A REVIEW OF SOCIAL MEDIA CRIMES IN INDIA

Mr. Rajdeep Ghosh, Assistant Professor of Law at Rashtriya Raksha University, Gandhinagar

ABSTRACT

Instances are rare where people are unaware of social media platforms. In the present era, social media has turned out to be omnipresent where within a few seconds only information is transmitted to unlimited sources and persons with more speed than a bullet even. People find these very useful for entertainment, business, and information (including confidential/private) sharing cum generating purposes. Usage of social media platforms also makes the users susceptible to crimes via or on the same platforms and instances are growing speedily where many ill-intended people misutilise these platforms and compromise the data of other netizens who use social media causing a gross violation of the rights of the bonafide users. In such situations, the protection of the rights of the bonafide users and punishing the culprits become a very pertinent task. This article shall endeavor to identify, detect and review the crimes that are done in or through the social media platforms in India and to provide as to how the bonafide users would legally deal with these under the prevailing laws along with putting forward a few suggestions to be followed by the users, law enforcing agencies and the legislatures for better detection, prevention, and regulation of the said crimes.

Keywords: Social media, crime, India, prevailing regulating laws, the efficiency of the laws, suggestions

1. INTRODUCTION

Bill Gates once aptly observed that "the internet is becoming the town square for the global village of tomorrow." One of the greatest outputs of the internet was the emergence of social media platforms. Social media platforms are those technology and internet-based platforms which are used by netizens to share their ideas, thoughts, expressions, and information through the usage of virtual communities and networks.[1] To put it differently, social media platforms are online platforms for online social communication and interaction between persons of different age groups. As of January 2022, three have been more than 4.62 billion social media users across the globe.[2] Among the various social media platforms, the largest platforms are Facebook, Youtube, Instagram, Twitter, Tiktok, Pinterest, Linkedin etc. These platforms are also known as intermediaries.[3&4] Before the early years of the twenty-first century, most crimes were perpetrated behind closed doors, with conventional media broadcasting information about them on their terms. **According to Ray Surette**, the introduction of social media in the first decade of the twenty-first century has resulted in a new sort of 'performance' crime, in which people construct stories of their law-breaking using text, photographs, and video, which are then widely spread online.[5] By some estimates, India is the second-largest internet consumer after China in India and has more than 800 million users.[6] The information shared on the floor of the Rajyasabha by the Minister concerned regarding the data of crimes done in or through cyberspace from 2017 to 2019 including social media platforms is over 93,000 registered cases.[7]

2. PREVAILING SOCIAL MEDIA CRIMES IN INDIA UNDER DIFFERENT LAWS

[1] Dollarhide, Maya. "Social Media: Sharing Ideas and Thoughts." *Investopedia*, Investopedia, 8 Feb. 2022, https://www.investopedia.com/terms/s/social-media.asp, last accessed on 22/02/2022

[2] Retrieved from https://datareportal.com/social-media-users, last accessed on 22/02/2022

[3] "Social media intermediary" defined (in Rule 2(w)) of Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 as one who "primarily or solely enables online interaction between two or more users and allows them" to exchange information;

[4] Retrieved from https://fpf.org/blog/indias-new-intermediary-digital-media-rules-expanding-the-boundaries-of-executive-power-in-digital-regulation/#:~:text=%E2%80%9Csocial%20media%20intermediary%E2%80%9D%20defined%20(,them%E2%80%9D%20to%20exchange%20information%3B%20 and, last accessed on 26/03/2022.

[5] Retrieved from http://blogs.lse.ac.uk/usappblog/2016/01/28/how-social-media-is-changing-the-way-people-commit-crimes-and-police-fight-them/, last accessed on 21/02/2022

[6] "The Indian Telecom Services Performance Indicators" (PDF), Telecom Regulatory Authority of India (TRAI), 30 June 2021, retrieved 22nd February 2022.

[7] Retrieved from https://www.timesnownews.com/india/article/over-93000-cybercrimes-in-three-years-as-internet-penetration-rises-can-india-do-more-to-combat-cybercrime/716251, last accessed on 21/02/2022

Social media crimes fall under the broader ambit of cybercrimes that are regulated by cyber laws. Cyber-law is a generic term that encompasses under it all the laws regulating the activities in cyberspace including crimes done under the traditional law i.e., the India Penal Code, 1860, or crimes that are specifically defined under the Information Technology Act, 2000 or under any particular judgment or special law.

