JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

EMERGING TRENDS OF CYBERCRIME IN INDIA WITH SPECIAL REFERENCE TO WOMEN

Abhishek Singh (Author)[1] Dr Khaleeq Ahmad (Co-Author)[2]

Abstract

India is not an exception among the countries around the world which keep facing the growing criminal tendencies in cyberspace. This paper looks at the cybercrime trends emerging in India covering the feminization aspect. The research examines different types of cybercrimes including cyberbullying, cyber-harassment, cyberstalking, the revenge porn, financial fraud, and the identity theft, etc. The research shall deal with techniques and technologies which are used by cyber criminals to target women which include social engineering, phishing, malware attacks and social media exploitation among others. The paper proceeds to explore the legal and regulatory framework in India that deal with the issue of cybercrimes against women which includes the provisions of the Information Technology Act, 2000 and subsequent amendments to cater to the newer issues. Additionally, it mentions the role of law enforcement agencies, investigation and prosecution difficulties, and the necessity of specialized training and infrastructure integration to deal with online crimes appropriately. Furthermore, it comes to light that psychological and social consequences of cybercrime for women can comprise of privacy violation, mental health effect, and the society custom. It furthermore analyzes preventing steps including cyber security campaigns, digital literacy programs, encryption, and secure online platforms. Through the critical examination of the state-of-the-art research, case studies and data, this note seeks to provide insights into the dynamic nature of cybercrimes in India and the specific vulnerabilities that women face in the digital world. The outcomes and suggestions of this study can be used as a basis by policy pundits, law enforcement, advocacy groups and others to develop ways and means to prevent cyber threats and build a safe web for the fairer sex.

[1] Student of B.A.LL. B Final Year, Law College Dehradun, Uttaranchal University, Dehradun, Uttarakhand, India, singhabhishek2268@gmail.com.
[2] Assistant Professor, Law College Dehradun, Uttaranchal University, Dehradun, Uttarakhand, India, khaleeqamu@gmail.com.

Key Words – Cybercrime, Cyber Stalking, Cyber Law, Women, IT Act

I Introduction

Increasingly, cybercrime is a matter of concern in India, characterized by a rapid increase in the number of reported online offences. The cybercrime has not spared any participant of the society, particularly women. The proliferation of new technologies and the wide use of the internet has created a new space for criminals to target individuals, especially women, by employing different techniques like phishing, online harassment, cyberbullying, identity theft, and financial scams. The targeting of female with social media platforms by cybercriminals is one of the new trends of cybercrime in India. Women are more prone to online maltreatment and cyberbullying since those occasions discriminate on their sex while using platforms like Facebook, Twitter, and Instagram to spread hate comments, threats and intimidation. These can have profound effects on mental health and well-being of the women, often resulting in anxiety, depression, and even suicide in extreme cases. Of the disturbing trends is the growing number of instances where women are stalked and harassed online with their attackers using online platforms to track their victims, gather personal data, and harass them. It may result in women's safety and security being jeopardized, which may then progress to physical harm or death in extreme situations. Along with identity theft and financial fraud, cybercriminals are increasing their efforts to steal personal information of individuals such as bank account details, credit card numbers, and social security number. These criminals use complex methods for the purpose. Women are the most likely crime victims in this category because they are assumed to be weaker and less knowledgeable about web security standards. In order to recognize the emergence of cybercrimes targeting women in India, it is important to create awareness on online security measures and be safe on the internet. Women need to be made aware of the risks that involve social media platforms use and about the necessity of safeguarding their privacy online. Moreover, law enforcement agencies must work on making themselves stronger.

The recent cybercrime trend in India particularly women clearly show the necessity of sensitizing, educating, as well as enforcement measures to guard women from online dangers and to see that they remain safe and secure in the internet era. Through the solution of the problems mentioned above, we can develop a safer and more secure internet for women of India.

