LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

(ISSN: 2583-7753)

Volume 1 | Issue 4

2024

EPITOME OF SOCIAL MEDIA AND CYBER CRIME – SOCIOLEGAL PERSPECTIVE

Marru Vaaghdevi[1]

I. ABSTRACT

The world's use of social media is expanding gradually. To connect with one another, people of all ages and genders are opening accounts on online social networks.Some people have followers ranging from dozens to thousands distributed over several profiles. With the use of social media, individuals may connect, interact, and share content with others all over the world. But there are also a lot of false profiles out there. False accounts frequently spam reputable people by uploading offensive or unlawful stuff. Moreover, false accounts are made to harass a known individual by falsely portraying them. The enormous development in the usage of social media and networking sites has made it easier for cybercriminals to carry out unlawful operations. Social media is like honey to a wasp when it comes to cybercrime. Scammers view social media users as a captive, gullible audience that may be convinced to partake in actions they might typically be more skeptical about. Together with the ability to exchange ideas and pictures, social media has effectively developeda platform for cybercrime. Online threats, stalking, and cyberbullying are frequent crimes perpetrated on or as a result of social media. Cybercrimes may be decreased, however, by adopting precautions like using antivirus software, closing browser windows, and not pursuing strangers you find online.

The paper examines how social media affects young people as well as the factors contributing to the rise in cybercrime on social media. The Research paper lays emphasis on typical types of cybercrimes committed through social media and looks at how the law may beused to spot such crimes and stop them before they happen. The Rresearch paper also makes some recommendations on how to raise awareness of cybercrime's effects effectively and holistically among the nation's young.

[1] 2nd year B.A.LL.B student, Damodarm Sanjivayya National Law University, Visakhaptnam.

 (ISSN: 2583-7753)

II. KEY WORDS:

Social Media, Cyber Crimes, Young People , Law, Types of Cyber Crime

III. INTRODUCTION:

Social media refers to any digital tool that enables people to create and share content with the public quickly.[2] It is accessible from any internet-connected device, such a computer, smart phone, iPad, or other mobile device. Among the well-known social networking sites are Facebook, WhatsApp, Twitter, Instagram, and Linked In. Social networking is a great way to make connections, meet new people, share ideas, and expand businesses.

In the current digital era, social networking websites are widely used, which has drawn onlinescammers who want to boost their chances of obtaining victims to create many social media accounts and join various social media platforms.[3] A huge number of people utilize social networking sites, which they may access from their smart phones, laptops, or other devices. And people like sharing new videos and photos, as well as writing text or leaving comments, to show off their knowledge. With only a single finger movement, users of these websites mayconnect with acquaintances, but the majority of people are still ignorant of the dangers involved. In essence, when we use these websites, we are revealing all of our personal data, which may be misused. Facebook, What's App, and Instagram are some of the platforms whereone may rapidly get information about their whereabouts and personal profile.[4]

Social media's design aims to engage people and connect them with one another. People may now speak with one another, and corporations and other organizations can also interact with customers. The public can receive information via news sources as well. Social media has madeit possible for people to interact with one another quickly and simply. Real-time social networking has made information more widely available.

---

[2] 'Social media' (*Merriam Webster. com dictionary*) <Social media Definition & Meaning - Merriam-Webster >accessed 10 Jan 2023

[3] 'Impact of Social Media on Cyber Crime in Today's Digital Age' (*The Cable* , May 4, 2021)<https://www.thecable.ng/impact-of-social-media-on-cyber-crime-in-todays-digital-age> accessed 28 Dec 2023

[4] Swati Sharma , Vikash Kumar Sharma, 'Cyber Crime Analysis on Social Media' (2020) XI (I) BSSS Journal of Computer <https://bssspublications.com/PublishedPaper/Publish_258.pdf> accessed 30 Dec 2023

 (ISSN: 2583-7753)

On the internet, there is an incrediblequantity of social media data. On the internet, it's usual to see people exchanging information, thoughts, and frequently. People utilize social media for a number of reasons. Many people will just utilize it as a sourceof enjoyment. Some will use it to observe the actions of activists. Others will use it to search for information. It's uncommon for individuals to associate social media with news and publicinformation. Statements of criminality, however, might be interpreted in several ways. The privacy and security of the accounts provide a significant problem while using social medianetworking. Within social media sites, a large amount of data is constantly flowing. People may socialize with other like-minded folks who share their interests thanks to these internet platforms. There are several chances for users to engage on collaborative projects, produce material, interact with others, and play games. [5] Online anonymity, privacy, and security worries are legitimate. It is challenging to ascertain the precise identity of a person online or how secure their online data is. Internet users totalled4,168,461,500 as of March 2019. In essence, this represents 50.08% of the global population. Online users who utilize social media number 2.22 billion globally. This explains why 31% ofinternet users utilize social media. By 2021, the population is anticipated to exceed 3 billion.[6]

