ORIGINAL RESEARCH PAPER

Law

KEY WORDS: Cyber Crime, Judiciary, Legal Precedents, Information Technology, Women

COMBATING CYBER CRIME AGAINST WOMEN IN ADMINISTRATION OF JUSTICE

Dr. Suryakant C Solanki

Principal(I/C), Sheth D L Law College, Bhuj

ABSTRACT

The development of technology not only expands scientific horizons but also challenges the legal system. Computers, the internet and cyberspace are collectively known as information technology. The current challenge of the law is to interfere with information technology. These challenges are not limited to any traditional legal category but to almost all legal categories. Cyber crime can be combated by setting the legal framework, strengthening the administrative framework and punishing the accused according to a fast and effective justice system. The Supreme Court develops legal precedents through its decisions which act as guidelines. This is achieved by providing legal recourse, setting precedents, and guaranteeing the effective application of the law. By characterizing, and offering remedies for these violations, these legal precedents create consistency in the way cyber crimes against women are handled. The Supreme Court provides its authoritative interpretation of the laws that are now in effect as well as the requirements of the Constitution in order to combat online violence against women. It actively contributes to the analysis and formulation of legislative frameworks, seeking to ensure that they are comprehensive and adaptable enough to keep up with the evolving nature of cybercrime. It actively participates in the examination and creation of legal frameworks, attempting to guarantee that these frameworks are thorough and flexible enough to change as cybercrime does.

INTRODUCTION

Despite occupying a special position within society women are among the most marginalized groups. Since women's welfare was a concern shared by the drafters of the constitution granted a number of rights that are included in the list of fundamental rights. The criminal laws are in place to safeguard women's dignity as well. The crime against women is evolving together with the times. These days, crime is not just restricted to physical harm. People are disseminating pornographic material and harming women's reputations in the name of freedom of speech and expression.

Criminal activity carried out on a computer is one of the newest forms of crime against women. Cyber crime includes more specialized crimes like viruses and phishing schemes though traditional crimes can also be committed while using a computer. According to the risk of ransomware, spam and malware in the digital sphere India ranked third most vulnerable in 2017. Compared to traditional crimes, Cyber crime is completely different. Technology is causing more issues particularly for women even though it is supposed to improve society. To stop cyber crime against women in India has also passed a separate law. A successful attempt to stop cybercrime against women is made by the Information Technology Act.

Meaning

Cyber crime refers to any criminal activity using or involving a computer system or network including offenses like unlawful possession and the provision or distribution of information via a computer system. The initial stages of cyber crime began with hackers attempting to breach computer networks. While some did it only for the excitement of breaking into top-secret networks and others did it in an attempt to obtain private, sensitive information. Computer viruses were eventually introduced by thieves, causing malfunctions on both home and office computers. Since the invention of computers, the majority of crimes have included physically damaging phone and computer networks.

Computer viruses are malicious software or code that has the ability to replicate, corrupt or delete data. Cyber terrorism may apply to large-scale computer virus usage such as that which occurs with bank, government, or hospital networks. Computer hackers also commit credit card fraud and phishing schemes, such as requesting bank account details.

International Context

It was evident that illegal conduct could occur on computer systems and as consumers had access to increasingly sophisticated communications cybercrime chances increased. Investigations into cyber crimes usually take international human rights legislation into account when analyzing privacy issues. Human rights norms stipulate that legislation must be sufficiently explicit to indicate the situations under which authorities are authorized to employ investigative measures as well as that there must be appropriate and effective safeguards against misuse. Countries indicated that a variety of restrictions and safeguards on investigations together with the protection of privacy rights under national law were in place.

The Convention, which was signed in Budapest on November 23, 2001, is the first international agreement on crimes committed through the Internet and other computer networks. It specifically addresses copyright violations, fraud involving computers, the use of child pornography and offenses against network security. Its primary goal is to implement a common criminal policy that protects society from cyber crime through the adoption of suitable legislation and the promotion of global cooperation.

Indian context

Women have always been regarded as deities in India. In society, they have a special place. However, since foreign invaders arrived, India has seen an increase in crimes against women. These crimes have never stopped happening. They have only assumed a new shape and medium since they were first perpetrated in the real world. Cybercrimes including bullying, blackmail, abuse, harassment, and modesty are becoming frequent occurrences. In current age of information technology, cyber crimes that mostly impact Indian women include cyberspace harassment, cyber stalking, cyber defamation, morphing, email spoofing, hacking, cyber pornography, cybersex trafficking, cyber sexual defamation, and cyber teasing.

