International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Digital Violence and Gender: A Legal and Social Analysis of Cyber Crimes Against Women

Aditi Kulkarni

Assistant Professor DES' Shri. Navalmal Firodia Law College, Pune (Maharashtra)

Abstract

The advancement of digital technologies has undoubtedly transformed modern communication, but it has also opened new avenues for gendered violence against women. This research paper explores the growing menace of cybercrimes against women, examining the socio-cultural and psychological reasons of such gender-based offenses. It analyzes various forms of cyber violence—including cyberstalking, image-based abuse, doxing, and sextortion—and evaluates the legal responses under Indian law including Indian Constitution, BNS, etc. The paper further examines international conventions such as CEDAW, ICCPR, ICESCR and the Budapest Convention to assess global standards in addressing online gender violence.

Keywords: Cybercrimes against women, online gender-based violence, Indian cyber law, image-based abuse, international legal frameworks

Introduction

In the present digital era, technological development in the field of computers and internet have brought the world closer than ever. The world is almost without boundaries. This virtual environment created by interconnected digital technologies, particularly the internet, is referred as cyberspace. It includes all online platforms, networks, computer systems, and digital communication tools that allow users to interact, share content, and access data across the globe. This cyberspace is used constructively as well as destructively by people. It can be a space for innovation, connection and for cybercrimes like hacking, identity theft, online fraud, and harassment. Illegal activities in cyberspace can target individuals, organizations, or even governments. Unlike traditional crimes, cybercrimes are often borderless, allowing perpetrators to operate remotely and anonymously from anywhere in the world. This paper aims to discuss different aspects of cybercrimes especially regarding women. It is important to discuss cybercrimes against women because they reflect and amplify existing gender-based violence in a new digital form. These crimes not only invade privacy but also cause severe psychological and emotional harm. Bringing attention to these issues is crucial for ensuring a safe and equal digital environment for women.

Crimes Against Women- Social, Psychological & Jurisprudential Dimensions-

Discrimination and violence against women is continuing from long period in not only in India but also almost all over the world. Patriarchal societal structure where men hold primary power often limits women to subordinate roles, reinforcing gender inequality. In many cultures, traditional beliefs and religious interpretations assign women secondary roles, emphasizing obedience, modesty, and domestic duties. These social norms discourage female education, independence, and public participation. Historically, women have had limited access to education, which restricts their opportunities for employment,

leadership, and financial independence. Education is key to empowerment, and its absence keeps women dependent and voiceless. This further leads to women's financial dependence on male family members, which reduces their ability to make independent choices, leave abusive relationships, or participate equally in society. Some stereotypes consider women as weak, emotional, or unfit for leadership. These social conditions have led to discrimination and further into violence against women. As a result, girl children were considered as unwanted and burdensome. Thus, practices of sex selective abortion, female infanticide were practiced. Subordination of women can be seen through practices like female genital mutilation, child marriages, dowry death, honor killing, teenage pregnancy, domestic violence, sexual harassment, lower literacy rate, lower wages than men, etc.

Social factors help us to understand overall social causes while psychological factors indicate individuals' separate causes for violence against women.

Every individual's psychological drivers often stem from learned behaviours, distorted beliefs, personal insecurities, and mental health issues. The urge to dominate, control, or assert power is a common motivation for those who commit acts of violence against women. This may stem from insecurity, low self-esteem, or an upbringing that normalized male superiority and control. Some individuals internalize negative beliefs about women—seeing them as inferior, emotional, or deserving of punishment. People with poor impulse control, anger management issues, or high levels of trait aggression are more likely to commit violent acts. Women often tolerate such acts of domestic violence due to their dependence or social gender stereotypes. Viewing women primarily as objects for male pleasure can dehumanize them and reduce empathy. This often contributes to crimes against women such as rape, sexual harassment, assault, and exploitation, blackmailing, stalking, etc.

