Research Article

Maharaja Surajmal Institute Law Journal

Year 2024, Volume-1, Issue-1 (January - June)

www.acspublisher.com

A Critical Analysis of Types and Techniques of Cybercrime against Women: Laws and Judicial Expositions from Indian Perspective

Rakesh Kr. Handa[1] and Mohd. Rizwan Ansari[2]

[1]Assistant Professor, University School of Law & Legal Studies, Guru Gobind Singh Indraprastha University, Delhi.
[2]Research Scholar, University School of Law & Legal Studies, Guru Gobind Singh Indraprastha University, Delhi.

ARTICLE INFO

Key Words: Cybercrimes, Cyberspace, Cyber-stalking, Cyber-morphing, e-mail spoofing; Cybercrimes against Women.

doi: 10.48165/msilj.2024.1.1.5

ABSTRACT

The current century is the era of science and technology. Over the past few years, there have been numerous mechanical advancements. The development of information technology gave rise to the cyberspace, where internet connectivity allows users to access information and store data, among other things. The common man now has access to the internet, which is improving their quality of life. The most recent trend in information and communication technologies is similar to the fact that no coin has only one side. Cybercrimes were created when some individuals with criminal mindsets began using the internet for their illicit activities. Cybercrime and the exploitation of women are both continuously rising due to new technology. This article focusses on the new challenges surrounding cybercrimes against women in India and the factors contributing to their rise. In this article, suggestions have been provided by the authors which are helpful in combating cybercrimes.

INTRODUCTION

Women continue to experience various forms of harassment today, as they did for many generations. Every year on 8th March, we celebrate the World Women's Day to show our appreciation for women for their contributions to society in various ways. In India, women are worshipped as goddesses, but the reality paints a depressing and worsening picture of this. The reality is that women are only worshipped in spiritual settings during religious ceremonies and festivals. However, in everyday life, they are subjected to many forms of oppression and have frequently been the targets of physical, psychological, and sexual abuse.

We are living in the age of information technology and internet. The discovery of computer has been a blessing to the students, teachers, scholars, lawyers, business tycoons, doctors and many other professionals. People use the internet because it allows them to successfully gather and share data with others, regardless of their location in the world. People frequently use the internet at their homes, offices, educational institutions, and other

*Corresponding author.
E-mail address: XXXXXXXX (XXXXXXXX)

Received 15.03.2024; Accepted 10.05.2024

places. As a result, it has introduced us to a new world where we may express our ideas and culture's values.

Every coin has two sides good as well as bad. Similarly, any mechanical advancement is suitable for both constructive uses and destructive ones. The advancements of information technology not only enlarge our prospect but cause a few fresh challenges too to legal framework. When the internet was first created, it's bad behavior was not considered by its creators. However, the criminal attitude of human brain science began to be misused by using the internet as a tool for crime, giving rise to cybercrime, and the world now faces a significant threat from such cybercriminals. With development of technological advances, cybercrime and the exploitation of women are growing and posing a serious hazard. It is estimated that 75% of cybercrimes target women, adolescents, and children. Bollywood actress Celina Jaitley filed a complaint with the Mumbai Police against two websites, one of which was external, alleging that her images had been altered and transferred to advance undergarments items. However, unless they start to consider reality, most women are unaware of these wrongdoings; by the time they do, it is already too late.

