Social Media Platforms and Cyber Crimes: An Entangled Relationship

Priyanka Mittal [1]
[1] Research Scholar
Email: [1] priyankaagarwal088@gmail.com

Abstract

Today, the internet[1] has ingrained itself into our daily lives to the point where it is difficult to imagine existence without it. Because of the development of technology, digital media has emerged as an important part of person lives, the rapid use of mobile information, and social media, that offer venues for simple connection with people all over the world. While technology provides numerous benefits, it also provides risks to humans. Digital media has turned into a refuge for criminals since it has increased the number of offences committed online. There is no longer anyone who is not amazed by the benefits of the internet, and the important digital media platform is accessible to everyone. The main factors contributing to social media's appeal are its privacy and the development of a real environment where people may interact, swap pictures, meet people, enjoy games, become infatuated, have arguments etc, before ever having met in person. However, it is now common place for thieves to improperly use a victim's name, address, location, and other personal information, especially in cases involving women. Cyber crime has increased among person of all age group and is now a worldwide issue due to the confidentiality and fakeness present in social media as well as jurisdictional concerns.

The impact of digital media on young people and the causes of the rise in cybercrime on social media are described and discussed in the paper. The study also examine the role of the law in resolving and preventing cybercrime via social media and covers the typical types of cybercrime that occur there. The study also suggests several measures for adequately and comprehensively educating the nation's youth concerning the effects of cybercriminals.

Keywords: Electronic media, Electronic crime, Policies, confidentiality, compassion, protection

1. Introduction

Digital media has fundamentally altered how data is used and communicated among people, and it has also become a necessary component of every organisation, whether it be a government agency or any other private entity. It gives users a platform to easily share information and thoughts with a significant section of the population while avoiding the use of conventional media venues. Social media has been playing a significant influence in influencing people's thoughts and beliefs. Social networking site data is a useful source of information for analysing the flow of ideas, viewpoints, and opinions, among other things. Knowing how often data is shared, who is sharing it, and what the information is about is extremely valuable. This can be helpful in a variety of ways, such as disseminating information about any crisis to billions of people. A current example is the dissemination of

information about the lockdown procedures during the pandemic. However, social media is typically not used to share news or any other public issues; rather, it has evolved into a significant political media outlet.

Digital media, when used properly, can inform the audience about any event occurring around the world and spread awareness of it. In terms of the number of users, social media is the software's success story of the last ten years. Facebook's growth from 2.45 billion monthly users in 2020 [2] to 2.75 billion monthly active users by July 2021, a rise of 14 percent over a year, gives an idea of the increasing popularity of social media. Because of their popularity, these websites attract cybercriminals like nectar to a bee. One of the best and most strongest tools, digital media, has recently turned into a heaven for criminal activity. Cybercrimes have surged over the past ten years because of the rise in internet users. Cybercrimes are wrongdoings carried out on a computer. Alternately, any unlawful activity involving a network of computers or other electronic devices is referred to as a "cyberattack." Our personal information is easily accessible to cybercriminals on social networking sites, e-commerce websites, and other internet services.[3] They can also attack our social media identities using sophisticated techniques like malware. Another strategy is to create a bogus online persona with the intention of defaming someone or stealing their credit card number and other information that may be easily obtained from online shopping sites. Teenage attacks and gender-related assaults are two of the more severe kinds. Child pornographic content is on the rise in cyberspace, with moms and kids of all ages as its main targets, due to the confidentiality of the culprit. Children are also deceived by such cybercriminals, who use fictitious web-based interactions and identities.

