IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, February 2025

Sexual Offences Cyber Space and Internet

Shri. Gani Manik Nadaf
Research Student, Bharati Vidyapeeth, Deemed University, Pune, Maharashtra, India
ganinadaf@gmail.com

Abstract: *The internet is most important platform for the daily life. One cannot stay away from the internet. It becomes most essential thing for various purposes of the man. The internet has revolutionized the way we communicate, interact and access information. In various fields like Government offices, Banks, School colleges, commercial purpose the internet is used as basic need for all. However, it has also created new opportunities for hackers and for sexual offenders to commit crimes. Cyber crime including sexual offences has become the significant concern globally. The internet can be both a blessing and a curse, depending upon how it is used. The internet can be used for good or evil, and it can have both positive and negative effects. Shopping, learning, employment etc. are the benefits of internet whereas social media, temptation, instance gratification are the negative effects of the internet. Day by day the offences relating to women are increasing due to more use of social media. The people may use the internet for the good purposes. So that it will become beneficial for the wellfare of the society. The people can also use the internet via social media due to which the offences cannot be done by them and the wrong doors could not take the undue advantage of the internet.*

Keywords: internet

I. INTRODUCTION

Cyber Crimes are crimes that happen over the web where the perpetrator of the crime, shielded by the veil of a computer screen need not establish physical contact with the victim or may not always revealed their identity. Cyber Crime is Combination of Crime and Computer Resource. Cyber crimes are committed while in the cyber space. Categories of Cybercrimes are as crimes where a computer is the target of the crime, crimes where a computer is a tool of the crime, and crimes where a computer is incidental to the commission of the crime. They include crime like, cyber terrorism, intellectual property infringement, hacking, industrial espionage, on-line child exploitation, internet usage policy abuses, illegal purchase of goods, sexual assault, internet fraud, software piracy, viruses, impersonation and many more Crimes over the internet could be in the nature of

- Cyber stalking
- Cyber bullying
- Cyber harassment
- Identity theft
- Breach and violation of privacy/confidentiality
- Voyeurism
- Revenge pornography, though falling within the ambit of cyber harassment, is one such cyber crime which has seen a lot of discussion of late owing to increased instances of non-consensual pornography

Legal Provisions Under Various Laws

Although a comprehensive regulatory framework with regard to laws governing the cyber space, particularly such acts is yet to be framed, there exists certain legal provisions under various Statutes which can come in aid of a person who is a victim of cyber violence.

1. The Indian Penal Code, 1860

Prior to 2013, no law directly dealing with online harassment or crimes pertaining to women in the cyber space. The 2013 Criminal Amendment Act to the Indian Penal Code, 1860 by way of Section 354A to Section 354D

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, February 2025

1. Section 354A: A man committing any of the following acts – a demand or request for sexual favours; or showing pornography against the will of a woman; or making sexually coloured remarks, shall be guilty of the offence of sexual harassment, may be punished with rigorous imprisonment for a term which may extend to three years, or with fine, or with both. In case of the first two and with imprisonment of either description for a term which may extend to one year, or with fine, or with both.

2. Section 354C defines 'Voyeurism' as including the act of capturing the image of a woman engaging in a private act, and/or disseminating said image, without her consent. For the act to qualify as 'Voyeurism', the circumstances must be such where the woman would "usually have the expectation of not being observed either by the perpetrator or by any other person at the behest of the perpetrator". A person convicted under this section is liable to be punished with fine as well as imprisonment up to three years on first conviction and seven years on subsequent convictions.

3. Section 354D introduced a provision for stalking which also covers cyber stalking.

Stalking has been defined to mean an act where a man follows or contacts a woman, despite clear indication of disinterest to such contact by the woman, or monitors the cyber activity or use of the Internet or electronic communication of a woman. A man committing the offence of stalking would be liable for imprisonment up to three years for the first offence, and shall also be liable to fine and for any subsequent conviction would be liable for imprisonment up to five years and with fine.

Other than the specific amendments that have been made to the Code, there exist certain other provisions under which cyber crimes may be reported or the accused may be charged. These are:-

1. Section 499: To defame a person is to do an act with the intention of harming the reputation of the person. Defamation by publication of visible representations of an imputation concerning the woman, when done with the intention to harm her reputation, is punishable with imprisonment for a term, which may extend to two years, or with fine, or both.

2. Section 503: Threats made to any person with injury to her reputation, either in order to cause alarm to her, or to make her change her course of action regarding anything she would otherwise do/not do is punishable as criminal intimidation. The act of blackmailing a person on the internet, as was done in the case mentioned above can be brought within the ambit of this provision.

3. Section 507: This provision provides the quantum of punishment for Criminal Intimidation when the same is by a person whose identity is not known to the victim. Any anonymous communication, which amounts to criminal intimidation under Section 503 stated above, is punishable under this section.

4. Section 509: Any person who utters any word or makes any sound or gesture, or exhibits any object with the intention that such word, sound or gesture or object be heard or seen by a woman and insult her modesty, or intrudes a privacy, may be charged under this section and imprisoned for a term that may extend to 3 years and also with fine. Instances of lewd comments or remarks made over the Internet, or other explicit images and content forcibly shared over the web may be penalized under this section.

2. The Information Technology Act, 2000 as amended by the Information Technology Act, 2008

1. Section 66C of the IT Act makes identity theft a punishable offence. Instances of cyber hacking would be covered by this provision. Under this provision, whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, 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 rupees one lakh.

2. Section 66E of the IT Act deals with the violation of the privacy of a person. Capturing, publishing or transmitting the image of a private area of any person without her consent, under circumstances violating her privacy, is punishable with imprisonment, which may extend to three years, and/or fine.