Cyber Crimes

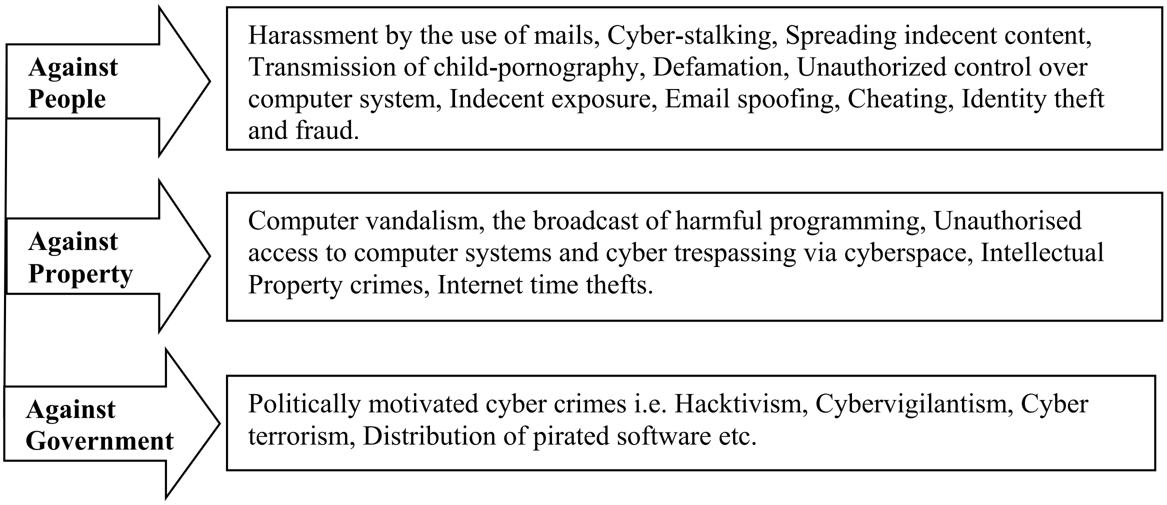
Cybercrimes don't have an exhaustive definition. Understanding computer crime and how it evolved into cybercrime is necessary to comprehend it. Cybercrime is criminal activity that takes place online. Computers are used both as tools and as targets in cybercrime. Cybercrime is a broad phrase that includes actions committed or encouraged by the use of technological advancement in computers. Cybercrime has not been statutorily defined in any statutes with regard to its precise definition. The U.N. Congress on Prevention of Cyber Crime and Treatment of Offenders defined cybercrime as falling into the following two groups:

1. Cyber crimes, when used narrowly, connotes a computer crime and incorporates any illicit activity directed through use of electronic operations that compromises security of computer systems and the data they process.
2. In wider terms, cybercrimes encompass all computer-related offenses and include any illegal activity carried out in connection with or through the use of a computer system or network, involving offenses like illegal possession and the offering or distribution of information via a computer system or network.

The definition of cybercrime is not even mentioned in the Information Technology Act, 2000. However, Cybercrime is a voluntary and intentional act or omission that causes harm to a person, their property, or their computer systems and is punished under the Information Technology Act of 2000 or the Indian Penal Code. Cybercrime is an umbrella term used to encompass any offences committed on or through the use of the internet. A cybercrime is defined as an offense that makes use of a computer, either as a tool, a target, or a means of carrying out more wrongdoing.

Categories of Cybercrimes

Cybercrimes can be divided into three groups; crimes committed against people, property, and governments.



Against People

Harassment by the use of mails, Cyber-stalking, Spreading indecent content, Transmission of child-pornography, Defamation, Unauthorized control over computer system, Indecent exposure, Email spoofing, Cheating, Identity theft and fraud.

Against Property

Computer vandalism, the broadcast of harmful programming, Unauthorised access to computer systems and cyber trespassing via cyberspace, Intellectual Property crimes, Internet time thefts.

Against Government

Politically motivated cyber crimes i.e. Hacktivism, Cybervigilantism, Cyber terrorism, Distribution of pirated software etc.

Cybercrimes against persons and cybercrimes resulting in harm to property[1]

These cybercrimes are generally classified as:

1. Cyber Stalking: Use of cyberspace to terrorise, control, or threaten a target so that they dread danger or death, either to themselves or to those near to them.
2. Cyber Pornography: Possession, creation, importation, display, publication, or distribution of pornography especially child porn or other offensive items via the internet.

Cybercrimes against property or resulting in harm to property[2]

These cybercrimes, which typically use cracking techniques, include popular varieties like:

1. Flooding: A type of online vandalism that denies access to authorised users of a website or system
2. The creation and distribution of viruses and worms: This is a sort of cybervandalism that damages data and may even erase it.
3. Spoofing: When non-authentic individuals assume the identity of a legitimate user online, it may result in actual or attempted fraud, critical infrastructure failures, or both.
4. Phreaking: It is a type of online fraud or theft that involves leveraging technology to place free phone calls.
5. Violation of intellectual property rights and copyright: This type of cybercrime is the unauthorised copying of a target's data or software.