Considering that there have recently been disclosures about schoolchildren plotting to rape a young girl on social media[4], it continues after this. A recent example of the "Bois locker room" was the Instagram issue. Alok Mittal, the head of the NIA (National Investigation Agency), claims that every sixth cybercrime in India "is reported on digital media.In our nation, there were approximately 250 cases of cybercrimes involving digital media in 2019 and 400 cases in 2020.[5] In addition, there have been examples of social media rose by 53% in 2021.[6]

2. Overview of Electronic Media

Through the use of the web, phone and online discussions, chat rooms, and a variety of other elements, electronic media provides a stairway that connects people to the rest of the world. Because the process is so straightforward, kids may quickly and simply sign up to become members of any social networking platform. Any social media network that a person want to use requires them to register with their personal information. Once registered in, individuals can view the platform's content and communicate with other members of the network by sharing photographs, facts, or information. Young people frequently use Facebook, Twitter, Instagram, WhatsApp, Snapchat, and other popular social media platforms.

However, because face-to-face interaction has dramatically diminished in global epidemics, electronic media also influences society's isolation. Anxiety, FOMO, depression, and a number of other issues follow, which have an effect on people's mental, emotional, and psychological health. People worry about their privacy more and more these days. The third party uses the people's personal information to engage in cyberbullying and cybertheft against teenagers. Due to the availability of offensive content on social media, youth are more

vulnerable to these things. They spend their days in online chat rooms as a waste of time. Furthermore, false information spreads more fast than true information and can be done thus for any reason, including to incite hatred among various racial and religious groups or to deceive people, creating virtual hate crimes worse.

The fact that digital media has smoothly merged into our way of life is the essential reality. Because of this, the field of digital universe is considered to be relatively young in terms of the problems it raises with human rights and obligations.

Although electronic communication is frequently used to remain in contact it can also lead to social isolation. Direct interaction has been significantly diminished by the use of digital channels. A number of investigations and pieces of inquiry have demonstrated that adolescents who suffer isolation from society may suffer from a variety of adverse effects on their fret, despondency, and terror of being left out, as well as their intellectual, moral, physical, and mental components. Adolescents also commonly steal online and indulge in cyberbullying on social media. There is a very high possibility that a third party may exploit a person's private information on social media because of its lack of protection.[7] Youth wasting time on these platforms by engaging in online conversation rather than doing anything productive is another facet of this. Hackers also target on adolescents who are young in addition to children. Social media exposes users of all ages to criminals who utilize the information provided on these platforms inappropriately. Sexually explicit material is spreading among particular demographics more frequently on these social networking sites. On social networking sites, teenagers have occasionally talked of raping a child. Digital media, on the other hand, disseminates information but also makes it easier for misleading figures to spread. WhatsApp is the primary tool for disseminating false information, and the fact that some people still think it is worrisome. Such rumors may be spread in an effort to stir up enmity and violence among various groups. Because they are the most adaptable and open group, children may be the ones who are most impacted by internet media. Due to the growth of such online media, the idea of interaction and communication has evolved. Computer crimes have risen recently during COVID, [8] according to studies.

The reality is that electronic media has ingrained itself into our culture and has taken over the majority of lives of individuals. Despite being a great venue for individuals information, electronic media often includes rumors and inaccurate data. Since we can access everything over the network on a portable device, face-to-face contacts and actual encounters are becoming increasingly rare in our life.

3. Types of Cyber Crimes

According to the National Cyber Crime Reporting Portal [9], 5 cybercrimes are highlighted –

Email scam and Phishing: Phishing is a type of e-commerce scam that happens when a false email requesting sensitive personal and financial information appears to be from a certain firm.

As a result, it deceives the user into exposing their personal information so they can later exploit it.[10] In May 2020, a fake email campaign that promised to release a user's confidential video footage unless a bitcoin ransom was paid was reported to the country's federal counterterrorism authority.[11]

Identity Theft – Social networking have made this a much similar occurrence. In this kind of crime, the perpetrator uses social media platforms to get the victim's personal information.[12]

This is done so that the victim's information can be used to apply for credit, loans, or other forms of financial aid. It also involves obtaining sensitive statistics to get acquire to bank balances or maybe using it to defraud people or a violation under the victim's identity. According to research by the finacial Times, 4 out of 10 Indians have been victims of identity theft.[13] According to National Crime Records Bureau data, there were a total of 1545 and 1597 cases of identity theft (section 66 C of the Information and Technology Act) and defrauding by personation (section 66 D of the IT Act) in 2016. The increase was evident in 2017, when 3724 and 2296 cases, respectively, were reported under Sections 66C and 66D.