Social media is predicted to include some negative factors since approximately a third of the world's population uses it. Cyber criminals are capable of a variety of nefarious acts. It may start with a simple thing like disseminating hate speech against someone or attempting to undermine a government. These thieves use a number of techniques to get information from their victims. Methods of social engineering are used most frequently. Cyber criminals purposefully instill a sense of urgency and anxiety in their victim to cause panic. As a result, the victim won't be able to act reasonablyor confront the cyber-criminal about the incident.[7]

The below graph shows how popular social media is in India, despite the fact that the

[5] Emily Ngo, 'Social Media: The Unseen Risks of Cybercrimes' (2020) Anna Maria College <https://annamaria.edu/wp-content/uploads/2021/06/Emily-Ngo-Fall-2020.pdf> accessed 28 Dec 2023

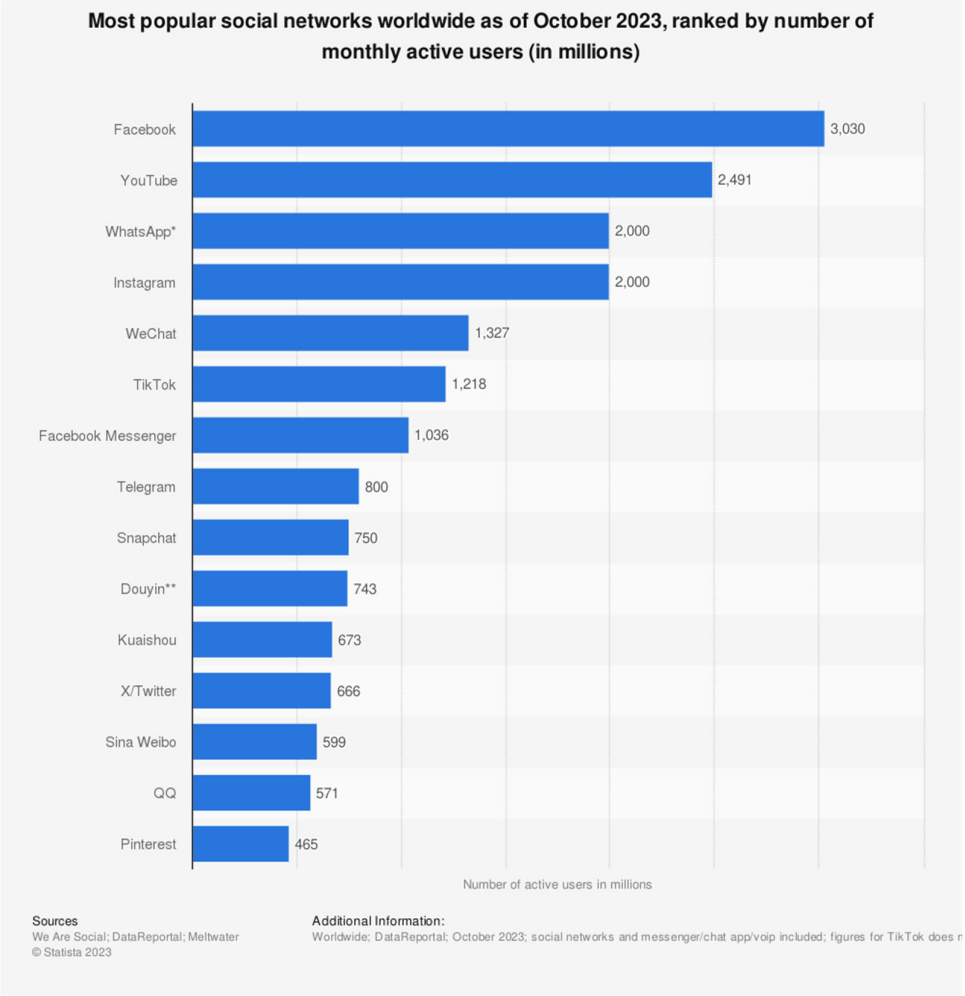
[6] 'Digital 2019: Global Digital Overview' (Datareportal, Jan 31,2019) <https://datareportal.com/reports/digital-2019-global-digital-overview> accessed 5 Jan 2023

[7] n 4

bulk of users are teenagers. Information belonging to that person might be hacked by anyone, and it could be used inappropriately by others. Anybody with access to your profile information and your photographs is free to establish a new profile using your name and information. The background activities of many people go unnoticed. Like in 2016, when one of the largest hacksin history affected close to 3 billion Yahoo accounts.[8] According to the number of active accounts as of January 2023, this statistic lists the top networks globally. With a combined total of over one billion monthly active members, Meta Platforms controls four of the largest social media networks: Facebook (main platform), Instagram, WhatsApp, Facebook Messenger, and Facebook. Facebook claimed having over 3.8 billion monthly users of its primary Family product as of the second quarter of 2023.[9]

[8] n 3

[9] Stacy Jo Dixon, 'Global social networks ranked by number of users 2023' (*Statista.com*, Oct 27, 2023) <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/> accessed 10 Jan 2024