2.1 UNDER THE INDIAN PENAL CODE, 1860

There are many situations and circumstances where social media crimes, abuses, and wrongs are dealt with under various provisions of the Indian Penal Code, 1860

- **Section 354-D** i. e., **Stalking** in which punishment may be up to 3 years + Fine for the first conviction and up to 5 years + Fine for second or subsequent conviction;
- **Section 506** i.e., punishment for **Criminal intimidation** (7-year year punishment depending on the appreciation of facts of the case)
- Posting of defamatory comment or material against someone- Offence under Section 66A of the IT Act, punishable with imprisonment.
- Even liking or sharing such comments can constitute an offense.
- Posting defamatory material or comment- Criminal defamation under Section 499 of IPC.
- Posting of defamatory material or comment against someone- he or she can sue you before the civil court and seek damages besides injunction.
- Posting or selling pornographic material on the net- Offence under Section 292, 292A, 293, 294 IPC punishable with imprisonment.
- Posting secret information, documents of Government, photographs of prohibited place- Punishable for the violation of Officials Secrets Act.
- Posting copied material on the website- Offence under the Copyright Act.[8]

2.1.1 The Information Technology Act, 2000:

[8] Retrieved from https://www.legalhelplineindia.com/social-media-law-india/, last accessed on 25/03/2022

The Information Technology Act, 2000 was enacted in order to combat and regulate the emerging technological crimes and wrongs along with giving recognition to electronic transactions. As social media platforms have seen rampant growth in contemporary times, they simultaneously vehemently increased the number of cyber wrongs and crimes through the usage of social media platforms. In the heading, the provisions of the Indian Penal Code, 1860 pertaining to the social media crimes were discussed and under the present heading, the social media crimes that fall under the broader ambit of the Information Technology Act, 2000 will be discussed as follows.

1. **Section 66 i.e**., Punishment for Hacking which may be imprisonment up to three years and fine which may extend up to two lakh rupees or with both;

2. **Section 66A** i.e., Offence of bullying - Sending any message (through a computer or a communication device) that is grossly offensive or has menacing character; any communication which he/she knows to be false, but to cause insult, annoyance and criminal intimidation comes under this section. For this, the available punishment is up to three years with a fine.[9]

Section 66A of the IT Act has been enacted to regulate the social media law in India and assumes importance as it controls and regulates all the legal issues related to social media law in India. This section restricts the transmission, and posting of messages, emails, and comments which can be offensive or unwarranted. The offending message can be in form of text, image, audio, video, or any other electronic record which is capable of being transmitted. In the current scenarios, such sweeping powers under the IT Act provide a tool in the hands of the Government to curb the misuse of the Social Media Law India in any form.

However, in 2015, a landmark judgment upholding the right to free speech in recent times, the Supreme Court in ***Shreya Singhal and Ors. V/s Union of India[10]*** struck down Section 66A of the Information & Technology Act, 2000. The ruling which is being lauded by the common man and legal luminaries alike, found the Cyber-law provision to be open-ended, vague, and unconstitutional owing to the restriction it caused to the Indian citizens' right to free speech.[11]

[9] This Section has been declared to be unconstitutional by the Hon'ble Supreme Court of India in Shreya Singal V/s U.O.I. (2015)
[10] AIR 2015 SC 1523
[11] Retrieved from https://blog.ipleaders.in/social-media-offence/, last accessed on 23/03/2022

3. MOST RAMPANT SOCIAL MEDIA CRIMES IN CONTEMPORARY TIMES

The avenues of social media crimes have been expanding very speedily. It is now been seen in metro city to normal city to villages or in short, it is evident in nook and corner of the society in one or other form provided internet works there and the same would keep growing as the internet penetration has been witnessing a very rapid high including in villages also which got intensified with Jio service provider and the outbreak of the Covid-19 pandemic. There are certain crimes that have been reported from time to time to have been committed very rapidly in the most rampant manner. These are explained under the following heading.