Obscene content – Sharing or sending pornographic material is illegal and punishable under Section 67 of the Information Technology Act. Obscene is defined as "offensive to modesty or decency; vulgar, dirty, and unpleasant" by the Supreme Court in one of the key cases.[14]The Supreme Court also made a distinction between obscenity and pornography. Additionally, criminals alter social media images, produce pornographic content, and distribute it online with disregard for the victim. According to the Hindustan Times, a man who was producing, distributing, and posting photographs was detained of Hindu deities figures on digital media.[15]

Online scam or fraud – Online fraud and scams have gained attention in the era of the internet where everything is accessible. Another fraudulent online behaviour is the cloning of a person's account in order to obtain personal information. The perpetrators create a new account using photos and pictures, then entice friendship and family too divulge bank account information or any other sensitive information. Occasionally, they will also send offensive content to foster disdain. According to the National Crime Reports Bureau, there were 15051 offences with a fraud purpose reported in 2018 out of 27,248 total cases, or 55.2% of all cybercrimes reported.[16]

Cyberbullying – A person is forced to do something they do not want to do by bullying, which is a type of harassment. Young people and teenagers frequently experience it. This has grown to be extremely typical. Among many other things, it involves making fictitious websites about people, making comments, posting offensive words about people, spreading pointless images or videos of people, and more. In a research conducted in Delhi by the NGO Children Rights and society, over 9.3 percent of 632 teenagers reported seeing cyber harassment, and 50% of them did not report it to their guardians, instructors, families, or any relevant digital media companies.[17]

4. Laws Under Indian Legislature

According to the head of the National Investigation Agency (NIA), social media is used by criminals in India to conduct every sixth online crime. This is well known that India passed its first information and technology law in 2000 based on the UNCIRAL model suggested by the United Nations General Assembly. Together with other provisions spread throughout this Act, Chapter XI of this Act deals with offences and crimes. There is no mention of the definition of "cybercrimes" in any law or regulation. Slang for everything having to do with computers, information technology, the internet, and computer games is "cyber." It follows that "cyber-crimes" are crimes involving computers, information technology, the internet, and virtual reality.

Cybercrime laws can be found in several statutes and even in regulations written by different agencies. A number of cybercrimes are punished by the Information Technology Act, 2000

("IT Act") and consequently the Indian Penal Code, 1860 ("IPC"). As is to be expected, several provisions of both the Indian Penal Code and the Information and Technology Act cross over.

The Knowledge Technology Act, which was passed in 2000 to oversee, control, and address issues related to IT, governs social media in India. Social networking sites are under the definition of "intermediary" under the 2000 Indian Information Technology Act (IT Act 2000). Social networking websites in India are thus accountable for a number of activities or behaviors that are illegal under Indian law.

The IT Act's Section 66A, which controls and regulates all legal matters related to social media law in India, has been put into effect to handle the country's social media laws. The transmission, uploading, and emailing of texts, letters, and suggestion that may be insulting or unjustified is expressly prohibited under this section. The offensive message is frequently some type of text, image, music, video, or other electronically stored data that can be communicated. The government currently has a tool at its disposal to prevent any exploitation of the Social Media Law India thanks to the broad powers granted by the IT Act.

However, in 2015, during a landmark judgment upholding the proper to free speech in recent times, the Supreme Court in Shreya Singhal vs Union of India [18] , struck down Section 66A[19] of the Information & Technology Act, 2000. The judgment which is being praised by the commoner and legal luminaries alike, found the provision of cyber law to be open-ended, vague and unconstitutional because it restricted the fundamental right of freedom of speech of Indian citizens.