Cybercrimes against Government or Technical Non-offences[3]

In the field of cybercrime, there are a number of politically driven, contentious, and technical non-offenses:

1. Hacktivism: Hacktivists who combine their hacking prowess with their interests in activism to further their causes.
2. Cybervigilantism: The fusion of vigilantism with cyberspace.
3. Cyberterrorism: The convergence of cyberspace and terrorism. It refers to unauthorized attacks next to computers, networks and data amassed within when prepared to terrorize or intimidate a government or its citizens for the advancement of political or societal objectives.

Cyber Crimes Against women

Cybercrime against women is any sort of sexual or gender-based violence that takes place online or on a computer.[4] The following are examples of cybercrimes that target women in particular: -

1. Cyber Morphing Against Women

Editing the original image to make it appear significantly or completely different is known as morphing. Cyber morphing occurs when an unauthorized user using a phony ID, downloads the victim's images and edits them, then reloads them. It has been experiential that womanly images are acquired from websites using forged IDs and then uploaded another time using fake accounts after being altered. If such morphed image is transmitted it may also amount to punishing and transmitting obscene images and such actions are punishable under the I.T. Act, 2000 under Section 67, 67A. The offender can also be booked under IPC section 509.

An important case involving morphing occurred in the *Air Force Balbharati School case (Delhi),*[5] when a student was mocked by class fellows for having a spotty face. He made decision to revenge himself and scanned images of class fellows, merged with naked pictures and uploaded online. When the father of a class fellow; who was featured online learned regarding it, he complained. The I.T. Act of 2000's sections 43 and 66 provide for the punishment of such acts. Such offenders may also be booked under IPC Section 509.

2. Cyber Pornography Against Women

The word pornography, derived from the Greek words 'porni+ grapein' in which 'porni' refers to 'prostitute' and 'graphein' refers to 'documentary'. Pornography accurately means 'Documenting a Prostitute' or 'Depiction of acts of Prostitutes'.[6] When obscene material is published, transmitted, or made to be published electronically, it is referred to as cyberpornography.[7] Cyber pornography is generally defined as online

[1] Bernadette H. Schell and Clemens Martin, "*Cybercrime*" 30 (ABC-CLIO Inc., California, 2004)

[2] *Ibid*

[3] *Ibid*

[4] Ramandeep Kaur, "Cyber Crime Against Women- Present Scenario" available at https://www.academia.edu/31755698/CYBER_CRIME_AGAINST_WOMEN-PRESENT_SCENARIO (accessed on 26 March, 2023)

[5] Abhimanyu Behera, " Cyber Crimes and Law In India," 31 *IJCC* 19 (2010)

[6] Garima Goswami & Dr. Ghulam Yazdani, "Combating Cyber Crimes Against Women: Need For Effective Laws" 45 (3) *Indian Bar Review* 166 (2018)

[7] C. Coteanu, *"Cyber Consumer Law and Unfair Trading Practices"* (Kluwer Law International, 2010)

material that encourages erotic or sexual behaviour.[8] It is written or illustrated material that supports degrading or harsh sexual behaviour against at least one member by referring to it or showing it. Photos of female people are collected from their personal collections and altered for obscene purposes by using selected images. An incredibly well-known example of this is the *DPS MMS Scandal,*[9] in which an MMS attachment showing a schoolgirl in an inappropriate situation was created and distributed across several websites.