Discrimination and crimes against women are not merely indicative of deeper structural inequalities and patriarchal power imbalances in society violate the legal rights and protections under constitutional, statutory, and customary laws. It violates principles of equality, dignity, liberty, and bodily autonomy enshrined in the Constitution of India, particularly under Articles 14, 15, and 21. Judicial pronouncements have progressively expanded the ambit of women's rights by interpreting existing laws in consonance with constitutional morality and international human rights obligations, notably the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW). Courts have adopted a purposive and transformative approach to statutory interpretation to ensure that laws serve as instruments of social change and gender justice.

Moreover, the doctrine of 'due diligence', recognized in international human rights law, imposes a positive obligation upon the State to enact, enforce, and implement laws effectively, to protect women from all forms of violence, whether perpetrated by State or non-State actors. The failure to do so may result in a breach of both domestic constitutional mandates and international treaty obligations. There are statutory provisions aimed at recognizing, preventing, and penalizing acts that infringe upon the bodily integrity, dignity, and autonomy of women.

Cyber Crimes Against Women: Causes And Types-

The social, psychological factors of crimes against women started in digital space also in the early 2000s, as internet access expanded. There was introduction of social media and digital communication tools, smartphones with cameras, cloud storage and easy sharing of private content, etc. Privacy in both the virtual and physical worlds is literally vanishing. Not only internet user women but also teenage girls,

homemaker women, working women, celebrity, writer, activist women, transgender women and even tribal women who are completely unaware of computer technology are victim of cyber crimes.

Council of Europe notes that cyberviolence is an increasing problem worldwide and there is more increase in it since Covid-19 pandemic. It is often gender-based targeting women and girls. Cyberviolence hampers the full realisation of gender equality and violates women's rights. These crimes disproportionately target women, inflicting psychological harm and deterring their full participation online.

As reported by International Telecommunication Union's (ITU) 2017, men in two-thirds of the world's countries use the internet at a higher rate than women. This highlights both the exclusion of women from the digital sphere and the increased tendency of men to achieve technological progress. Most of the women are unaware of their legal rights and are fearful of social exclusion and stigma. As a result, women are comparatively softer target and are increasingly susceptible to cyber-attacks. Social media, messaging apps, and online forums have become tools for harassment, stalking, and abuse. Activities like revenge porn, doxing, and cyberstalking are specifically designed to target and shame women. These crimes often involve violations of privacy and personal dignity, deeply impacting women's mental health.

The anonymity provided by cyberspace acts as a shelter for individuals committing cybercrimes. It empowers perpetrators to act without fear of immediate consequences. Unlike physical crimes that require proximity, cybercrimes can happen across countries and cultures, making them easier to commit.

Lack of Awareness and Cyber Hygiene also contribute to occurrence of cyber crimes against women. Many women, especially in developing countries, may not be fully aware of privacy settings, digital rights, or how to report cybercrimes. This makes them easier targets for crimes like phishing, identity theft, or blackmail through hacked personal data.

Women frequently fall victim to certain types of cybercrimes, such as extortion, intimidation, cyber pornography, sharing explicit material, harassment, and bullying, defamation, morphing, creating fake profiles. etc. Some of cyber crimes against women are discussed below.

- **Cyberstalking-**

Cyberstalking and related online harassment involve a course of conduct via digital means (social media, email, messaging, etc.) that is repeated, targeted at a specific woman. It is often intended to dominate, intimidate or control her. Such conduct can include unwanted messages, threats, and continuous unwanted contact. It often causes the victim severe emotional distress and fear of harm. It may involve posting false or degrading statements, impersonating the victim, or publicly revealing sensitive information. Online stalking frequently escalates the gendered nature of abuse by involving sexualized threats or misogynistic taunts. Victims experience ongoing fear, reputational damage, anxiety, and may restrict their online and offline activities.

- **Image-Based Sexual Abuse-**

Image-based sexual abuse refers to the non-consensual creation or distribution of sexually explicit or suggestive images and videos of a woman. This includes so-called "revenge pornography," deepfake pornography, hidden-camera recordings ("upskirting"), and other intimate media shared without the concerned woman's consent. In this, both real and digitally fabricated images are used. Such images are obtained by perpetrators from woman's partners or by hacking and then are disseminated via websites, social media or messaging. The intent is typically to humiliate, shame or control the victim by eroding her reputation, coercing her into sexual acts, or exerting power after a relationship ends.