The repeal of Section 66A does not, however, result in an absolute right to freedom of speech because similar provisions of the Indian Penal Code (IPC), such as Section 295-A[20], which deals with intentionally insulting religion or religious beliefs, Section 153-A, which sets forth guidelines for encouraging hostility between groups on the basis of faith, race, and other factors, Section 499, which discusses defamation, and Section 505, which deals with statements that encourage public mischief, will still apply to social media Invoking Sections 499 and 500 of the IPC would be one of the key provisions that might be effective against publishing offensive and defamatory content on social media. Under the IPC, a defamatory statement may be uttered orally, in writing, by signing, or by visible representation if it is done so with the intent to cause injury or knowledge that it is defamatory (IPC, section 499). As a result, section 499 of the IPC is broad enough to cover the dissemination of defamatory material online or through electronic means. Additionally, section 500 of the IPC makes defamation a crime.

Additionally, the prohibition on immorality may be a justifiable limitation on the "basic right to freedom of speech".

The scope of obscenity offences has increased because of technology. Today, anyone may easily access obscene content (including pornography) from the comfort of their own homes by clicking a mouse The creation and quick global transmission of such items are made possible by the Internet. The absence of a widely agreed-upon definition of obscenity makes legal regulation difficult. What is viewed as pornographic content in one country may not be in another.

The lack of efficient technological filters to remove unwanted content from the internet causes a lot of issues for consumers. The conventional legislation that governs obscenity

(including pornography) in India[21] is included in a few IPC clauses. Under Section 292 [22] of the IPC, it is also illegal to sell, rent out, distribute, display in public, or circulate obscene material, among other offences. Section 3 and 4 of the Indecent representation of Women (Prohibition) act 1986 [24] further criminalise the circulation or publication of pornographic images of girls. These regulations can be utilized to punish those who disseminate offensive content online.

Because of the aforementioned, even though section 66A of the IT Act has been declared unconstitutional by the supreme court, a victim of a cybercrime would not be left without recourse and would instead utilise the appropriate provision and law to demand the required relief. Although the Information Technology Act does not contain remedies for all cyber offences, other laws provide the necessary protection.

5. Conclusions / Suggestions

Social media has demonstrated its promise in a variety of areas of life, from utilising the people to overthrow our government to closing the distance between astronauts and scientific enthusiasts around the globe. According to an Aljazeera study, social media platforms like Facebook, Twitter, and others are extremely important to protest organisers.[25] Given the enormous volume of information available on social networking sites, there are many possibilities for the use of huge data in various fields. Social networking sites can be used by marketers to understand consumer behaviour and create successful marketing efforts.

The British government started monitoring Facebook, Instagram, Twitter, and blog feeds on social media.[26] The study's summary and some key findings are described here, along with the author's suggestions for how to stop such crimes. The lack of an absolute law anywhere on the globe is one of the main problems with cybercrime. The issue worsens as a result of the disproportional growth ratio of all internet-and cyber-related regulations. The Information Technology Act and the IPC changes represent a positive beginning, yet cybercrime challenges and difficulties still exist.

In addition to laws, there is a literacy gap that needs to be closed. The problem of jurisdiction is crucial to the viability of every lawsuit that is brought. These days, geographical lines appear to be eroding due to the expansion of online. Therefore, the idea of territorial jurisdiction as indicated in Section 16 of the Criminal Procedure Code and Section 2 of the International Private Law will have to give way to an alternate form of conflict settlement. Since all of the information is frequently destroyed, evidence loss may be a fairly typical and expected concern. Furthermore, the system of crime investigation is paralysed by the acquisition of knowledge outside of the territorial limits. Building a technological crime & investigation infrastructure with highly technical employees at the other end is also crucial for the Cyber Army.