Most popular social networks worldwide as of October 2023, ranked by number of monthly active users (in millions)
Facebook 3,030
YouTube 2,491
WhatsApp* 2,000
Instagram 2,000
WeChat 1,327
TikTok 1,218
Facebook Messenger 1,036
Telegram 800
Snapchat 750
Douyin** 743
Kuaishou 673
X/Twitter 666
Sina Weibo 599
QQ 571
Pinterest 465
Number of active users in millions
Sources
We Are Social; DataReportal; Meltwater
© Statista 2023
Additional Information:
Worldwide; DataReportal; October 2023; social networks and messenger/chat app/voip included; figures for TikTok does n

IV. CYBER CRIME:

Cyber-crime is a phrase used to describe a wide range of illegal activities, from electronic cracking to denial-of-service assaults, in which computers and computer networks play a significant part or function as a device, goal, or place. It can also refer to conventional crimes when the criminal action is made possible by computers or networks.[10] Theft of intellectual property, unauthorized access to the system, and data destruction are all examples of cybercrime. It is getting more and harder to analyze crime data on a daily basis since crime is rising along with the associated data. Without an automated method, gathering crime news willbe a tedious and time-consuming process.[11]

The term "cybercrime" combines two notions based on the root "cyber," which is derived fromthe word "cybernetic," which is derived from the Greek word "kubernân," which means "to lead or control."[12] Regardless of whether they make use of a single network, all digital activities fall under the "cyber" environment. Since no court can assert jurisdiction, cyberspace has no borders. Cybercrime is any criminal activity involving a computer, computer system, or computer network. Additionally, any crime committed online is referred to as a cyber-crime. The IT Act makes a distinction between online violations and online crimes. The former is a legal or procedural infraction that may or may not result in a penalty payment obligation because the offender is subject to civil litigation. However, as the perpetrator bears criminal accountability, an offence is a forbidden conduct that is sanctioned by a fine and/or incarceration.

Cyber-attacks often come in three different shapes. They start by attacking digital identity. Theyaccess the sensitive personal data that is available on social media and other e-commerce websites using sophisticated virus tools; they steal credit card information or fabricate identities on social media. Attacks against women and

[10] Halder, D., & Jaishankar, K., *Cyber crime and the Victimization of Women: Laws, Rights, and Regulations* (Hershey, PA: IGI .Global. 2011)
[11] n 2
[12] Editor, 'The Vocabularist: How we use the word cyber'(bbc.com, March 15 2016) <https://www.bbc.com/news/magazine-35765276>accessed 5 Jan 2024

youngsters come in second. Child pornography is a business that benefits from the expansion of the internet. When compared to males, it is women and children who are most commonly harmed by the spreading of violent or pornographic content online. Young people are routinely duped by fake accounts and conversations on social media, and they become victims of thieves both online and offline. Infrastructure attacks are the third. Forinternet terrorism, infrastructures are typically easy targets. These assaults on essential services have unanticipated effects on the economy, health care system, military, power, and other areas, which might paralyze a country.[13]

V. TYPES OF CYBER CRIMES

The variety of cybercrimes renders the online environment open to dangers of all kinds. Corporate crime and personal crime are the two main categories of cybercrime. Corporate cybercrime includes threats to a company's database or company's being attacked by hacking or by flooding the system with traffic. Cyber-stalking, cyber-assassination, bluffing, and othertechniques are frequently employed to seduce targets which comes under personal cybercrime.To be able to traverse the online world safely, one has to be aware of these crimes.

1. **Cyber-stalking:** It is a crime when a criminal annoys a victim using electronic communications, such email, instant messaging, messages posted to a website, or messages submitted to a discussion forum. Cyber stalkers rely on the facelessness the Internet offers to stalk their victim undetectable.

2. **Cyber-assassination:** It is not a particular criminal offense, tort, or act of misconduct, but rather an assassination or defamation carried out through digital media, often the Internet. TheUnited Nations Declaration of Human Rights and the Fundamental Human Rights of the European Union both encompass fundamental rights, however the penalties for "Cyber assassination" differ from nation to nation.

3. **Hacking:** It is the act of getting access to a computer, whether intentionally or unintentionally,and reading, copying, or producing data without intending to

[13] Alexander S. Gillis, 'Cyber attack'**(** *techtarget***)** <(https://www.techtarget.com/searchsecurity/definition/cyber-attack>accessed 7 January 2024

delete it or cause malicious computer damage.