Although India entered the computer age, cyber crime was punished under the Indian Penal Code 1860 until the Information and Technology Act 2000 was passed. However, the Information Technology Act of 2000 was passed in order to prevent cyber crime, as the Indian Penal Code lacked the necessary authority to provide punishment for such crimes. The Information Technology Act was amended in 2008 to include new cyber crimes and to include provisions for punishment. It is still necessary to amend the Information

Technology Act in light of the current evolution of cybercrime. The complete punishment for cyber crime against women is still not available under this act. Efforts have been made to eradicate cyber crime by periodically changing the National Cyber Security Policy and the Cyber Cell in India is currently working to do the same. Now, victims who are girls can file complaints through the POCSO e-box of the National Commission for Protection of Child Rights (NCPCR). POCSO e-box is a simple and straight forward medium for reporting.

Cyber Crime Against Women

- Stalking

Cyber stalking is the practice of tracking a person's online activities by sending unsolicited emails, leaving posts on message boards the victim frequents, joining chat rooms the victim frequents, and so on.

- Bullying

Cyber bullying is the purposeful use of ICTs especially smart phones and the internet to cause distress to another person.

- Defamation

It entails posting false material about the individual on the internet or disseminating it throughout the victims' social and support networks. This is a simple way to destroy a woman's reputation by inflicting severe emotional suffering on her.

- Morphing

Morphing is the process by which an unauthorized person using a false identity downloads the victim's photos, edits them and then uploads or reloads them. Users have been detected to steal images of women from websites and then publish or re-post them by fabricating false profiles after modifying the images.

- Spoofing

It usually refers to an email that appears to have come from one source but was really sent by another. It could result in financial harm.

- Phishing:

Phishing is the effort to get private information with the goal of obtaining sensitive data, such as a login and password.

- Trolling:

Trolls are criminals who use the Internet to propagate conflict. They initiate arguments or cause distress to victims by posting offensive or controversial content in online communities, hoping to elicit an emotional or disturbing reaction from them.

- Grooming

Cyber grooming is the practice of establishing an online friendship with a young person and then coercing or tricking them into engaging in sexual activity.

- Pornography

Cyber Pornography poses a concern to female internet users. Pornographic websites and publications created with computers and the internet would fall under this category.

Legal Protection

- Article 19 and 21 of the constitution offer safeguards to women against cybercrime. Article 19(1)(a) grants women the fundamental right to freedom of speech and expression. Additionally, Article 21 ensures that women in India have the right to live in the digital realm with dignity.
- The Indian Penal Code (IPC) includes several sections that address cyber crimes against women in India. These sections encompass various offenses related to obscenity, insult to modesty, outraging modesty, and pornography. Specifically, Section 292-294 deals with obscenity, Section 509 addresses insult to modesty, and Section 354 covers outraging modesty.
- The Information Technology (IT) Act of 2000 also contains provisions to combat cyber crimes against women. Section 66A pertains to the transmission of offensive messages through communication services while Section 65 addresses tampering with computer source documents. Section 70 deals with the tampering of confidential information and Section 72 focuses on online stalking. Furthermore, Section 42A and Section 66 are applicable in cases of data hacking. Data theft is covered by Section 43B, 66E, and 67C, while Section 67A specifically targets pornography-related offenses.
- The Protection of Children from Sexual Offences (POCSO) Act of 2012 provides legal safeguards for girl children. It includes provisions such as Section 3 for penetrative sexual assault, Section 5 for aggravated penetrative sexual assault, Section 7 for sexual assault, Section 9 for aggravated sexual assault, Section 11 for sexual harassment of a child, and Section 13 for the use of a child for pornographic purposes.

The Indian Constitution ensures that women have equal rights to life, human dignity, and freedom of speech and expression. However, it appears that the Information Technology Act of 2000 does not adequately protect the modesty of women in general. Unlike the Indian Penal Code, the Constitution of India, and the Code of Criminal Procedure, the IT Act does not contain specific provisions to address crimes against women. Similarly, the Protection of Children from Sexual Offences Act of 2012 is also not fully equipped to prevent cyber crimes against young girls.

Role of judiciary

The Indian judiciary plays a crucial role in combating cyber crimes committed against women and children specifically by issuing important judicial decisions and guidelines that have not only shaped the legal framework but also protected the rights and well-being of the victims. Within this context, the Indian courts have actively dealt with numerous instances of cyber stalking which involves the continuous and unwelcome online harassment or stalking of an individual.