3.1. CYBER-STALKING

Cyber-stalking is one of the practices whereby someone stalks or harasses another one over the internet. When one person shows disinterest but the other person instead of being knowing the disinterest concerned tries to harass or follow the person through the internet or electronic media then it is cyber-stalking or internet stalking or online stalking. The stalking in physical form in the physical world has greatly been replaced by stalking in the virtual world due to the Covid-19 pandemic, that too primarily through the usage of social media platforms. This has been dealt with under the provisions of the Indian Penal Code, 1860 mainly under Section 354D & Section 509 of IPC and under certain particular circumstances also under the provisions of Information Technology Act, 2000. Cyber-stalking includes false accusations of a defamatory character or hacking for vandalizing the victim's website making sexual comments for publishing things that are intended to defame any person or personally targeting the victim of a crime or making fun or humiliating someone to form a gang against them. There are many reasons for cyber-stalking which include jealousy, obsession, and attraction, erotomania, sexual harassment, revenge, and hate. There are many kinds of Cyber-stalking also, say for example stalking through emails, internet stalking, and computer stalking, catfishing, monitoring and checking location chek-ins on social media, visiting virtually through google map street views, hijacking webcam, installing stalkerware, looking at the geotags to track the location.[12] There are again a few types of Cyber-stalkers for example obsessional stalkers, obsessive love stalkers, erotomanic stalkers.

[12] Cyberstalking in India - Meaning, Types & Provisions in Law, retrieved from https://www.lawyered.in/legal-disrupt/articles/ what-is-cyberstalking/ , last accessed on21/03/2022

There are cyber cells which we can be approached in case of Cyber-stalking and there is also an online grievance redressal forum started by a National Commission for Women and other government agencies which can help to report the same to the websites concerned or one can also offer an FIR in the local police station or one can also report the same to the CERT i.e., Computer Emergency Response Team, these are responsible in order to protect the cyber victims and for investigation of the same issues.[13]

If the stalking is done in an obscene manner then that will attract section 292 of the Indian penal code. Again Section 507 IPC states that if there is cyber-stalking attached with criminal Intimidation through anonymous communication then this Section can also be invoked to punish the culprit. Then under section 509 of IPC, a stalker can be charged if he infringes the privacy of a lady by making any gesture by emails, messaging or any other platform of social media and this offence can be punished under this section but when we see closely then we find that there are many lacunas of these legal provisions and this includes it is gender bias provisions in as much as its focus are solely on women's modesty and that overlooks the reality that cyber-stalking can also take place against men so it is not a gender-neutral provision then under Information Technology Act 2001 provision that is Section 67 which is actually a copy of section 292 Indian Penal Code. The current provision provides for the determination of any published obscene material in electronic form about the victim on social media then the accused will be charged under section 67 of the Information Technology Act. There is another section i.e., Section 67A of the IT Act. This was inserted after the 2008 amendment, it actually has provides for punishment to any person who tries to publish any material which is sexually explicit in nature and that is published through electronic forms like emails, messages, or social media and Communications. Then again there is another section that is section 67B of the IT Act that also was inserted by virtue of the 2008 Amendment Act for the first time and this section again provides for the punishment of the persons who are involved in targeting children below the age of 18 years and disseminate content depicting the teenagers engaging in sexual behaviour and thus terrify them.[14] To conclude, we can say that the Information Technology Act or the Indian Penal Code does not specifically address the subject of Cyber-stalking and but still, there are provisions under which we can bring cyber-stalking into the Court of law

[13] CYBER STALKING IN INDIA – Vidhisastras, retrieved from https://vidhisastras.com/cyber-stalking-in-india/, last accessed on 24/03/2022

[14] 3 Laws on Cyberstalking in India as Per IT Act and IPC, retrieved from https://www.writinglaw.com/cyberstalking-laws-in-india/, last accessed on 23/03/2022

and the current provision should be considered and should be enhanced so that the victim's interests should be protected.