II Recent Trends of Cybercrime

Cybercrime in India is increasing as a result of the fast growth of digitalization of a number of industries and rise in Internet usage around the country. The changing look of the technological background presents both the edges to the cyber criminals using advanced methods of attacks but also the opportunities for the individuals, businesses and governments. Following are recent cybercrimes -

i. *Phishing and Social Engineering Attacks:* Among various cybercrimes in India, phishing continues to be the most rampant. Spammers dupe naive users by the mail, messages or calls in order to make them give away their login details, credit card information or personal data. Social engineering strategies are targeted at people's minds; therefore, people are more likely to be deceived.

ii. *Ransomware Attacks:* Ransomware attacks have spiked dramatically, compromising organizations of all calibers such as the government agencies, healthcare institutions, school systems, and businesses. The offenders use the malicious software to encode important data by requesting ransom payments in return of the decryption keys. The WannaCry and Petya were significant cases with severe consequences that spread across the planet as well.

iii. *Data Breaches and Information Theft:* Data breaches involving prominent persons in India have exposed millions of its users' personal details including Aadhaar information, bank details, contact numbers etc. Cybercrimes such as the data theft is sold on underground forums or used for identity theft, financial fraud, or targeted phishing campaigns.

iv. *Cyberbullying and Online Harassment:* Social networking, instant messaging and other internet services have contributed to the increasing cases of cyberbullying and harassment mainly among children, adolescents as well as women. Verbal abuse, intimidation, and non-consensual distribution of private content create emotional alarm and safety issues.

v. *Financial Frauds and Digital Payment Risks:* With growing usage of electronic payments, malefactors steal information from bank networks, mobile wallets, and online transaction interfaces. For instance, card swiping, SIM swapping and fake apps/phishing sites target users' bank accounts and result in unauthorized transactions and money loss.

vi. *IoT Vulnerabilities and Botnet Attacks:* Building up the Internet of Things (IoT) devices entails brand new security issues. IoT devices that are of low quality are used as botnet members, for DDoS attacks, or to get away with data theft. Fundamental device security along with frequent updates prevent them from being easily exploited.

vii. *Emerging Threats:* Deepfakes and AI Manipulations: Recent advancement of deepfake technology, which is supported by AI, create new threats by making it possible to modify audio, video, or text content in such ways that they become fake or misleading. AI-based attacks not only take advantage of weaknesses in cybersecurity defenses, but also pressure the need for flexible security measures. Create an Amazon.com profile that provides valuable information about the products and services that are offered by the company.

viii. *Regulatory Compliance and Data Protection:* Due to the recent enactments of the Personal Data Protection Bill and related amendments to the Information Technology Act, businesses and organizations in India now take the task of staying in compliance with regulations and implementing stringent information protection measures seriously.

The tackling of these trends is a cohesive movement comprising of government agencies, police department, cyber experts, businesses, and public awareness campaigns. Boosting cybersecurity awareness, proactive threat intelligence, plus investment in cybersecurity technologies, incident response readiness, and effective enforcement of cybersecurity laws can help India win over cybercrime and secure its digital environment.

III Legal Protection Against Cybercrime

A. INFORMATION TECHNOLOGY ACT, 2000

In 1996, to encourage global regulatory uniformity, the UN International Trade Commission introduced the e-commerce model rule. This model legislation has been approved by the UN General Assembly as the basis of numerous cyber rules. India quickly became the 12th nation in the world to legitimize cyber laws. Post the first draft, established in 1998 by the Ministry of Commerce under the E-Commerce Act, adopted in May 2000 by revised Bill on information technology. Finally, with the implementation of the IT Act in October 2000, things were under regulation. This Act carefully traced any trifle online, cyber and worldwide Network operation or purchase. The small behaviours and the global cyberspace response levied significant legal consequences and penalties. The act soon altered the Indian Penal Code (IPC) 1860 (45 of 1860), the Bankers' Books Evidence Act 1891 (18 of 1891), the Indian Evidence Act (IEA), 1872 (1 of 1872) and the Reserve Bank of India (RBI) Act 1934. These reforms intended to provide legal recognition for transactions carried out by electronic data interchange.