4. **Cracking:** It is a method for gaining unauthorized access to a computer with the intention of doing harm**.**
5. **Carding:** It is a type of credit card fraud when pre-paid cards are charged using a stolen creditcard. Carding is the practice of using a stolen credit card to purchase gift cards from stores thatmay later be sold to others or used to purchase other items that can be exchanged for cash.
6. **Bot Networks:** These are a group of connected computers that are sometimes referred to as "zombies" because they have a virus that enables a thief to control them. Thefts of trade secrets, the appropriation of trademarks, and other intellectual property crimes are all examples of cerebral property crimes.
7. **Theft:** It is the most prevalent type of cybercrime nowadays. Credit/Debit Card Fraud, whichoccurs increasingly frequently these days, occurs when someone uses a debit/credit card without authorization to deceitfully get money or property. Credit/debit card numbers may beobtained from some leaky websites or through identity theft schemes. If we don't utilize it wisely, a computer may also hack this number.
8. **Identity theft:** It occurs when someone steals another person's information without that person's knowledge in order to engage in fraud and theft. Identity may be readily compromisedwhen we divulge important private information to an open company, irregularly in response to an email to streamline promotion or membership information, or when we do so on social networking sites without any privacy or security.
9. **Cyber terrorism:** It is one of the most deadly types of cybercrime. It uses the internet to carryout violent acts, such as slow-moving or significant disruptions of normal activity. Cyber terrorism is also defined as the observant use of disruptive actions. Now that this has spread its wings, terrorist organizations are engaging in cyber-brain warfare and influencing people's minds in order

to further their own ends.[14]

VI. INFLUENCE OF SOCIAL MEDIA ON CYBERCRIME IN THE CURRENT DIGITAL ERA:

Social networking services like Facebook, LinkedIn, Instagram, Twitter, and Orkut are widely used. The exponential growth and impact of these websites have attracted thieves, putting bothindividual privacy and national security at risk. According to authorities at the National Investigative Agency, social media is utilized by every sixth criminal in India. According to data from the National Crime Records Bureau (NCRB), there was a nearly 70% yearly rise in cybercrimes between 2013 and 2015. According to a study by security solutions firm Symantec, India came in second place after the US among nations targeted for cybercrimes using social media in 2014. Today, cybercrimes may take on many different forms to conduct offences such as invasion of privacy, defamation, identity fraud, obscenity, cyberterrorism,etc.[15] Now let's examine the influence of social media on cybercrime in the current digital era.

1. The number of cyber criminals globally has grown due to the widespread use of socialnetworking platforms.

2. Since social media allows for anonymous communication, most online fraudsters are able toevade detection after taking advantage of gullible victims.

3. Cyber criminals can easily construct a false identity on social media and use it to contact people anywhere in the globe.

4. It is simple to spread malicious software and websites on social media with as many usersas possible in a very short period of time.

5. It is simple for people to spread false information on social media

[14] M.Shruti, 'Types of Cyber attacks'(*Simple learn* ,Oct 11,2023)< https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks> accessed 12 January 2024

[15] Shivani Shinde Nadhe, 'India, a soft target for cyber criminals: Study' *(Business Standard*, May 11, 2015) <https://www.business-standard.com/article/current-affairs/india-a-soft-target-for-cyber-criminals-symantec-115050900513_1.html > accessed 10 January 2024

that can endangernational or international security.

6. Because social networking services are so popular, internet scammers can open as manyaccounts as they want under different names and utilize them for illegal activities.

7. The majority of private, sensitive information is now posted openly on social media. Ofcourse, this makes consumers more vulnerable.

8. Because there are so many social networking sites, it is simpler for cyber criminals to sendphoney and unwanted messages to unwary victims via their numerous social media accounts.

9. The rise in cyber terrorism is also partly due to the proliferation of social networking sites.

10. As a result of social media becoming a haven for online fraudsters, the criminal underworld on the dark web, where cybercriminals trade stolen sensitive data, is growing.

Social media, however, is also a powerful instrument for preventing cybercrime since it allows for the easy capture of images or videos of offenders while they conduct cybercrime. In a matter of minutes, several anti-corruption organization's and law enforcement personnel can access theimage and recorded video. This will undoubtedly be very beneficial in the investigation and conviction of cybercriminals.[16]

VII. FACTORS THAT HAVE CONTRIBUTED TO THE GROWTH IN CYBER CRIMES:

Cyber specialists have identified a number of factors that have contributed to the growth in cyber-crimes, including a lack of understanding, excessive use of or addiction to social media, and increased online activity among those seeking to make money during the COVID-19 epidemic. The majority of cybercrime cases involving social media come from Facebook and Instagram.[17]

[16] n 2

[17] Palkhiwala D, 'Lack of Awareness, Social Media Overuse Reasons for Rise in Cybercrime, Say Experts' (*Hindustan Times*, January 18, 2022) <https://www.hindustantimes.com/cities/pune-news/lack-of-

Social media has without a doubt permanently changed how we communicate. Social networking has become more important than ever since so many of us have been forced to waitout the COVID-19 outbreak in our homes. Whether we utilized them to pass the time or converse with friends and family, our social media feeds have made us feel connected, informed, or just plain amusing. However, it has also been employed to spread rumors, publicize scams, and, more recently, to steal information from COVID vaccination cards. These examples just scrape the surface of the many ways threat actors may use us on social media. In reality, it appears that fraud has only increased throughout the epidemic as network defenders race to keep up with the cutting-edge techniques used by cybercriminals. Threat actors on social media continue to leverage our naivety against us despite security upgrades and patches that help ward off upcoming attacks. Because of this, security knowledge is one of the finest resources we have when utilizing social media.