Although this statute's extraterritorial operations are covered by Section 75, these operations may only be useful if they are supported by provisions that acknowledge informational orders and warrants issued by competent authorities outside of their jurisdiction and measures to encourage cooperation for the sharing of evidence of computer crimes between law enforcement agencies. Judges who are tech and cyber aware are urgently needed.[27] The judiciary is crucial in ensuring that the enactment is in accordance with current events. The P.I.L. (Public Interest Litigation), which the Kerala Supreme Court likewise accepted via email, is one such situation that requires acknowledgment.

- To improve cyber privacy these different preventive measures can be kept in mind by the people. [28] These include: Avoid letting your address or photos of yourself be used inappropriately. Never give pictures to anyone you meet on the internet, especially a stranger.
- Use anti-malware software and keep it updated on your laptops, smartphones, and other devices.
- Always pay on social networking sites securely to prevent credit and bank information from being stolen.
- Cybercrime on social networking sites should be made known to students.The destructive consequences of this virtual environment should be conveyed to them.
- Website owners and intermediaries should continue to monitor traffic and regulate any anomalies on their sites.
- Make use of the privacy settings offered on different social networking sites, like Facebook, Instagram, Twitter, and others.
- Avoid clicking on any unauthorised links on social networking sites because they can be false and made with the explicit intention of capturing your data.

In light of the aforementioned facts and the current situation in our nation, it is frequently claimed that modifications to the Information Technology Act are necessary to prevent cybercrime. India should also possess the necessary technology to completely defeat cybercriminals. In addition, as the fourth pillar of democratic, the media should play a significant role in raising public awareness of the need for social responsibility when using social media to prevent cybercrimes from occurring.

Cybercrimes have been a threat to social media since its inception, despite the fact that it is one of the main channels for their promotion. This manifests as fraudulent transactions, hacking, pornography, cyberbullying, and stalking. Despite the fact that India has numerous laws to deal with these cyber offences, the number of convictions is very low. The field of cyber forensics is young and expanding. Determining the actions and techniques to find cyber evidence must be promoted. Additionally, the Information and Technology Act must be construed in harmony with Indian law and statutes in order to manage and prevent cybercrime.

References

[1] Prashant Sharma, 'Core Characteristics ofWeb 2.0 Services' (Tech Pluto Staff, 28 Nov. 2008) accessed 23 February 2013

[2] Menlo park, Facebook Reports Second Quarter 2021 Results, FACEBOOK INVESTOR RELATIONS(july30,2021),https://investor.fb.com/investor-news/press-releasedetails/2021/facebook-reports-second-quarter2021-Results/default.as

[3] RESEARCH Gate, May 2019, Digital Media-Related Cybercrimes and Techniques for Their Prevention,TariqRahimSumro&MumtazHussain, https://www.researchgate.net/publication/333944511

[4] Suchetana Ray and Anirban Ghoshal, Every sixth cybercrime in India committed through social media: NIA, HINDUSTAN TIMES (Aug 25, 2019, 00:51 IST), https://www.hindustantimes.com/india-news/every-sixth-cybercrime-in-india-committed-

throughsocialmediania/storKscgnwjcTZ0pzVeVaOiN6M.html#:~:text=are%20growing%20exponentiallyEvery%20sixth%20cybercrime%20in%20India%20is%22committed%20through%22social%20media,annually%22between%202013%20and%202015.

[5] Sandhya Keelery, Number of cybercrimes related to social media across India 2019-2020, STATISTA (Oct. 16, 2020), https://www.statista.com/statistics/875916/india-number-of-cyber-crimes-related-to-social-media/#:~:text=In%202017%2C%21there%22were%21overcrime%21reported%21in%21the%21country

[6] Casey Crane, 33 Alarming Cybercrime Statistics You Should Know in 2021, HASHED OUT (Nov.14,2021),https://www.thesslstore.com/34-alarming-cybercrime-statistics-you-should-know/

[7] Umarani Purusothaman, Impact of social media on youth, RESEARCH GATE (Oct. 2019), https://www.researchgate.net/publication/336617719_Impact_of_social_media_on_youth.