3. Cyber Stalking Against Women

One of the most frequently talked-about online crimes worldwide is cyber stalking. It entails tracking a person's whereabouts while routinely sending emails to the victim and posting statements (often threatening ones) on discussion boards. Females are the primary victims of this kind of crime. It has been noted that 75 percent of the victims are women. Sexual harassment, a preoccupation with love, retaliation, and hatred, as well as ego and power trips, are the typical motivations for cyberstalking.[10] Sites, conversation groups, visit rooms, emails, texts, and other platforms are utilized to target women. A significant case of a woman's online privacy being violated is cyber stalking.[11]

Ritu Kohli's case is the first instance of cyberstalking in the country, according to Pawan Duggal, an expert in cyber law. Ritu Kohli began receiving texts and emails from a mysterious source, which she ignored. Stalker posted her phone number and personal details online and used vulgar and dirty language. She consequently started receiving a variety of repulsive calls. She reported the incident to the police, who tracked the offender's IP address. The Delhi police detained the Cyber stalker, who was booked under section 509 of the Indian Penal Code and the Information Technology Act of 2000.[12]

4. Cyber Bullying and Trolling against Women

Trolling and Bulling are under researched issues in the arena of cyber crimes. In India, these two in the computer mediated communication system targeting women are particularly important because of patriarchal social mindset, and susceptibility of women to be attacked in the physical space due to gender Bullying or Trolling on the internet.[13]

Cyber-bullying is the act of bothering, undermining, or threatening someone while using a phone, texting, email, chat room, or social networking site like Facebook, Instagram, or Twitter. Cyber-bullying refers to the use of internet communication to threaten an individual, frequently through sending messages with a threatening or defamatory tone.

5. Cyber Defamation Against Women

Another frequent abuse regarding women in online realm is cyber defamation, which includes libel and slander. It takes place when somebody publishes derogatory information online regarding somebody or sends messages or mails to anyone that contains defamatory information. Despite the fact that both men and women can experience this, females are more vulnerable.

SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra-Jogesh Kwatra,[14] was the nation's first case of cyberdefamation. An employee of the defendant company started sending vulgar and defamatory emails to the managing director of the company. To harm the company's reputation, the emails were sent to a sizable number of their business partners. The Delhi High Court was requested by the plaintiff. The worker was prohibited by a replacement order from sending, disseminating, and transmitting messages that are defamatory or harmful to the people who were offended.

6. Harassment of Women Through E-mails

Cyber harassment is a pattern of behaviour used repeatedly with the intention of upsetting or upsetting a person online. Online abuse of a person involves using email, social networking sites, instant messaging, and other channels.[15] Fundamentally, email

[8] V.K. Jaswal & S.T. Jaswal, *"Cyber Crime & Information Technology Act, 2000"* p.21 (Regal Publications, New Delhi, 2014.

[9] http://en.wikipedia.org/wiki/DPS_MMS_Scandal (accessed on 31 March, 2023)

[10] Dr. Asmita A. Vaidya, "Cyber Crimes Against Women" 2(6) *Criminal Law Journal* 161 (June, 2012)

[11] Dr. S.K. Mohapatra, "Victimisation of Women Under Cyberspace in India Environment" 2 (3)(1) *International Journal of Academic Research*, 221 (Jul-Sep, 2015)

[12] Archna Sharma, "Cyber Stalking and Plight of Women in India- A Legal Perspective" 1 *RMLNLU* 183 (2017)

[13] Halder Debarati and K. Jaishankar, "*Cyber Crimes Against Women in India*" 45 (Sage Publications Private Limited, New Delhi, 2017)

[14] https://indiankanoon.org/doc/31110930/ (accessed on 21 March, 2023)

[15] Eesha Shrotriya & Iti Prajapati, "Devising A Legal Mechanism For Redressal Of Online Abuse And Harassment With Special Reference To Information Technology Act, 2000" 4 *KSLU-SLR* 5 (2017)

harassment is the same as letter-based harassment. Following the 2008 amendment to the IT Act, new provisions are now included as sections 67-A to 67-C. Sections 67-A and 67-B contain criminal penalties for the offences of distributing or transmitting child pornographic or sexually explicit material, and Section 67-C establishes an intermediary's obligation to hold and protect data for the duration and in the manner specified by the central government. Despite the fact that these provisions make no mention of email harassment, they are still used to charge offenders under IPC sections, 354, 509 and 292-A for insulting a woman's modesty and printing or distributing pornographic material with the intent to extort or blackmail.