Scammers will continue to weaponize social media going ahead since it is such an accessible attack channel, and collaboration on cybercriminal forums will almost probably continue.[18]

VIII. LEGAL FRAMEWORK IN INDIA:

The Indian Penal Code, 1860, the Criminal Procedure Code, the Information Technology Act,or any other legislation, depending on the circumstances and facts of the case, may be used to prosecute and punish individuals who have committed significant crimes. They either make offensive or spammy remarks on social media, set up phony profiles, pointlessly follow individuals, or text random people for fun.[19]

A. REPORTING A CYBERCRIME:

It is now simpler to report a crime, and the identity is not made public without

awareness- social-media-overuse-reasons-for-rise-in-cybercrime-say-experts-101642523512673.html> accessed 28 Dec 2023

[18] Editor, ' How Cybercriminals Weaponize Social Media' (*Relia Quest,* August 25, 2021) <https://www.reliaquest.com/blog/how-cybercriminals-weaponize-social-media/> accessed 30 Dec, 2023

[19] Gupta K, ' Social Media Platforms and Cyber Crime' (*The Daily Guardian,* March 28, 2021) <https://thedailyguardian.com/social-media-platforms-and-cyber-crime/> accessed 30 Dec 2023

permission. Direct reports of these offences may be made at cybercrime.gov.in. Your complaint will then be directed to the relevant department in your region through the government website. As a result, going to a police station or bank is easier. (for a financial crime). The name's secrecy has prompted more people to make complaints, particularly those concerning sexual harassment. It is crucial that people are informed of these crimes in order toprevent them.

B. IMPACT ON PRIVACY

The concept of privacy includes the opportunity to decide how one's personal information should be collected and utilized, as well as the right to manage such information. Under Article21 of the Indian Constitution, which addresses the right to life and liberty, "Right to Privacy" is recognized as a Fundamental Right. Although the right to privacy is not mentioned explicitly in the Constitution, it has been acknowledged in several legal rulings. The implications of the right to privacy in the virtual world are still up for debate.

Facebook and Orkut are two instances that may be used to show the potential invasion of privacy in social media. One of the earliest extensively utilized social networking sites, Orkut,lost its appeal when Facebook joined the market. A large portion of them left their accounts inplace, allowing public access to their sensitive data. The user's personal information will be visible to everyone who enters their name into a search engine owing to Facebook's public search feature. When the privacy settings for data like gender, networks, usernames, emails, phone numbers, pictures, and videos are set to "Public," a person's identity is put at danger. Additionally, using the apps and games that are available on social media poses a serious risk to a person's identity. Secure mode is not functional for these programs. They also demandaccess to all personal data.

Social media hacking is typically seen as a violation of data protection legislation. Informationabout a person, such as name, residence, interests, family, etc., is frequently accessible on manysocial networking websites. The IT Act's Sections 43A, 72A, 69, and 69B govern data protection in India. By including a definition of "Sensitive Personal Data or Information," Section 43A broadens the scope of data protection. It also places

obligation on data controllers to adhere to "Reasonable Security Practices." Data handlers and cyber criminals may be subject to a hefty fine that exceeds Rs. 5 crores in the event of an infraction. According to Section 72A, an intermediary is accountable if he discloses "personal information" collected while providing services under a contract and such disclosure was done knowing it would likely lead to the wrongdoer's unjust loss or gain. Under Sections 69 and 69B, the State may issue directives allowing for the monitoring, collection, or interception of traffic data or information using anycomputer resource.[20]

C. CYBER DEFAMATION

According to Section 4 of the IT Act and Section 4 of the Indian Penal Code, cyber defamationis illegal in India. Earlier, Section 66A, which punishes the dissemination of very offensive material, also identified cyber defamation. However, the Supreme Court has invalidated this since it is in violation of Article 19(1)(a) of the Indian Constitution.[21]

D. CYBER PORNOGRAPHY

Pornographic websites and magazines are examples of cyber pornography, also known as cyberobscenity, which offers a platform for inciting sexual conduct online. The Hecklin's criteria, which states that "the tendency to deprave and corrupt those whose minds are open to such immoral influences" is what defines obscenity, is used earlier. The Supreme Court defined "obscene" as something that is "offensive to modesty or decency, lewd, filthy, and repulsive" in the case of **Ranjeet Udeshi v. State of Maharastra**[22]. Obscenity that serves no societal purpose or financial gain is therefore ineligible for protection under the free speech clause. Additionally, the Supreme Court stated in **Ajay Goswami v. Union of India**[23] that the standardfor evaluating a work should be that of "an ordinary man of common sense and prudence and not an out of ordinary or hypersensitive man". The IT Act's Section 67B penalizes child pornography in accordance with Article 9 of the Convention on Cyber Crime.