The penalty for cybercrime is protected by Section 66F. This portion will be considered to have detrimental effects on vital facilities in circumstances when either of three forms of defined operations resulting in injury or death to any individual caused or significant harm to supplies,

utilities, property or disturbances that are important to a community existence is carried out. These infrastructures are defined by section 70 of this Act as secure networks. In this clause, the person who violates the requirements of the respective sections shall be punished up to 10 years and fined. Section 70B creates an "Indian Computer Emergency Response Team" for support in electronic protection accidents and other cyber-safety-related emergencies.

The IT Act requires any device to be designated as a security mechanism by the proper government, with direct or indirect consequences for the CII facility, as well as CII. When informed as a "protected system," the CII shall be granted protections against any improper disorder or access using tighter regulations. In some cases, this feature of CII considered being "protected systems." These involve the UIDAI Servers, the Terra Protected Network, and the Long-Range Detection and Tracking Device. The banking and financial processes have also been monitored. However, the broad importance of the protected structure has contributed to the goal to define regions that ought to be protected. This includes the case of governmental governments such as the government of Chhattisgarh which interpret these systems openly to include any kind of network connections and computer systems.

B. THE NATIONAL CYBER SECURITY POLICY, 2013

The cited policy expressed cyberspace as a shared resource for disparate players that are not readily distinguishable from each other, as was cyber-security. This policy determines the different ways that cyber protection can be successfully managed. These approaches include threats detection, intelligence exchange between stakeholders, survey and response planning. The key aim of this policy was to demonstrate how crucial it is to secure personal data from cybercrime and the vital infrastructure economic and socially. While this strategy acknowledged the numerous facets of cyber-security, it had not differentiated between disparate approaches to national cyber-security and the way the government plans to address these concerns. This involves failing to explain how cyber threats or cyber-terrorism need to be handled while coping with the sensitive infrastructure of data loss cyber threat. Such deficiencies involve a shortage of material interventions or goals to accomplish cyber-security

IV Evaluation of Cybercrimes against Women

Cybercrimes against women in India are a serious issue that needs to be addressed urgently. The assessment of these crimes demonstrates a number of disturbing trends and issues. The most important problem about the cybercrimes against women in India is about the lack of the awareness and education about the online safety. Some women do not even know that they are exposed while

surfing the internet; hence they are susceptible to cyber criminals. Further, there is an absence of proper policies and laws which are intended to safeguard women from online misuse and sexual harassment. Other problem is the social stigma that is attached to cybercrimes against women. Most women who are victims of these crimes do not speak up as they are afraid that society would disgrace them or they will be looked down on. The lack of media coverage makes it impossible to gather the real data on the number of women who are victims of cybercrimes being committed in India. Furthermore, sexual cybercrimes committed against women go unpunished and this worsens the situation in India. The high rate of offenders being set free without punishment signals that such conducts are accepted in the society. To deal with these problems, it is critical that women are taught about internet safety, and stricter laws and regulations should be put in place to keep them safe from cybercrimes. In addition to that, changing societal views regarding cybercrimes against women is also a need which should include support for victims and punishment for the offenders.

The instance of cybercrimes against women in India pinpoints the need for immediate measures to curb this expanding menace and protect the women online.

V Judicial Approach

The Indian judiciary, therefore, performs its vital function of making sure that the guilty is prosecuted and where the need be, judicial assistance is provided for the defenseless victims from their government.

Enforcing Laws: This tribunal has the burden of grave the cybercrimes against women but also the cybercrime law of 2000 and the Indian Penal Coding. The courts often act as a governing body to punish criminals and ensure the law is observed.

Providing Legal Redress: The judiciary creates a means for redressal of cyber wrongs by victims through a speedy fair and unbiased legal process and delivering a verdict.