7. Cyber Hacking Against Women

Hacking is declared a crime as per section 66 of the IT Act of 2000, only when it is done dishonestly and fraudulently.[16] Hacking itself is not an offence under Section 66; instead, the *mens rea* requirement applies.[17] The term 'hacking' is used to describe a wide range of human activities that obstruct the smooth operation of computer networks and systems. However, due to its vagueness, the term 'hacking' is not used in the majority of legal systems. Computer espionage, computer trespassing with the intent to obtain data or to obstruct the intended use of a computer, damaging a protected computer using a variety of tools, such as malware, or trafficking in passwords and other hacking tools are just a few of the criminal offences related to hacking that are defined by the U.S. Computer Fraud and Abuse Act.[18]

Once they get access to the computers that run networks, hackers can change information, destroy files, and create evidence of their actions.[19] The 'White Hat' subgenre of hacking is characterized by inventive cyber-world exploits driven by the hacker's desire for knowledge. White Hats frequently break into systems by permission to look for security holes in the network that could allow unauthorized cyber hackers' access. The dark side of hacking, also referred to as Black Hat or cyber crime, includes malicious computer exploits that are driven by the invader's desire for vengeance, sabotage, extortion, or purely for their own benefit. Black Hat exploits, like conventional crimes, can result in damage to people or property.

8. Email Spoofing Against Women

Spoofing is a common tactic used by crackers to try and manufacture false data like phony bank statement. Email spoofing is practice of sending email that looks to have come from one source but was actually sent from another.[20] E-mail 'spoofing' refers to a false mail movement in which sender's info and other elements of mail heading are misrepresented so as it seems as though the email came from another source. The email's characteristics, like From, Return-Path, and Reply-To fields, complete it. Cybercriminals regularly utilize this technique to take personal info and photos from unwary females, then exploit those details to extort those women. The ***Gujrat Ambuja's Executive Case,***[21] is the best example of email spoofing. The person responsible in this instance for defrauding and extorting the NRI with a base in Abu Dhabi pretended to be a young woman.

Factors of the Growth of Cybercrime against Women

The legal and sociological factors that have contributed to expansion of cybercrime regarding women can be separated into two categories:
1. Legal factors
2. Sociological factors

1. Legal Factors

Cybercriminals profit from the absence of clear and stringent laws safeguarding women. There is I.T. Act, 2000 which deals cybercrimes but there is lack of specific provisions for some specific crimes committed in cyber world.

i. Information Technology Act, 2000

The Information Technology Act, 2000's purpose is very evident even before it is introduced. It was created primarily to promote internet commerce; as a result, it addresses financial and commercial crimes including hacking and breach of confidentiality. Nowadays, it is popular for people to engage in cyber-bullying, email spoofing, cybersex, hacking, and invasions of

[16] R.K. Chaubey, *"An Introduction to Cyber Crime and Cyber Law"* p. 45 (2009)

[17] H. Chander, *"Cyber Laws and IT Protection"* p.76 (2012)

[18] Sandeep Kumar Sharma, "An Overview of Cyber Crimes Vs. Cyber Law- Indian and International Perspective" 1 *VITSTA Law Journal* 25 (2017)

[19] Prof. Gurjeet Singh, "Emergence of Cyber Crime: A Challenge for The New Millennium" 29 *Indian Socio-Legal Journal* 20 (2013)

[20] Amogh Prabhu Dessai, "Cyber Crime in India" 4 *The Bangalore Law Journa*l 511 (2013)

[21] G. Rathinasabapathy and L. Rajendran, " Cyber Crimes and Information Frauds: Emerging Challenges For LIS Professionals" *Conference on Recent Advances in Science & Technology* (2007)

privacy, yet the Information Technology Act, 2000 does not specifically address any of these things under any Provision. The majority of cybercrimes are dealt with in accordance with Sections 66 (hacking), 67 (publishing or transmitting obscene material in electronic form), and Section 72 (breach of privacy).

ii. **Indian Penal Code, 1860**

There are no explicit sanctions under Indian Penal Code, 1860 protecting women in particular from online offences. However, the Indian Penal Code, 1860, provides special protection for women, such as by outlawing forced marriage, abortion, kidnapping, and other offences against women's modesty, among other things. Sections 354, 354-A, 354-B, 354-C, and 354-D of the Criminal Law Amendment Act of 2013 added to the IPC and allowed for the legal management of MMS outrages, pornography, morphing, defamation, and other related issues.

