VOLUME 4 | ISSUE 2

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

CRITICAL ANALYSIS OF CYBER CRIMES CAUSED IN TWENTY FIRST CENTURY BY ABUSEMENT OF SOCIAL MEDIAS

- Dr. N. Nisha Devi[1]

Abstract

The advent of recent technological developments apart from its connectivity and accessibility feature, also leads to major complicated issues especially in social medias by impersonating one's own identity. This paper exposes the current cybercrime issues in India that are most prevalent in social medias in which the fraudsters uses such platforms for money related scams, also the closed circle theory used by them that aims the selected sections of people for such crime. Subsequently various Indian quantitative samples are analyzed in the view of the emotional attributes of the victims of the crime, which benefits the cybercriminals for this cause. In order to monitor such crimes, there are effective Indian statutes, that govern such cyber-scams and been a pioneer for many other countries in curtailing cybercrime through technology. The capacity building among the law enforcement authorities is also the need of the day for being equally competent in knowing the guilty intention of the cyber criminals. The reports of National Crime Records Bureau stands as an advocating document that technological implications are the point of origin of such crime, meanwhile that cannot be withered away from the people, rather more effective preventive measures alone will solve this cybercrimes which focuses monetary scams in India.

Keywords: Cybercrimes, Cyber Money-Scams, Impersonation, Misrepresentation, Social Media.

[1] Assistant Professor, Government Law College, Chengalpattu

Cyber Crimes - An Introduction

In the Industrial Revolution era 4.2, which paves way for the scope of data technology and data exchange especially in the cyber-physical systems (CPS) and propagates more complex actions of humans that are to be substituted to the cyber network. Of late, due to the drastic development of digital platform, more participants play an active role here, compared to the conventional way of interaction. Indian cyber security issues always been an example for the direct proportionality in the increased crimes and cyber attacks. National Crime Records Bureau (NCBR) reported that cyber crimes in India have been in a drastic growing factor of about 11.8% rise in 2020.[2] With this context, the fraudsters took a digitized weapon called "Digital Impersonation" of famous persons in the social medias to deceive the victims friends and well-wishers. The Mens Rea behind this act is the guilty intention to make money scam and for fraudulent representation of the actual person, which is an offence for "cheat by personation" by knowingly substituting one person for another under Section 416 of the Indian Penal Code.[3] With this increasing contemporary crime nature, efficient cyber laws accompanied by proactive cyber law enforcement mechanism is the need of the day for India. Since the cyber criminals are being the black hat hackers and indulge in data theft, the opponent (law enforcement agency) should be well equipped with the latest updates in the information technology field.

How misrepresentation occurs in social medias.

In this growing trend of vast usage of social medias, many people have even multiple accounts for the same platform. culprits use this as an opportunity to have their monetary gain by interacting in such kind. Money scam is the prima facie of the crime which is accompanied by section 420 of the Indian Penal code, "Cheating".[4] Owing to the focus on the famous personalities and VIP's in the society, the fraudsters steal the in formations from their original

[2] The Hindu, https://www.thehindu.com/news/national/india-reported-118-rise-in-cyber-crime-in-2020-578-incidents-of-fake-news-on-social-media-data/article36480525.ece (last visited Feb. 20, 2022)

[3] Indian Penal Code, 1860, Section 416, No.45, Act of Parliament, (India)

[4] Indian Penal Code, 1860, Section 420, No.45, Act of Parliament, (India)

identities and create an cloned copy of the victims account. Though in reality these such literal way of cheating is merely difficult, in social medias and online platforms it becomes a very easy process for them. This circumstantial supports prove that there are around 200 million fake Facebook accounts are there globally for the purpose of looting money by sending various related messages.[5] Misrepresentation is in its true nature that even the original identity of the social media account is put forth for various questions.

The best example for growing misrepresentation in the social medias especially in Facebook is the more than 30 billion pieces of digital contents are shared through this and many miscellaneous updates and other are done here and then by the users of the profile. when it comes for the place of the customers review, then the user behavior is given due importance by the social media company in order to remain in peak among its competitors. another stereotype that has been created among the Indian nations is that the reliability of the complex nature of using such platforms for any cause in which the trust worthiness will not be doubted, and significantly not all individuals across the sub-continent are literates, which adds on the supportive nature for the acceptance of the opponents misrepresentation without any haphazard nature.[6]

