support the health and wellness of all members of the school or community, it is critical to address all types of bullying and prejudice. Additionally, people have experienced cyberbullying from groups or individuals they have never met. A wide range of unpleasant or unlawful behaviours can be carried out through technology such as –

- Intimidation and threats;
- Harassment and stalking;

[4] Singh, A. (2022, July 27), " *Amid row over Ranveer Singh's 'nude' photoshoot, what are the laws that deal with obscenity?*, https://news.abplive.com/explainers/amid-row-over-ranveer-singh-s-nude-photoshoot-what-are-the-laws-that-deal-with-obscenity-in-india-1544773 (Last visited January 28, 2023).

- Defamation
- Peer rejection;
- Impersonation;
- Manipulation;
- The unauthorised release of personal information or photographs.

Cyberbullying occurs in a variety of locations and mediums in cyberspace, and it is no surprise that it is the most common in places where teenagers congregate. Initially, many kids congregated in chat rooms, and as a result, the majority of abuse occurred there. Cyberbullying has several negative consequences that extend into the real world. For example, many targets claim to be unhappy, sad, furious, or disappointed. Additionally, studies have discovered a correlation among both cyberbullying and low self-esteem, family problems, academic difficulties, violence in schools, and a variety of antisocial behaviour. And at last, cyberbullied youngsters have demonstrated suicidal thoughts.

The first thing we wonder is why cyberbullying is such a big problem. The answer to this is that an increasing number of children are utilizing and embracing internet interactivity. They do so for a variety of reasons, including schoolwork, keeping in touch with friends, playing games, learning about celebrities, sharing their digital creations, and many others. Because online communication tools have become such an integral part of their life, it is unsurprising that some young people have chosen to utilize technology to be spiteful or frightening to others. Teens are vulnerable to victimization because they are always linked to technology.

Understanding and talking about cyberbullying; incorporating cyberbullying prevention into relevant policies and practices; ensuring reporting routes are accessible and visible; promoting positive use of technology; and evaluating the impact of prevention activities are all key elements of an effective approach. To facilitate ongoing dialogue and guarantee that members of the community are not unintentionally encouraging cyberbullying due to a lack of understanding, it is critical to raise awareness and promote understanding regarding cyberbullying. Both the victim of bullying and witnesses may find it challenging to report the behaviour. Reporting cyberbullying may be especially challenging for young people if doing so

may reveal information about their online habits that they do not want to share. Technology use encompasses both feelings and actions; it is, above all, a social activity that allows young people to feel connected to their peers. Telling a young person who has been cyberbullied to turn off their phone, delete an account, or stay off the internet as a response to the cyberbullying might also be viewed as a disruption of their social life and as punishment. Realizing that this is likely to be a response, may deter some people from reporting.

LAWS DEALING WITH CRIMES COMMITTED ON SOCIAL MEDIA

Under The Information Technology Act, 2000 - Section 66 A states that any person who sends grossly offensive messages or texts through computers or the internet or any communication device is punishable under this section. Any information which is false or sent with the purpose of annoying, insulting, or injuring the other person is also punishable under this section. The punishment prescribed is imprisonment for a term of three years with a fine[5]. As per Section 66C, identity theft is punishable with imprisonment of either a term that may extend to three years and also a fine that may extend to one lakh[6].

Section 66 E applies to the violation of bodily privacy which is capturing and transmission of pictures of any person without their consent[7]. Such an act violates the Right to Privacy guaranteed under Article 21 (Right to Life) of the Constitution[8]. Section 67 states the punishment for publishing or transmitting obscene material in electronic form. This section includes all forms of obscene publications. The punishment prescribed under this section is up to five years of imprisonment and a one lakh fine for the first conviction and up to ten years of imprisonment and a two lakh fine for a subsequent conviction[9].

Section 67A[10] deals with the publishing of sexually explicit/pornographic material. It criminalizes the publication and transmission of sexually explicit/pornographic material in

[5] Information Technology Ac, 2000, s 66A
[6] Information Technology Act 2000, s 66C
[7] *Ibid*
[8] Constitution of India 1950, art 21
[9] Information Technology Act 2000, s 67
[10] Information Technology Act 2000, s 67A

electronic form. However, the loophole here is that it's viewing, downloading, possession, etc is not an offence. The term 'sexually explicit' connotes something which is something more than obscene, thus, a more severe punishment[11].

Under The India Penal Code - Section 292 of the IPC also bans the sale, distribution, renting, exhibition, or circulation of obscene material[12]. Criminal intimidation means that anyone who threatens a woman with the intent to harm her and conceals his/her identity by taking precautions can face up to two years in prison under Section 507 of the IPC[13]. This is extremely useful and effective when dealing with online trolls or rape threats because a complaint can be filed against the harasser without knowing his or her identity.

Defamation is typically used in slightly elevated cases. However, anyone who purposefully uses words, signs, or visible depictions, or publishes anything with the intent of harming your reputation can be charged with defamation under Section 499 IPC[14]. This offence includes comments on social media, as well as obscene images or videos posted for easy display. Online stalking is also punishable under Section 354D of the IPC. The Perpetrator can face up to three years in prison and a fine. If such an incident occurs again, the repeat offender will face five years in prison and a fine[15].

PREVENTIVE MEASURES

As everyone, whether a child or an adult, is on social media nowadays, it is critical to take certain precautions. Some precautionary measures that everyone can take to keep themselves safe, secure, and out of the crosshairs of crimes committed on social media are as follows –

- Profiles can be made invisible to public searches.
- Limit the number of people who can find you via an internet search.
- Limit what people can learn about you by conducting a web search.

[11] Information Technology Act 2000, s 67A
[12] Indian Penal Code 1860, s 292
[13] Indian Penal Code 1860, s 507
[14] Indian Penal Code 1860, s 499
[15] Indian Penal Code 1860, s 354D

- Log out at the end of each session.
- Don't share your social media login credentials.
- Accepting friend invitations from people you don't know is never a good idea.
- Do not click on any links that appear suspicious.
- Keep your privacy settings on social media profiles as low as possible, especially for the public/others.
- Remember that information scattered across multiple posts, photos, status updates, and comments may reveal enough about you for a scammer to steal your identity and defraud you. As a result, when sharing anything on the internet, proceed with extreme caution.

CONCLUSION

When we post something on social media, we must always be cautious; it makes no difference whether the user is a girl or a boy, whether he or she has a fair or dark complexion; rather, the user should be aware of the people on social media with whom he is connected or added. The government and its agencies are doing their part; additionally, the Information Technology Act of 2000 was passed to combat crimes such as cyber stalking, cyber trolling, phishing, and hacking. Furthermore, we should keep track of what we post on social media and whom we share it with.

We should also keep our accounts secure by regularly changing passwords, updating the security policies established by individual agencies, not adding unfamiliar people to our list of knowns, and not disclosing personal information such as OTP, passwords, and so on. The most important thing to remember is that if you ever feel stalked or fall into one of these traps, you must immediately report all genuine information to the nearest police station or the city's cybercrimes department.