3. Section 67 prohibits, and punishes with imprisonment extending up to three years and fine for first conviction and to five years and fine upon second conviction, the publication, transmission and causing of transmission of obscene content. Obscene content has been defined in the same manner as in Section 292 of IPC, and therefore the test of obscenity is to be the same as under that provision

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, February 2025

4. Section 67A makes the publication, transmission or causing of transmission of sexually explicit material punishable with imprisonment extending up to five years and fine for first conviction and to seven years and fine upon second conviction.
5. Section 67B makes publication/transmission of sexually explicit content depicting children punishable.

3. Indecent Representation Of Women (Prohibition) Bill, 2012
The Indecent Representation of Women (Prohibition) Act regulates and prohibits the indecent representation of women through the media of advertisements, publications etc. The Indecent Representation of Women (Prohibition) Amendment Bill, 2012 seeks to broaden the scope of the law to cover the audio-visual media and content in electronic form, and distribution of material will also include distribution on the Internet and the portrayal of women over the web.

Various types of Crimes at a glance

A) Internet crime using the Internet infrastructure-
(i) Hacking
(ii) Theft of information/passwords
(iii) Theft of credit card numbers
(iv) Launch of malicious programs
(v) Espionage
(vi)Spamming Web based crimes-

B) Website related crimes-
(i) Cheating and frauds
(ii) Insurance frauds
(iii) Gambling
(iv) Distribution of pornography
(v) Sale of pirated software

C) Crime through E-mail
(i) Threats
(ii) Extortion
(Iii) defamation
(iv) Launching of malicious software

D) Use net related crimes-
(i) Discussion on methods of hacking
(ii) Sale of stolen credit card numbers
(iii) Sale of stolen data

E) Internet related chat crimes
(i) Cyber stalking
(ii) Fraudsters use chat rooms for developing relations with unsuspecting victims
(iii) Criminals use it for meeting conspirators
(iv) Hackers use it for discussing their expertise of showing the techniques
(v) Podophiles use chat rooms to allure small children

Preventing Cybercrimes: A Collective Responsibility
The rapid growth of the internet and technology has transformed the way we live, work, and communicate. However, this increased connectivity has also led to a rise in cybercrimes, which can have devastating consequences for individuals, businesses, and societies. Preventing cybercrimes requires a collective effort from governments,

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, February 2025

organizations, and individuals. In this essay, we will explore the ways to prevent cybercrimes and promote a safer online environment.

Individual Precautions

Individuals can take several precautions to prevent cybercrimes

1. Use strong passwords: Use unique and complex passwords for all online accounts.
2. Keep software up-to-date: Regularly update operating systems, browsers, and other software to ensure you have the latest security patches.
3. Be cautious with emails and attachments: Avoid opening suspicious emails and attachments, and never click on links from unknown sources.
4. Use antivirus software: Install reputable antivirus software to protect against malware and other online threats.
5. Use two-factor authentication: Enable two-factor authentication whenever possible to add an extra layer of security.

Organizational Measures

Organizations can also take several measures to prevent cybercrimes:

1. Implement robust security policies: Develop and enforce comprehensive security policies to protect against cyber threats.
2. Conduct regular security audits: Regularly audit systems and networks to identify vulnerabilities and address them before they can be exploited.
3. Provide employee training: Educate employees on cybersecurity best practices and the importance of online safety.
4. Use encryption: Use encryption to protect sensitive data, both in transit and at rest.
5. Have an incident response plan: Develop a plan to respond quickly and effectively in the event of a cyber attack.

Government Initiatives

Governments can also play a crucial role in preventing cybercrimes:

1. Establish cybersecurity laws and regulations: Develop and enforce laws and regulations to prevent and prosecute cybercrimes.
2. Provide public awareness campaigns: Launch public awareness campaigns to educate citizens on cybersecurity best practices and the importance of online safety.
3. Support cybersecurity research and development: Fund research and development initiatives to improve cybersecurity technologies and techniques.
4. Collaborate with international partners: Collaborate with international partners to share intelligence and best practices in preventing cybercrimes.
5. Establish incident response teams: Establish teams to respond quickly and effectively in the event of a cyber attack.

II. CONCLUSION

Information and communication technology (ICT) systems are now essential for our lives as is water and electricity. Many individuals, corporate bodies and government entities rely on ICTs and computer networks to perform simple and complex tasks. However, cyberspace is becoming unsafe as many businesses, agencies and individuals are being hit by cyber criminals in the country. The prevalence of cybercrime has increased in nation. The United States and the United Kingdom are the third-largest country in the world internet crime, while 5.5 percent of the world's hackers are said to be civilians. Most young people, as the "Yahoo" kids are promised, have taken advantage of fraudulent online transactions, electronic shopping and e-commerce growth to engage in heinous crimes. As such, it is affecting the image of the outside world, and cyber security should be given serious attention. Preventing cybercrimes requires a collective effort from individuals, organizations, and governments. By taking individual precautions, implementing organizational measures, and supporting government initiatives, we can promote a safer online environment and reduce the risk of cybercrimes. Remember, cybersecurity is a shared responsibility, and together, we can make a difference.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, February 2025

REFERENCES

[1]. Cybersecurity and Infrastructure Security Agency. (2022). Tips for Avoiding Cyber Threats.
[2]. Federal Bureau of Investigation. (2022). Cyber Crime.
[3]. International Telecommunication Union. (2022). Cybersecurity.
[4]. National Institute of Standards and Technology. (2022). Cybersecurity Framework.
[5]. United Nations. (2022). Cybercrime.