[20] Editor, ' Cyber Crime & Privacy" *(cisindia)*< https://cis-india.org/internet-governance/cyber-crime-privacy> accessed 12 January 2024
[21] *Sreya Singhal v. Union of India* AIR 2015 SC 1523
[22] *Ranjeet Udeshi v. State of Maharastra* AIR 1965 SC 881
[23] *Ajay Goswami v. Union of India* (2007) 1 SCC 169

Obscenity on the internet is illegal. On the basis of Sections 66E and 67, it places an obligation on the perpetrator. In order to safeguard bodily privacy, Section 66E makes it illegal to take images of another person's private areas without that person's permission. Section 67A makes it illegal to publish and transmit sexually explicit material online.[24]

E. CYBER CRIME AGAINST WOMEN:

Women all across the world are now more vulnerable to technical crimes including morphing, false profiling, and cyberbullying because to social media platforms. Although the InformationTechnologies Act and the IPC both make some effort to stop these offenses, their efficacy is still up for question. Women are also taught by society to ignore the cyberbullying they encounter on social media. As a result, males have started to take over even these online places.Feminist activists who express their own ideas on social media have come under fire from theiropponents.

They use social media to make sexual jokes and character assassinations and to threaten to rapeothers. The possibilities available to women on social media for speech and expression are quite limited. These offences are increasing despite the state and police taking harsh action. Social media is preferred by criminals since it hides their identity and does the same thing.

IX. THE VARIOUS TYPES OF CRIME AGAINST WOMEN

Women have been the victims of a variety of crimes. Among them are:

1. Cyber stalking:

Cyberstalking, which involves surreptitiously following someone or observing their online or offline behavior in order to learn anything about them or obtain personal information about them without their agreement, is one of the most popular cybercrimes targeting women nowadays. Stalking is the invasion of someone's privacy with the intent to fear, torment, torture,or intimidate the victim. Without the victim's knowledge or agreement, the perpetrator contactsand attempts to establish contact. One of the most common cybercrimes affecting women nowadays is cyberstalking,

[24] n 19

which involves secretly following someone or analyzing their online or offline behavior in order to learn anything about them or collect personal informationabout them without their knowledge. Invasion of privacy for the purpose of frightening, torturing, torturing, or intimidating the victim is known as stalking. Without the victim's consent or knowledge, the offender contacts them and makes an effort to build a relationship.

Cybercrime happens when similar actions—including password cracking, hacking for the samegoal, or when someone improperly uses the woman's identity—are carried out on purpose usingthe internet, email, or any other kind of electronic communication. The security of the victims' devices is frequently breached in order to collect any electronic device's private content, whichis subsequently utilized to extort or monitor the victims. Hackers have been known to take datafrom mobile devices that may be used to convict a criminal. It carries fines and up to three years in prison when committed for the first crime. Moreover, the penalty might be increased to five years in prison and a fine if it is repeated.

2. Cyber Pornography

Online pornographic content production, dissemination, and communication are common practices. This legislation was formerly covered under Section 292 of the IPC, which dealt withthe crime of obscenity and covered anything that was vulgar, catered to voyeuristic inclinations, or aimed to humiliate and corrupt individuals. This definition has been updated to include the generation of any profits from such a companyas a felony that is subject to legal sanctions. The consequences are a 5000-rupee fine and a five-year jail sentence. A guy violates Section 354A of the IPC, which outlaws' sexual harassment,if he knowingly sends pornographic material to a lady against her will by email, WhatsApp, orany other method. The IT Act's Section 67A also forbids these types of actions when sexuallyexplicit materials are communicated, published, or handled as such in any electronic form. The maximum penalties under the IT Act are 5 years in prison and a fine that may exceed 10 lakhs for a first conviction, and 7 years in prison and a fine that may exceed 10 lakhs for a second conviction.

3. Morphing

This includes manipulating the victim's photo in a way that betrays the victim's original identity, downloading it from the internet, putting it on social networking sites, or using any other method that might damage the victim's reputation. It is now such a prevalent practice that anybody may use it for amusement or to exact retribution, endangering the woman's modesty. It involves employing easily accessible automated software to combine the victim's image withthat of another lady wearing scant or nude clothing in order to immediately damage the victim's reputation in front of a broader audience. The most common target is a celebrity for hilarious reasons.

Sections 66 and 43 of the IT Act, which forbid actions including unauthorized downloading, copying, extracting, wiping, and changing of data, apply to these infractions. (Offenses involving computers). The accused may also be held accountable under a number of IPC clauses, such as S. 354A for sexual harassment, S. 290 for public annoyance, S. 292A for obscenity, and S. 501 for defamation.