- **Doxing-**

Doxing, in simple words, means disclosure of private personal data. It is the act of researching and broadc-

asting an individual's private, personally identifiable information online without consent. This may include home address, phone numbers, employment details or even unpublished intimate data. It is done deliberately to expose the victim publicly. By revealing personal data, offenders make it easier for others to contact, threaten or stalk the victim in real life. Because women are more vulnerable to certain forms of violence, the exposure of their private information carries a high risk of physical and emotional harm. Targets of doxing may face unsolicited contact, threats, stalking or violence.

- **Impersonation-**

Impersonation occurs when an offender creates a false online persona or otherwise assumes someone else's identity to deceive or harm the victim. In legal terms, it means, "pretending to be someone else or falsifying the identity of a person with the intention of harming, defrauding, intimidating or threatening." Online impersonation can take two main forms. First, a perpetrator may pose as a trusted acquaintance of the woman (a friend, colleague or romantic interest) to elicit private information or intimate images; this is often called "catfishing." Second, the offender may pretend to be the woman herself – posting messages or content in her name on social media – with the aim of damaging her credibility or reputation. Both approaches are used to facilitate other crimes (e.g. doxing, blackmail) or to isolate the victim by sowing distrust among her contacts.

- **Online Defamation-**

The cyberlibel or cyberslander involves the publication of false statements or rumors on digital platforms that damage a woman's reputation. In law, defamation requires a false assertion of fact made publicly that injures the person's good name. Here, the "cyber" aspect is merely the medium: the content is spread via blogs, social media, news sites or comment forums. The content may include fabricated accusations (sexual, criminal, or immoral conduct) or malicious gossip. Because online content is easily shared and searchable, the harm is magnified: reputational damage can persist long after the original posts are removed.

- **Trolling-**

Trolling refers to sending deliberately provocative, insulting or hateful messages to women online in order to provoke or humiliate them. It includes malicious posting of inciting content including rape threats or violent images aimed at women. Harassers may flood a woman's online space with abusive comments, sexually explicit harassment, or demeaning slurs. They often target women's appearance, sexuality or voice in the public sphere, using memes or derogatory tags.

- **Sextortion-**

Sextortion is nothing but online sexual extortion. It is a cybercrime where the perpetrator threatens to distribute a woman's sexual images or videos unless she provides sexual favors, or money. It is a form of sexual blackmail facilitated by technology. In sextortion, perpetrator coerces the woman by threatening to publish the content if demands are not met. The threat might also include fabricated intimate material like deepfakes to extort victims. The intention may be to humiliate, to retaliate and control the woman.

Indian & International Legal Framework-

There are special provisions in the Constitution to protect the interest of women. Preamble, which is considered as the key to the minds of makers of Constitution, lays down certain values with respect to the individuals, such as dignity of the individuals, liberty of thoughts, expression, belief, faith and worship, equality of status and of opportunity in all fields to eliminate discrimination, justice in social, economic and political matters.

Fundamental rights are conferred under Part III of the Constitution without discrimination based on gender. Besides this, Article 15(3) empowers legislature to make laws for safeguarding the interest of the women. Under Art. 15 (3), the law can only be made in favour of women and not against women. Also, the law enacted under the ambit of Article 15(3) shall not be considered in violation of right to equality.

One of the most important right under the Constitution is conferred through Art. 21. It has simple words- "No person shall be deprived of his life or personal liberty except according to procedure established by law". However, Indian judiciary has widened its scope to include various rights necessary for all individuals to have a dignified life. Right to life under Art. 21 is no more restricted to mere "animal existence" where bare breathing was considered sufficient. Now it encompasses all the aspects, which are required for a decent standard of living such as right to food, right to shelter, right to sleep, right to health, etc.