3.2 CYBER DEFAMATION

The Internet has become one of the easiest ways to communicate with people to share and to disseminate information, views, and perspectives, in fact, in a fraction of seconds, information can run over the internet and can reach an unlimited number of people. Now, when one person uses this platform for guilty intention and publishes anything by way of writing or by visible representation intending to injure the reputation or image of another person in the estimation of third persons or the public in general then it is known as cyber defamation. Defamation has been defined under Section 499 of the Indian Penal Code as "whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter excepted, to defame that person".[15] Sections 500 to 502 provide for the punishment of different types of defamations. **Section 500** states that "whoever defames another shall be punished with simple imprisonment for a term which may extend to two years, or with fine, or with both."[16] **Section 501** provides that "whoever prints or engraves any matter, knowing or having good reason to believe that such matter is defamatory of any person, shall be punished with simple imprisonment for a term which may extend to two years, or with fine, or with both."[17] **Section 502** mandates that "whoever sells or offers for sale any printed or engraved substance containing defamatory matter, knowing that it contains such matter, shall be punished with simple imprisonment for a term which may extend to two years, or with fine, or with both."[18] Further, **Section 503** states that "whoever threatens another with any injury to a person, reputation or property, or to the person or reputation of anyone in whom that person is interested, with intent to cause alarm to that person, or to cause that person to do any act which he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threats, commits criminal intimidation".[19] The Information Technology Act 2000 had section 66A which states that any person who sends

[15] Section 499 of the Indian Penal Code, 1860
[16] Section 500 of the Indian Penal Code, 1860
[17] Section 501 of the Indian Penal Code, 1860
[18] Section 502 of the Indian Penal Code, 1860
[19] Section 503 of the Indian Penal Code, 1860

or disseminates any grossly offensive material or menacing character through a computer resource or communication device in cyber-space.[20]

3.3 CYBER TROLLING

- Posting of defamatory comment or material against someone- Offence under Section 66A of the IT Act, punishable with imprisonment.
- Even liking or sharing such comments can constitute an offense.
- Posting defamatory material or comment- Criminal defamation under Section 499 of IPC.
- Posting of defamatory material or comment against someone- he or she can sue you before the civil court and seek damages besides an injunction.
- Posting or selling pornographic material on the net- Offence under Section 292, 292A, 293, 294 IPC punishable with imprisonment.
- Posting secret information, documents of Government, photographs of prohibited place- Punishable for the violation of Officials Secrets Act.
- Posting copied material on the website is an Offence under the Copyright Act.[21]

3.4 Fake profiles, fraud, cheating by personation[22]

Creating fake profiles or creating profiles of other persons without that persons' consent on social media platforms and doing anything which is illegal or not justified by law for the time being in force is another form of social media crime in as much as this type of activity would either be intended to commit fraud or to cheat any person by way of personation[23][24] or to make morphed photographs, doctored video or to publish or transmit any private or confidential data

[20] This Section has been declared to be unconstitutional by the Hon'ble Supreme Court of India in Shreya Singal V/s U.O.I. (2015)
[21] Retrieved from https://www.legalhelplineindia.com/social-media-law-india/, last accessed on 24/03/2022
[22] "Cyber Crime Cell." *Cyber Crime Unit- Delhi Police*, http://www.cybercelldelhi.in/socialmediacrimes.html , accessed 31 Mar. 2022.
[23] Personation means pretending to be a person who he is not.
[24] Punishable under Section 66D of the Information Technology Act, 2000

or information[25], obscene information[26] in contravention with the law of the land.

3.5 Hacking and dealing with sensitive, personal, and confidential data of the bonafide user

The term 'hacking' was initially defined under Section 66 of the Information Technology Act, 2000 as "whoever with the intent to cause or knowing that is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking". But the 2008 Amendment Act replaced this provision with a new provision and changed the outlook of hacking in new terms and these terms and essential elements have been provided under Section 43[27] which says that if any person without the permission of the owner or any other person who is in charge of a computer, computer system or computer network does anything specified in the section itself would be liable to be penalized and Section 66[28] says that if any person does anything that is provided under Section 43 with dishonest intention or fraudulently would be liable to be punished. In simple words, all hackings are not punishable after the 2008 IT Amendment Act[29] and thus ethical hacking or white-collar hacking is not a crime at present in India. Under Section 66 for the commission of the crime of hacking, the punishment for the guilty person is extended up to three years of imprisonment or upto five lakh rupees or both.