4. Sending Obscene/ Defamatory/ Annoying Messages

The sharing of a woman's private photographs or the publication of her photos and contact information on pornographic websites are two examples of cybercrime against women. Since that it infringes on women's basic right to privacy, this also qualifies as defamation. Email, WhatsApp, and other social media platforms may all be used to send offensive or unpleasant messages.

When an act does not qualify as a crime under the Information Technology Act, women frequently appeal to sections 354A, 354 for sexual harassment, 499 for defamation, and 509 for insulting women's modesty of the Indian Criminal Code.

5. Online trolling/ pulling/ blackmailing/ Threat and intimidation.

Cyberbullying, extortion, threats, and intimidation are among the crimes committed online against women. That has become increasingly regular recently. In order to damage another person's reputation or humiliate them because of their greater power or dominant position, bullying is defined as a pattern of recurrent behavior directed at that individual. It is carried outon computers or mobile devices with an internet

connection. The internet functions more as a hindrance than a help in many scenarios. In addition to this one, several situations arise every day. But, the traditional mindset in India is to accept such inappropriate behavior and to obstruct the offender until things get out of hand.

Our people not only disobey the law, but also have no morality. These situations are happeningmore often now. That often happens in regard to political concerns.

X. STEPS TO BE TAKEN TO STOP THE CRIME

A. At the level of the government

The National Cyber Crime Reporting Portal shall be recognized as the national portal forpurposes of reporting electronic material under the POCSO Act. The Union Government, through its authorized authority, shall have the right to restrict and/or prohibit any websites and intermediaries that host content including child sexual abuse. Law enforcement agencies should be authorized to break end-to-end encryption in order touncover child pornographers.

B. ARTIFICIAL INTELLIGENCE USAGE

Tools that can analyze the conduct of every internet user are now being created. As a result, itcan help to protect the user from participating in online abuse. A cybercrime committed online not only negatively affects the victim but also the victim's surroundings since friends, co-worker, and the media amplify the suffering. During theinvestigation for this project, it was discovered that the victims' requests for help from the authorities are seldom granted, and that the regular risk of physical violence is not treated seriously. The blocking idea is useless when offenders have many accounts on social networking sites. Additionally, the current legal structure does not fairly represent the actual situation. It is desired to have a complete and successful plan. When their rights are being abused online, women need to be firmly encouraged to speak up. Theeffectiveness of the plan to stop cybercrime against women and children must also beconfirmed by the government. The complainant's privacy must also be protected. Implementing requirements of IT legislation is inefficient for achieving the requirement. Society as a whole must establish a safe environment for women so they

may report abuse to the authorities without being concerned about being judged, feeling insecure, losing their jobs,or suffering other bad outcomes.[25]

C. PREVENTIVE MEASURES:

Citizens might keep in mind a number of preventative measures to increase Cyber security.These consist of:

1. To prevent picture abuse, never send any photos over the internet, especially tounknowing friends or total strangers.
2. Anti-virus software should always be updated to prevent virus assaults.
3. File backups make it possible to avoid data loss due to virus attacks.
4. To prevent the theft of credit information, payments made to access games and appson social networking sites must be conducted through a secure payment system.
5. Cybercrime awareness lessons for children must be provided.
6. The security software that allows cookie control should be chosen.
7. Website administrators and middlemen must keep an eye on traffic and control anyirregularities on the site.
8. Disallow searches on profiles.
9. Limit who can locate you on the internet.
10. Limit the information that may be found about you online.
11. After every session, log out. Don't divulge your social media login information.
12. Refuse friend requests from people you don't know.
13. Avoid clicking on shady links.
14. Keep your social media profile's privacy settings as rigorous as possible,

[25] Dwivedi A, 'Crime against Women through Social Media' (*Times of India Blog,* December 18, 2022) <https://timesofindia.indiatimes.com/readersblog/aashank-dwivedi/crime-against-women-through-social-media-48132/> accessed 5 Jan 2024

especially forpublic/others.

15. Keep in mind that small bits of information from various posts, photos, status updates, comments, etc. may add up to expose enough about you for a fraudster to take your identity and defame you. Therefore, exercise the utmost caution when posting anything online.[26]

XI. CONCLUSION

Social media has demonstrated its potential in a variety of areas of life, from using the public to overthrow our government to closing the distance between scientists and scientific enthusiasts around the globe. According to an Aljazeera story, demonstration organizers significantly rely on social media platforms like Twitter, Facebook, and others. Given the enormous quantity of information accessible on social networking sites, there are manypossibilities for the use of massive data in various fields. Social networking sites can be used by marketers to understand customer behavior and create successful marketing strategies. TheBritish government began monitoring Facebook, Instagram, Twitter, and blog posts on social media. Since the beginning of social media, cybercrimes have threatened it. This shows up asfraudulent transactions, hacking, malware attacks, online libel, and online stalking. Although India has strong legislation to deal with these offenses, the number of convictions is quite low.The field of cyber forensics is expanding. Finding ways to find cyber evidence must be encouraged. In order to manage cybercrimes, it is also important to alter Indian law so that it reads in accordance with the IT Act. Hence in fostering cybersecurity, individuals should avoid sharing sensitive information online and diligently log out after each session. Implementing protective measures involves keeping antivirus software updated and utilizing security tools with cookie control. Data security is enhanced through regular file backups, and online transactions should be conducted through secure payment systems. Upholding privacy entails limiting personal information, educating children on cybercrime awareness, and maintaining stringent