Setting Precedents: Of the judges' opinion and judgments, the judicial system forms the precedents which characterize the legal principles and the ways interconnected with cybercrime. These rulings can have the impact of case precedents with regards to future cases and facilitate the implementation of a consistent legal system.

Protecting Victims: The judicial branch protects woman who have been through forms of cybercrimes, by offering them the gates of judicial process. This entails among other things,

treating the victims with a respect, guarding their confidentiality and privacies while at the same time protecting their rights to privacy during legal proceedings.

Raising Awareness: Judiciary may also add fuel to the rising of consciousness level of women by teaching them about cybercrimes against them and legal remedies' procedures. Besides the publication of more stringent and constructive judgements and rulings, the judicial branch directly gets involved in the teaching of the public about crime vices and restoration of law.

The judicial system of India performs a pivotal function of safeguarding women against cybercrimes through the enforcement of law, redressing the laws, establishing case laws, guarding the victims, and educating the masses from these problem areas Through their adequate execution of such roles, the judiciary has the ability to ensure the establishment of safer and more secure atmosphere for women in digital era.

India as a nation has witnessed remarkable incidents of women safety in Cyberspace which not only laid down guidelines and case laws but also accepted the need to be more comprehensive in this area. Following are landmark judicial pronouncements -

i. Shreya Singhal v. Union of India

In this case the section 66A of the Information Technology Act (IT), 2000 was put on the trial, which gave the right of arrest for allegedly offensive posts online. The Indian Supreme Court had declared Section 66A unconstitutional for depriving the citizens of the nation of the constitutional right to free speech and expression. This judgment has thus protected internet expression as well as disallowed the abuse of cyber laws.

ii. Vishakha v. State of Rajasthan

The case Vishakha's judgment exposed the issue of women's sexual harassment at work and the lack of criteria to prevent them. The Supreme Court took up this issue and laid down guidelines which are known as Vishakha

Guidelines or Vishakha judgment which defines sexual harassment in work sphere and set up the mechanism of prevention, redressal and accountability. These regulations in effect impacted further legislations like the Sexual Harassment of Women at Workplace (Prevention, Prohibition, and Redressal) Act, 2013.

iii. Gurmit Singh v. State of Punjab

Here, the Supreme Court faced the matter of pornographic information on the internet generally, and more specific to women. The court has stressed the importance of regulation and reduction of obscene materials that degrade women's dignity. The court has advocated for the legal procedures that aim to eradicate such content online. This case was a basis for elimination of online obscenity and cyber pornography.

iv. Indu Jain v. Union of India

The petitioner disputed the legality of the elaboration of Aadhaar information on Social Media groups taking into consideration the issue of privacy and safety, especially the women. The Supreme Court reinforced the fact that personal information and privacy rights should be guarded, with the justices pointing out the risks of sharing sensitive info over the Internet. The judgment highlighted the role of both users and platforms on the safe-guarding of data including sensitive numbers like Aadhaar.

v. Sunitha Krishnan v. State of Andhra Pradesh & Ors

Sunitha Krishnan, a social activist, brought in a petition for removal of such videos which contained depictions of assault and rape that were circulated online. The Supreme court instructed the central bureau of Investigation (CBI) to investigate the case and take action against the persons who are making such offensive content. The case brought to attention the need for harsh measures against cybercrimes involving aggressive acts towards women with sexual predators.

Such cases not only shed light on the developing Indian justice system but also reflect the issues such as online harassment, privacy violations, sexual exploitation, and unauthorized dissemination of content pertaining to women. They deserve to be acknowledged especially for the significant role they played in the development.