The cybercrimes committed against any woman can violate her right to privacy, right to dignity, right to health depending on the gravity and type of the offence committed.

The cyber crimes like cyber stalking, morphing violate women's right to privacy. The Supreme Court of India considered right to privacy as part of right to life in case of Justice K.S. Puttaswamy v. Union of India (AIR 2017 SC 4161). Right to privacy is not defined under Constitution but it simply means right not to have any kind of intrusion or interruption or disturbance in one's personal life. This right is recognized not only under Indian Constitution but also recognized as one of the essential human right under various international instruments such as Universal Declaration of Human Rights (UDHR), International Covenant on Civil and Political Rights (ICCPR), International Covenant on Economic, Social, and Cultural Rights (ICESCR).

In the case of Consumer Education and Research Centre v. Union of India (AIR 1995 SC 636), the Supreme Court explicitly held that the right to health and medical care is a fundamental right under Article 21 of the Constitution. It was also held that this right to health and medical care, to protect health and vigour are some of the integral factors of a meaningful right to life.

World Health Organization defines right to health as well-being at all physical, mental and at social level. It is not restricted to mere absence of any disease or infirmity. It is wide enough to include all aspects related to health such as physical and mental well-being. Article 12 of ICESCR provides that all individuals have right to adequate standard of mental as well as physical health. This mental health aspect of right of health is infringed by cyber crimes.

Right to dignity is the core right, which is essential for the existence of human being and for having comfortable life. It is considered as the foundation of all other human rights. It cannot be enjoyed in isolation. it encompass all other rights which are essential for the enjoyment of this right such as adequate food, standard of living, safe environment, freedom from exploitation or abuse and others.

Apart from Constitution, new Bharatiya Nyaya Sanhita (BNS), 2023, which replaced Indian Penal Code (IPC) contains few provisions to address cybercrime, notably against women. These provisions are intended to strengthen legal protections against digital offenses such as online harassment, voyeurism, stalking, and illegal distribution of private content. Sec. 77 of it deals with Voyeurism, which criminalizes the act of capturing, publishing, or transmitting images of a woman's private parts or private acts without her consent. Sec. 78 deals with stalking which includes Cyberstalking as well. Section 78 addresses stalking in both physical and electronic forms. It penalizes individuals who monitor or contact a woman repeatedly through electronic means, such as emails, messages, or social media, despite clear indications of disinterest. Section 294 deals with the publication or transmission of obscene material, including

through electronic means. Section 303 deals with cyber theft. Under this provision, acts of theft of mobile phones, data, or computer hardware/software are penalized. Sec. 336 pertains to forgeries perpetrated with intent to harm a person's reputation, whether by physical or electronic means. It includes circumstances in which misleading information is circulated online to malign somebody. Section 356 penalizes defamation, including the sending of defamatory content through emails or other electronic communication. The BNS's inclusion of these provisions demonstrates its commitment to tackling the changing nature of crimes against women in the cyber space.

Apart from BNS, Information Technology (IT) Act, 2000 is India's primary legislation governing offenses committed using digital platforms. Several sections are directly applicable to cybercrimes affecting women. Section 66E penalizes the intentional capture, publication, or transmission of images of a person's private parts without consent, thus addressing voyeuristic behavior in digital spaces. Section 67 and Section 67A criminalize the publication or transmission of obscene or sexually explicit material in electronic form. These sections are often invoked in cases of revenge porn, morphed image sharing, and non-consensual content circulation. Section 66C deals with identity theft, such as creating fake profiles to harass or defame women, while Section 66D addresses cheating by impersonation, often used in online blackmail and scams. Section 72 punishes the breach of confidentiality and privacy, particularly when sensitive data or personal images are shared without consent.

In addition to criminal laws, several special legislations offer protection to women, even in cyber contexts. The Protection of Women from Domestic Violence Act, 2005 is increasingly being interpreted to cover digital abuse within domestic settings, such as surveillance through apps, threats via messaging, or emotional manipulation using private content. The Indecent Representation of Women (Prohibition) Act, 1986 addresses the publication or circulation of indecent images of women, including in online advertisements, social media, or other electronic platforms. These laws recognize the overlap between gender-based violence and the use of technology to perpetuate control or harm.