[8] AFP, Interpol warns of 'alarming' rise in cybercrime cases during Covid-19 pandemic, DECCANHERALD(Aug.042020,18:00IST), https://www.deccanherald.com/international/interpol-warns-of-alarming-rise-in-cybercrime-cases-during-covid-19-pandemic-868499.html.

[9] National Cyber Crime Reporting Portal, Ministry Of Home Affairs, https://cyberattack.gov.in/Webform/More

[10] Mayur Joshi, Phishing in India is becoming innovative, INDIA FORENSIC (Dec. 9, 2020), https://indiaforensic.com/understandingphishingindia/#:~:text=Phishing%20uses%20'spoofed'%20e%2D,numbers%2C%20account%20usernames%20and%20passwords.&text=Phishing%20mails%20take%20you%20to%20 fraudulent%20websites.

[11] PTI, Fake ransom seeking email scam prowling in Indian cyberspace, THE ECONOMIC TIMES (May 02, 2020, 15:00 IST), https://cio.economictimes.indiatimes.com/news/digital-security/fake-ransom-seeking-email-scamprowling-in-indian-cyberspace/75503847.

[12] Diganth Raj Sehgal, All You Need to Know About Identity Theft in Cyberspace in India, I PLEADERS (Sep. 2019), https://blog.ipleaders.in/all-you-need-to-know-about-identity-theft-in-cyberspace-in-india/.

[13] ET Bureau, 4 in 10 Indians have experienced identity theft: Report, THE ECONOMIC TIMES (Apr. 07, 2020, 05:51 PM IST), https://economictimes.indiatimes.com/tech/internet/4-in-10-indians-have-experienced-identitytheft-report/articleshow/75029916.cms?from=mdr.

[14] Ranjit D. Udeshi vs. State of Maharashtra, AIR 1965 SC 881, Para 7, p. 885

[15] Farhan Shaikh, Man booked for posting obscene content on social media, THE HINDUSTAN TIMES (June 20, 2020, 22:57 IST), https://www.hindustantimes.com/cities/man-booked-for-posting-obscene-content-on-socialmedia/story-P95J5EkCjzUFUFwpWCIhaJ.html

[16] GOI, Crime in India 2018, NATIONAL CRIME RECORDS BUREAU (MINISTRY OF HOME AFFAIRS), https://ncrb.gov.in/sites/default/files/Crime%20in%20India%202018%20-%20Volume%201.pdf.
[17] Rhea Maheshwari, In one year alone, cyberbullying of Indian women and teenagers rose by 36%, SCROLL.IN (Mar.16, 2020 · 09:30 pm), https://scroll.in/article/956085/in-one-year-alone-cyberbullying-of-indian-womenand-teenagers-rose-by-36
[18] Shreya Singhal vs U.O.I, AIR 2015 SC 1523 (India).
[19] The Information And Technology Act, 2000, § 66 A, No. 21, Acts Of Parliament, 2000 (India).
[20] Indian Pen. Code. § 295-A - Deliberate and malicious acts, intended to outrage religious feelings of any class by insulting its religion or religious beliefs
[21] Tariq Rahim Sumro and Mumtaz Hussain, Social Media-Related Cybercrimes and TechniquesforTheirPrevention,RESEARCHGATE(May2019),https://www.researchgate.net/publication/333944511_Social_Media Related_Cybercrimes_and_Techniques_for_Their_Prevent
[22] Dr. Rekha Pahuja, Impact of social networking on cybercrimes: A study, 4 Epitome(2019).
[23] Anubhav Pandey, Cybercrime and Social media Websites, Pleaders(2018), https://blog.ipleaders.in/cyber-crime-social-media/.