VI Conclusion

Cybercrime trends in India that are particularly dangerous for women call for immediate response strategies to be implemented in order to protect different online spaces and defend weak user groups. While technology continues to develop, so do the cyber criminals' tools - raising the complexity of ensuring safe and secure online environment. To tackle these problems, a multi- pronged approach that involves legal reforms, technology advancements, educational plans and societal interventions should be taken into account. Through digital literacy improvement, law framework reinforcement, technology solutions advocacy, and creation of a safe space for victims, India is able to address the rapidly growing problem of cybercrime against women. The overlap of gender-based violence and cyber victimization requires a thorough awareness of the peculiarities that are specific to gender, acknowledging that women often face more risks and vulnerabilities online. It is very important to empower women with education, advocacy and services because this is what will make them active players and safe in the digital world. In essence, the resolution of cybercrime will require more than the application of law enforcement or technological development. It includes principles of justice, security, respect, and human rights. Through collaborating across industries and communities, India can thus create a safer and more robust digital environment where all persons are free from the trauma of cyber harassment.

REFERENCES

1) Victimology: A sub-discipline of criminology, Pramod Tiwari, *available at:* http://www.dehradunlawreview.com/wp-content/uploads/2020/06/5-Victimology-A- subdiscipline-of-criminology.pdf (Visited on April 05, 2024)

2) Justice: An Exclusive Reserve for the Elite by Vibhuti Bahuguna, *available at:* http://www.dehradunlawreview.com/wp-content/uploads/2020/06/2-Justice-An- exclusivereserve-for-the-elite.pdf (Visited on March 25, 2024).

3) Women Rights vis a vis Human Rights by Puja Jaiswal, available at : http://www.dehradunlawreview.com/wp-content/uploads/2020/06/5-Women-rights- vis%C3%A0-vis-human-rights.pdf (Visited on March 26, 2024).

4) Protection of Women from Domestic Violence in India by Dr. A.K Pandey, *available at:* http://www.dehradunlawreview.com/wp-content/uploads/2020/06/1-Protection-of- womenfrom-domestic-violence-in-India.pdf (Visited on March 28, 2024).

5) Women's Human Rights- a discussion against sexual harassment, gender bias and violence by Dr. Puneet Pathak, *available at:* http://www.dehradunlawreview.com/wpcontent/uploads/2020/06/6- Women%E2%80%99s-human-rights-a-discussion-againstsexual-harassment-gender- bias-and-violence.pdf (Visited on March 30, 2024).

6) Judicial Response in the matters of Crimes against Women by Gyanendra Kumar Sharma and Pranav Vashishta, *available at:* http://www.dehradunlawreview.com/wpcontent/uploads/2020/07/3-Judicial-response-in-the-matters-of-crimes-against-women.pdf (Visited on March 31, 2024).

7) R. M. Johri, Principal Director (information Systems) Cyber Security – Indian Perspective, Office of CAG of India, *available at:* www.intosaiitaudit.org (Visited on April 02, 2024).

8) Kanika Chhabra and Gunjan Chhabra, "A Study on Emerging Issue on Cyber Law" 1

Advances in Computer Science and Information Technology (ACSIT) pp. 112-116 (2014).

9) Changing Dimensions of Cyber Crime *available at:* https://www.thehindu.com/news/national/andhra-pradesh/cyber-crimes-against-women- on-the-rise/article32399536.ece www.intosaiitaudit.org (Visited on April 02, 2024).

10) Changing Dimensions of Cyber Crime, *available at:* https://indianexpress.com/article/cities/mumbai/cyber-cells-first-conviction-man-gets-3- years-for-sending-obscene-messages stalking-colleague/ (Visited on April 04, 2024).

11) C.R.M. No. 11806 of 2017, GR/1587/2017, cited by Aditya Krishna in his article titled "Revenge Porn: Prosecution Under the Current Indian Legal System, available at *available at:*

https://actionagainstviolence.org/revenge-porn-prosecution-under-the- current-indian legal-system/?v=c86ee0d9d7ed (Visited on April 05, 2024).

12) AIR (2015) 5 SCC 1

13) (1997) 6 SCC 241

14) AIR (1996) 2 SCC 384

15) Writ Petition (Civil) No. 821 of 2020

16) AIR 2015 SC 226