2. **Sociological Factors**

Due to the victim's trepidation and shyness, the majority of cybercrimes go unreported. A woman frequently believes that she is to blame for any wrongdoing committed against her. The risk of cybercrime is substantially greater for women because the perpetrator's identity is unknown, and he can continue to extort and terrorize the victim using several names and online personas. Regardless of whether it occurs in real life or online, victims of sexual harassment still don't report it to the police because they are afraid it will interfere with their family life.

Some Safety Measures for Victims

Here are some suggestions on how women can protect themselves from online offences:

1. If you are keeping private info on your computer, you ought to be conscious of every demand for personal info. Never divulge any such details.
2. Treating your email address as crucial private information, similar to a mobile number or address, and only sharing it with those you recognize and believe online; are significant safety precautions.
3. While using public computers, you must erase your surfing history. Your history may be saved by web browsers. When using the internet, women should be wary because stalkers could try to con them.
4. We must verify our mail, blog or online accounts frequently. As a result, we shall be in touch with our online belonging accounts.
5. Online service providers and social networks all have privacy settings and protection measures. To protect oneself, one must make an effort to comprehend security strategies and use security measures.
6. In order to reduce the possibility that a Trojan virus, email virus, etc. will be attached to one's computer, one needs to confirm that anti-virus software is current and functioning properly. Firewalls serve as the first line of defense against hackers and viruses by blocking connections to erroneous destinations.
7. Changing passwords is a fantastic way to secure social networks and personal data. The majority of strong passwords include letters, numbers, and graphics.
8. Women should avoid receiving unwanted calls, texts, and emails. Women must record harasser calls and report them to the police if it occurs repeatedly.
9. Avoid revealing private residences. Business address may be used instead of it.
10. It is important to start an awareness campaign about cybercrimes in places like schools and universities, where women can be empowered and made to feel at ease. To advisory foundations, corporate workplaces, awareness campaigns, courses, and workshops on cybercrimes, lawyers, law trainers, social workers, police, and NGOs ought to be welcomed.

CONCLUSION

Similar to everywhere else in the globe, cybercrime against women is on the rise in India. The more we rely on technology to aid us and manage our lives, the more opportunities there are for wrongdoing. The regular style of doing things and the persistent nature of the cybercriminal are the primary problems with cybercrime. The IT Act, 2000 was passed by India, one of the few nations, to tackle cybercrime. Although it is clear from the Act's introduction that this Act broadly protects against business and financial wrongdoings, it is apparent that there is lack of definite system in place to assure the safety of women. There are, however, some procedures to cover a portion of the Act's infractions against women who use the internet. However, they are insufficient to address the problem. Adoption of rigorous legislation is required. To quickly identify the offender, the police, the judiciary, and investigative agencies must be updated regarding online application developments.[22] The legal system has an accountability to keep up with hi-tech progressions and ensure that new developments don't turn into tools for harassment and abuse.

[22] Dr. Farooq Ahmad, "*Cyber Law in India (Law on Internet)*" p.5 (New Era Law Publications, Haryana, 2011, Reprint 2015)

As a result, harsh criminal penalties as well as changes to educational framework; are crucial to combat cyber-crimes regarding women in India. To bring about such reforms, people, the government, social workers, NGOs, etc. must work together. People need to modify the way they think about women, and they need to foster a sense of community. Victimization of women online also reflects their status, dignity, and the way society views them in the real world. Because of the patriarchal syndromes that exist in our society, women are still victimized in both the online and offline worlds.[23]

The nation that doesn't respect women will never become great today or in the future, according to Swami Vivekananda. Let's fight to give women the prominence they deserve in order to make India a great nation.

[23] Sarmistha Neog, "Criminal Activities Agains Women in Cyberspace: An Analysis in Indian Context" 1 *GULJ* 138