Impersonating factors of closed circle theory

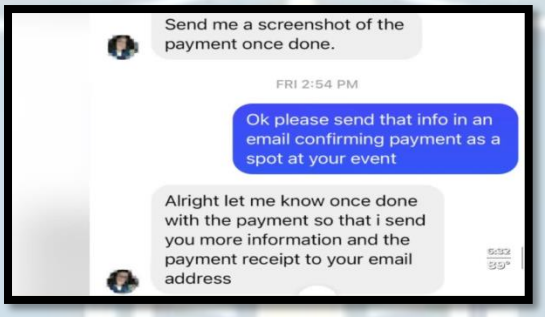
Money scams cybercrime is the old wine in the new bottle, which has its own true nature of fraudulency to general public. When a source is targeted by the attackers, it is mostly based on the closed circle theory[7] which intends to make efficient scams within that circle. In India, the most common issue is the Facebook money scams that have been reported several times to the cybercrime police departments. The best example can be of any institution where the victim is

[5] The Hindu Business Line, https://www.thehindubusinessline.com/info-tech/facebook-may-have-over-200-mn-fake-or-duplicate-accounts-globally/article22650261.ece, (last visited Feb. 22, 2022)

[6] Church, Mitchell; Thambusamy, Ravi; Nemati, Hamid. 2019. User misrepresentation in online social networks: how competition and altruism impact online disclosure behaviours. Behaviour and Information Technology. https://doi.org/10.1080/0144929X.2019.1667440

[7] Jahankhani, Hamid & Al-Nemrat, A.. (2012). Examination of Cyber-criminal Behaviour, International Journal of Information Science and Management

associated with in a high designation, of course it is common that his subordinates will be having a fiduciary relationship with that official, in this context if any help in any kind is been asked by the high designated person, then it is very hard for their subordinates to deny. This weakness has been a great advantage for the fraudsters. Family and friends are the next targeted groups where the question of strangeness do not exist. When such closed circle conversation arises it is negligible factor of arising many questions regarding the acceptance and the validity of the profile.



(Source: Screenshot of Facebook messenger conversation with the fake account)

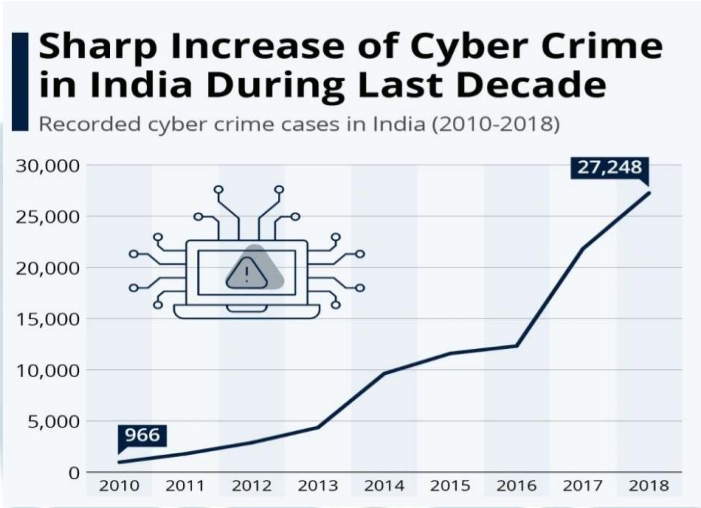
Various Indian samplings

Indian examples stands in par excellence for the fact that cybercrimes through misrepresentation is in full strength in the society. In September 2011, the very first incident took place in Bengal where the fake identity of social media was created for tarnishing a person's image. Subsequently, there have also been reported by the Alipore court that a 30 year old man was convicted for allegedly creating a fake facebook profile of a law student from a well recognized institute and by using the above said closed circle theory he has planned to gain from the monetary scam.[8] Fiduciary relationship is also the most essential matter of concern because most of the University Professors are targeted by the fraudsters that clearly indicates the fiduciary nature of relationship in society is more likely to gain them.

The approximate value of the clustered group of cyber attacks in the social media is not only limited to facebook but also to all the social media accounts, gone are the days where such platforms are used for the healthy info-building purpose and nowadays the only aim is to exploit

[8] The Times of India, https://timesofindia.indiatimes.com/city/kolkata/one-of-citys-first-fb-fake-profile-cases-ends-in-1-year-jail-fine/articleshow/81638641.cms, (Last visited on 26-02-2022).

the invention in all forms by neglecting the actual nature of the intent by his peers to us the forum. The famous decided case, Akshay kumar Vs. The State of Bihar on November, 2018 explains clearly how friendship is been used as a tool for the projection of the Mens Rea of the cyber intent of causing harm to their hormonal relationship[9]. All these factors explicitly prove the raising graph of cybercrime in India.