[26] Editor, ' Social Media Crime' (*Cyber Crime Cell*) <https://cyber.delhipolice.gov.in/socialmediacrimes.html#:~:text=The%20most%20commonly%20reported%20 and,when%20to%20call%20the%20police.> accessed 2 Jan 2023

social media privacy settings.

XII. REFERENCES:

- **Case Laws:**

1. Sreya Singhal v. Union of India AIR 2015 SC 1523

2. Ranjeet Udeshi v. State of Maharastra AIR 1965 SC 881

3. Ajay Goswami v. Union of India (2007) 1 SCC 169

- **Journal Articles:**

1. Swati Sharma , Vikash Kumar Sharma, 'Cyber Crime Analysis on Social Media' (2020) XI (I) BSSS Journal of Computer <https://bssspublications.com/PublishedPaper/Publish_258.pdf> accessed 30 Dec 2023

2. Emily Ngo, 'Social Media: The Unseen Risks of Cybercrimes' (2020) Anna Maria College<https://annamaria.edu/wp-content/uploads/2021/06/Emily-Ngo-Fall-2020.pdf> accessed 28 Dec 2023

- **Websites/ Blogs:**

1. 'Social media' (*Merriam Webster. com dictionary*) <Social media Definition & Meaning - Merriam-Webster >accessed 10 Jan 2023

2. 'Impact of Social Media on Cyber Crime in Today's Digital Age' (*The Cable* , May 4, 2021)<https://www.thecable.ng/impact-of-social-media-on-cyber-crime-in-todays-digital-age> accessed 28 Dec 2023

3. 'Digital 2019: Global Digital Overview' (Datareportal, Jan 31,2019) <https://datareportal.com/reports/digital-2019-global-digital-overview> accessed 5 Jan 2023

4. Stacy Jo Dixon, 'Global social networks ranked by number of users 2023' (*Statista.com*, Oct 27, 2023) <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/> accessed 10 Jan 2024

5. Halder, D., & Jaishankar, K., *Cyber crime and the Victimization of Women: Laws,*

Rights, and Regulations (Hershey, PA: IGI .Global. 2011)

6. Editor, 'The Vocabularist: How we use the word cyber'(bbc.com, March 15 2016) <https://www.bbc.com/news/magazine-35765276>accessed 5 Jan 2024

7. Alexander S. Gillis**,** 'Cyber attack'**(** *techtarget***)** **<**(https://www.techtarget.com/searchsecurity/definition/cyber-attack>accessed 7 January 2024

8. M.Shruti, 'Types of Cyber attacks'(*Simple learn* ,Oct 11,2023)< https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks> accessed 12 January 2024

9. Shivani Shinde Nadhe, 'India, a soft target for cyber criminals: Study' *(Business Standard*, May 11, 2015) <https://www.business-standard.com/article/current-affairs/india-a-soft-target-for-cyber-criminals-symantec-115050900513_1.html > accessed 10 January 2024

10. Palkhiwala D, 'Lack of Awareness, Social Media Overuse Reasons for Rise in Cybercrime, Say Experts' (*Hindustan Times,* January 18, 2022) <https://www.hindustantimes.com/cities/pune-news/lack-of-awareness- social-media-overuse-reasons-for-rise-in-cybercrime-say-experts-101642523512673.html> accessed 28 Dec 2023

11. Editor, ' How Cybercriminals Weaponize Social Media' (*Relia Quest,* August 25, 2021)

<https://www.reliaquest.com/blog/how-cybercriminals-weaponize-social-media/> accessed 30 Dec, 2023

12. Gupta K, ' Social Media Platforms and Cyber Crime' (*The Daily Guardian,* March 28, 2021)

<https://thedailyguardian.com/social-media-platforms-and-cyber-crime/> accessed 30 Dec 2023

13. Editor, ' Cyber Crime & Privacy" *(cisindia*)< https://cis-india.org/internet-governance/cyber-crime-privacy> accessed 12 January 2024

14. Dwivedi A, 'Crime against Women through Social Media' (*Times of India Blog*, December 18, 2022) <https://timesofindia.indiatimes.com/readersblog/aashank-dwivedi/crime-against-women-through- social-media-48132/> accessed 5 Jan 2024

15. Editor, ' Social Media Crime' (*Cyber Crime Cell*)

<https://cyber.delhipolice.gov.in/socialmediacrimes.html#:~:text=The%20most%20commonly%20reported%20 and,when%20to%20call%20the%20police.> accessed 2 Jan 2023