- Mrs. X v. Union of India and ors. (2023)

In the case of the High Court of Delhi played a crucial role in addressing cyber crime against women and children. The court took a proactive approach by ordering the removal of unlawfully published content from a pornographic website and directing search engines to de-index the content from their search results.

- Ritesh Sinha v. State of Uttar Pradesh (2019)

Another significant case is which shed light on the issue of sextortion where the accused had obtained explicit photographs of the victim and resorted to blackmail. The Allahabad High Court recognized that such actions violate an individual's right to privacy and respect. Consequently, the court held the defendant accountable for various charges including extortion and criminal coercion.

- State of Kerala v. Rahul Pasupalan and Another (2019)

The case of revolves around a sextortion incident in which the accused unlawfully disseminated explicit videos of a woman without her consent. The Kerala High Court recognized the seriousness of the offense and held the accused accountable under various sections of the Indian Penal Code, including voyeurism and defamation.

- Sabu Mathew George v. Union of India (2018)

In the case of the focus was on online advertisements that were promoting sex determination tests and female foeticide. The Supreme Court took action by directing the government to implement measures for regulating and monitoring these advertisements. Additionally, the court emphasized the importance of strict enforcement of the Pre-conception and Pre-natal Diagnostic Techniques in order to prevent any form

of gender-based discrimination.

- Shafhi Mohammad v. State of Himachal Pradesh (2018),

In the case of the focus was on the issue of privacy and the admissibility of electronic evidence particularly sexually explicit videos. The Supreme Court thoroughly examined this matter and emphasized the importance of safeguarding privacy rights and stated that any unauthorized intrusion into an individual's personal space including the unauthorized sharing of explicit material is a violation of privacy.

- Prajwala v. Union of India viii(2015)

The focal point of the case revolves around the issue of child pornography and the distribution of explicit content via the internet. The Supreme Court has instructed the government to work alongside internet service providers and social media platforms to enforce effective measures that will obstruct, eliminate, and deter the spread of such material using diverse technological methods.

- State Vs Jayanta Dasxvi(2017)

In the case of the defendant was a first-time offender who was found guilty by the court. It is crucial to recognize that the severity of criminal intent should not be underestimated. The defendant committed an act that displayed a disturbingly frequent occurrence of reckless behavior. Additionally, the court emphasized the importance of addressing the issue of women's vulnerability and safety, highlighting its significance within the scope of criminal law.

CONCLUSION

In the context of India, there has been a rapid increase in the number of cyber crimes against women, with new forms of crimes such as cyber trolling and cyber bullying emerging. However, the existing IT Act of 2000 does not encompass these specific crimes and the investigation process is inadequate. This lack of legal provisions to address cyber trolling and gender bullying is a significant flaw in the current legislation. Recognizing the importance of protecting the dignity and reputation of women in online spaces, the Supreme Court has consistently emphasized the need for safeguarding women's rights. The court acknowledges that cyber offenses including revenge pornography, cyber bullying, and internet defamation can have a profound impact on a woman's mental health and reputation. Given the dynamic and adaptive nature of cyber crime, it is crucial to adopt a continuously evolving approach to combat these offenses. This requires sustained efforts to raise awareness, enhance skills, and promote cooperation among various stakeholders, including the judiciary, law enforcement agencies, government institutions, and non-governmental organizations.

REFERENCES

1. The Constitution of India
2. Indian Penal Code, 1860
3. Information Technology Act
4. POCSO Act, 2012
5. Pandey Jai Narayan, Indian Constitution, Central Law Agency, Forty-Three Edition, 2010.
6. Duggal Pawan, Cyber Law, Lexis Nexis Publication
7. Tiwari Garima, Understanding Laws Cyber Laws & Cyber Crimes(Lexis Nexis Publication) 2014
8. Halder Debarati, Jaishanker,H; Cyber Crimes Against Women In India
9. https://www.thedailystar.net/law-our-rights/law-vision/urge-ratify-the-convention-cybercrime-1382548
10. https://www.floridatechonline.com/blog/cybersecurity/the-rising-cost-of-cyber-crime/
11. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf 12.https://www.google.com/amp/s/www.vskills.in/certification/tutorial/cyber-crimes-2/%3famp
13. https://i-probono.com/case-study/cybercrimes-against-children/
14. https://vikaspedia.in/social-welfare/women-and-child-development/women
15. http://www.indiaspend.com/cover-story/crime-against-women-up-83-conviction-rate-hits-decadal-low-18239
16. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
17. https://study.com/academy/lesson/what-is-cybercrime-definition-history-types-laws.html