(Source: National Crime Records Bureau of India)

Emotional attributes in white-collar cybercrimes

White-collar cybercrimes which intends to have only the online as a source of attack and destination of the attacked, many focuses in the analyzing trend of emotional attributes that pave way for catalyzing the process of attack in the positive manner. Indian societies have witnessed many emotional crimes in its history. The emotional intelligence is used by the fraudster in the name of social services and any cause for a noble nature, if this doesn't works out, then the target is in the name of his or her family and relatives. This concept of white-collar crime was explained by Donn Parkes in his early pioneering work in this area saw the computer, to a large extent, but the related aspect is somewhat peripheral to the well-placed offender and subsequently, the key to the offence - a technical tool or device to facilitate individual in a wrong intention was fulfilled. (Parker, 1976; 1980, 1983).[10] On the other way, if the cyber attack by the

[9] Akshay Singh @ Akshay Kumar vs The State Of Bihar on 29 January, 2020

[10] Christopher Hamerton, White-Collar Cybercrime: Evaluating the Redefinition of a Criminological Artifact, Journal of Law and Criminal Justice December 2020, Vol. 8, No. 2, pp. 67-79 ISSN: 2374-2674(Print), 2374-2682

fraudsters source, say for example, a facebook fake profile, is been questioned by the victim for such criminal intention, the fiduciary relationship as discuses earlier in this paper will be lost by the victim. In this juncture, a great question arises is what is the loss for a fake fiduciary relationship that has been put forth to danger? Here, the important concept "emotional attributes of the cybercrime" is inevitable in nature, since it is human tendency to have a concern for their societal relationship before which the security aspect falls secondary.

Societal stimuli that governs social media cybercrimes

In the era of modernization and culturalization, all the intention of a human behavior is majorly governed by their social stimulus or otherwise called as the external seed for Mens rea of a crime. We are in to the society where an individual's privacy is given more importance than the misbehaving intention with the information technology. In K.S. Puttaswamy Vs. Union of India,[11] the apex court guaranteed the significance of right to privacy as a Fundamental right enshrined in our Indian Constitution. With the eyes of such nature, the "Institution of Family", one of the social institution where we live in, cannot regulate the modes and means of the social media usage of one of its members. Meanwhile the cybercrimes are happening irrespective with socially excluded or included individuals, but the nature of primary socialization is comparatively absent in some cases and boosts the cybercrimes that occur in social medias.

Social alienation is the hidden factor of determining the wrong intention of the cybercrime, for example, if an socially healthy person interacts with his surrounding in a better way and his level of interaction remains great when comparing the socially alienated person. In search of such lost social relationship, many young minds wander around social medias for at least gaining the lost social connect. Furtherance, in this mindset the fakeness of the profile and the fraudulent nature behind the screen remains a mystery for many of the victims. Inversely, this effect of social relationship also remains the stimulus for a person's Mens rea to indulge in such social network crime.

Statutes governing digital impersonation

[11] Justice K.S.Puttaswamy(Retd) vs Union Of India on 26 September, 2018

Indian Laws are pro-active in monitoring and regulating the social media cybercrimes nevertheless the loop hole arises in the name of privacy. The father of Indian technology statute, "The Information Technology Act - 2000", ensures proper acceptance of technical issues and disposing the same in a speedy and justifiable manner. Especially in this Act, chapter XI, (Section 66 to 78) which deals with the offences relating to the information technology crimes acts a great tool for curbing social media cybercrimes. Initially, the person with the guilty mind, plans to attempt the cybercrime by cloning the victims original social media account by stealing the information's from them, where Section 66(E) of the Information Technology Act-2000 applies as *"Punishment for violation of privacy - Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both."*[12] Secondly the fraudster begins to cheat the targeted person by impersonation where Section 66(D) of the Information Technology Act comes in to picture as *"Punishment for cheating by personation by using computer resource - Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees."*[13] In addition to these criminal behavior, cheating by personation is also a punishable offence according to Indian Penal Code, in Section 416, which pronounces, *"Cheating by personation - A person is said to "cheat by personation" if he cheats by pretending to be some other person, or by knowingly substituting one person for or another, or representing that he or any other person is a person other than he or such other person really is."*[14]

Conclusion

Capacity building among the law enforcement agencies are the need of the day in such blooming nature of social media cybercrimes, it is the prime duty of the competent authority (the law enforcement agencies including cybercrime police department) to take both preventive and

[12] Information Technology Act, 2000, Section 66(E), No.21, Act of Parliament, (India)
[13] Information Technology Act, 2000, Section 66(D), No.21, Act of Parliament, (India)
[14] Indian Penal Code, 1860, Section 416, No.45, Act of Parliament, (India)

precautionary measures for such cybercrimes. If this process remains inactive without proper updation with the intent, organization, and commitment of such crime and sometimes more brainy than the persons who are committing such cybercrimes. Nevertheless the self precautionary measure by the users of any social media too is crucial to decide whether technological inventions remains boon or bane in our society.