Together, these provisions offer a legal basis for prosecuting a range of cyber offenses against women, from online stalking to digital sexual harassment.

Several international legal instruments, conventions, and guidelines either directly or indirectly address cybercrimes against women. Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), 1979 is a core international treaty focusing on women's rights. Though it predates the internet era, its General Recommendation No. 35 updated its interpretation of gender-based violence to include online and ICT-facilitated violence. It reads as – "Gender-based violence against women manifests in a continuum, including online abuse, cyberstalking, and harassment through digital means". The Convention on Cybercrime, also known as Budapest Convention is the first and most significant international treaty focused on cybercrime. Though it does not specifically address gender, it provides a legal framework to criminalize acts like unauthorized access, data interference, and computer-related fraud, which are often used in cyber harassment and abuse of women. India is not a signatory, but many countries collaborate under this convention for cross-border investigation and cooperation. Convention on Preventing and Combating Violence against Women and Domestic Violence of 2011 has provisions, which addresses stalking, including cyberstalking (Art.34), sexual harassment, which includes online forms like sending unwanted messages or explicit content (Art. 40). The International Covenant on Civil and Political Rights (ICCPR), 1966 guarantees the right to privacy under Article 17, which can be extended to protection from cyber violations like non-consensual image sharing or digital stalking.

Summary and Conclusion-

Crimes against women began as tools of control, domination, and punishment in a patriarchal society. As technology advanced, these methods evolved to include cyber-based violence, which reflects old patterns in new forms and which expands the reach and impact of abuse to cyber space. Cybercrimes targeting women are not merely technological offenses; they are manifestations of deep-rooted patriarchal attitudes reasserting control in the virtual realm. These crimes—ranging from cyberstalking and image-based abuse to doxing and sextortion—inflict psychological trauma, violate dignity, and undermine the autonomy of women. While Indian and international legal frameworks have evolved to some extent to address these harms, to prevent and penalize cybercrimes but it does not seem adequate. Though right to privacy, dignity, health, etc. are considered as fundamental rights of women, these rights are conferred through judicial decisions and through judicial interpretation of Art. 21. Thus there is possibility of reversing or altering these facets of Art. 21 by way of decisions of larger bench.

Though Sec. 294 of BNS penalizes sale, distribution, or public display of obscene material, including digital content, the term 'obscene' is undefined. There are no parameters or test to determine the obscenity. The court has evolved various tests to determine it. However, there is no set or fixed rule to determine it. It is decide from case to case depending upon the facts and circumstances of each case. It has left a great room for subjectivity.

The Artificial Intelligence has increased the risk of cybercrimes by many folds. Thus, it is essential to bring a separate law to regulate the functioning and use of AI and to decide the imposition of liability.

Apart from legal steps, there is also need to increase cyber literacy and cyber hygiene among women. Nationwide campaigns might be helpful to educate women and young users about digital rights, privacy, and available legal remedies, particularly in rural and marginalized communities.

Despite these legal developments, significant gaps persist in reporting, investigation, and prosecution of cyber offenses against women. The interplay between technology and patriarchal control necessitates both a legal and cultural shift.

References-

1. Bharatiya Nyaya Sanhita, 2023
2. Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), 1979
3. Convention on Preventing and Combating Violence against Women and Domestic Violence of 2011
4. The Protection of Women from Domestic Violence Act, 2005
5. Information Technology (IT) Act, 2000
6. Consumer Education and Research Centre v. Union of India (AIR 1995 SC 636)
7. Justice K.S. Puttaswamy v. Union of India (AIR 2017 SC 4161)
8. Universal Declaration of Human Rights (UDHR)
9. International Covenant on Civil and Political Rights (ICCPR)
10. International Covenant on Economic, Social, and Cultural Rights (ICESCR)