4. HOW TO INITIATE LEGAL ACTION AGAINST SOCIAL MEDIA CRIMES?

One can lodge an FIR in a local police station to have the matter investigated. Further, the concerned informant can also request the S.P. concerned to act speedily as the matter at hand requires. Further, he/she can lodge online complaints to the cybercrime reporting portal https://cybercrime.gov.in/ or can contact the National women's helpline number which is 181[30]

5. LIABILITY OF INTERMEDIARIES IN SOCIAL MEDIA CRIMES

[25] Punishable under Section 66E of the Information Technology Act, 2000
[26] Punishable under Section 67 of the Information Technology Act, 2000
[27] Section 43 of the Information Technology Act, 2000
[28] Section 66 of the Information Technology Act, 2000
[29] Laws Against Hacking In India - iPleaders, 2022, retrieved from https://blog.ipleaders.in/laws-hacking-india/ , last accessed on 02/04/2022
[30] Retrieved from https://citizenmatters.in/complaint-against-online-trolling-cyber-crime-guide-7172, last acc

India's new rules on intermediary liability and regulation of publishers of digital content have generated significant debate since their release in February 2021. **The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021** (the Rules) have "recast the conditions to obtain 'safe harbor' from liability for online intermediaries and unveiled an extensive regulatory regime for a newly defined category of online 'publishers', which includes digital news media and Over-The-Top (OTT) services."[31] From now onwards, the intermediaries will also be made responsible for any sort of wrongs or crimes that are done through their platforms except in certain exceptional situations.[32]

6. CONCLUSION AND SUGGESTIONS:

As we know that science can be used both as a blessing and as a curse. This saying also fits with the rampant usage of social media platforms which are used as a medium to unleash, cherish and boost up one's interest but simultaneously many times, these also hurt the life, liberty, interest, and property of persons. So, people must use these cautiously to avoid any sort of unnecessary and unavoidable harmful consequences.

About Sections of law under which the accused may be tried can be both under the Indian Penal Code, 1860 and Information Technology, Act, 2000 for cybercrime are the combination of crime + cyberspace. The legal provisions enumerated above are not exhaustive but are illustrative only. There are many other provisions regulating crimes done in cyberspace, including social media. But there are many situations where new horizons of crime are done via or in social media which have not been explicitly dealt with under any specific law which again gives room to the concerned courts of law for using their discretion and interpreting the existing provisions of law to deal with such grey or silent areas for ensuring justice.

SUGGESTIONS

Crime takes place in every society and in every generation because ill-intended persons exist in all forms of society but the intended victims can always take some precautionary measures by which they can protect or limit themselves from the commission of any crime or from the worse effects of the crime. Social media crimes are done in or through a virtual world that is comparatively new in criminal jurisprudence which has been spreading their presence in every

[31]Retrieved from https://fpf.org/blog/indias-new-intermediary-digital-media-rules-expanding-the-boundaries-of-executive-power-in-digital-regulation/, last accessed on 25/03/2022
[32] As per IT Rules 2011 relating to intermediary as amended from time to time till date.

nook and corner of society as the popularity of social media platforms has touched almost all segments of society starting from children to teenager to young people to aged people. In simple words, more users signify more number of probable threats, so the bonafide users should take utmost precautions and due diligence while using the so-called media platforms in order to protect themselves from the menace of growing social media crimes. The following are the few suggestions that the bonafide users may take into account, as precautionary measures, in order to protect, safeguard and prevent any probable social media crimes against them:[33]

i. The users should use strong passwords which cannot be easily known;

ii. The users should keep their social media accounts private and should not share their login details with anyone. They should make sure that what they share in or through their accounts can be accessed by the people of their confidence;

iii. The users should protect their data by way of encrypting the same;

iv. The users should take proper precaution and care to grant or accept the terms and conditions of any application in order to use them because it may contain harmful elements also;

v. The users should protect their identities on social media platforms as much as possible;

vi. The users should use the latest available security software for their computer systems and devices including mobile phones;

vii. The users should report the cyber incident or the cyber-crime that took place against them on or through social media platforms to the designated authorities or the local police without causing any unnecessary delay;

viii. The law enforcement and the investigating agencies along with the public prosecutors should be properly trained, skilled, and equipped with the emerging trends of technology-driven crime and technology-driven investigation techniques.

[33] MYADVO TECHSERVE PRIVATE LIMITED Container: MyAdvo.in URL: https://www.myadvo.in/blog/cyber-crime-in-india/ , last accessed on 03/04/2022