Page 2875 - 2884 **DOI:** *https://doij.org/10.10000/IJLMH.114724*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 6 | Issue 2

2023

Cybercrime and Women

KAVYA SRINIVASAN[1]

ABSTRACT

The growth of the internet and the virtual world has resulted in an increase in cybercrime, particularly online harassment of women. According to research, one in every ten women has encountered cyberviolence since the age of fifteen, with incidences increasing during the Covid-19 pandemic. Cybercrime against women is disturbing, and a number of states and international organisations are taking action. The Istanbul Convention outlines provisions for preventing and combatting violence against women committed over the internet. Through several penal law measures, the Budapest Convention addresses online and technology-facilitated violence against women. India has enacted legislation defining the consequences of cyberbullying and cyberstalking. However, the prosecution process remains difficult due to regulations that do not keep up with technological changes and law enforcement officials who lack funding, training, or expertise.

Keywords: *Cybercrime, Cyberlaws, Children, Pandemic, Women.*

I. INTRODUCTION

A new dimension of crime has emerged because of the expansion of the internet and the emergence of the virtual world, popularly known as cybercrime. It has led to a rise in online harassment of women. Despite the relatively recent and expanding phenomenon of internet connectivity, research by the World Health Organisation indicates that one in ten women have already experienced some form of cyber violence since the age of fifteen and the cases intensified with covid pandemic. Furthermore, attacks may occur more frequently against women who share many traits with the target group, such as women of colour, adherents of minority religions, or LGBTQ individuals. Cybercrime against women is an extremely concerning topic and requires prompt action.[2]

Multiple nations and global institutions have already envisaged on the path to foster the rights of women who are victims of cybercrime. Participants in the international conference on promoting the role of women in preventing, investigating, and prosecuting cybercrimes, held in San Jose on November 10–11, 2022, by the Council of Europe in partnership with the

[1] Author is a student at University of Glasgow, Scotland, United Kingdom.

[2] "A Training Handbook for Criminal Justice Practitioners on CYBERVIOLENCE ..." <https://www.unodc.org/documents/southernafrica/Publications/CriminalJusticeIntegrity/GBV/UNODC_v4_121022_normal_pdf.pdf> accessed February 5, 2023

 [ISSN 2581-5369]

Legislative Assembly and Public Ministry of Costa Rica, agreed that women have a critical role to play in effective criminal justice responses to cybercrime. The Istanbul Convention, a historic treaty for women's rights, provides countries with the most complete set of measures for preventing and combating all types of violence against women and domestic violence. It does not explicitly include the digital aspect of violence against women, but as intended by its drafters, the scope of Article 2's definition of that violence includes acts perpetrated in the internet sphere. Article 40, "any form of unwanted verbal, non-verbal or physical conduct of a sexual nature with the purpose or effect of violating the dignity of a person, in particular when creating an intimidating, hostile, degrading, humiliating or offensive environment," it is applicable to sexual harassment that is facilitated by technology and occurs online. Some forms of online and technology-facilitated violence against women are addressed directly and indirectly by the Budapest Convention through a variety of substantive criminal law provisions. Other provisions deal with behaviours that encourage such violence. The investigation of acts of online and technology-facilitated violence against women, as well as the collection of electronic evidence, would be made possible by the procedural authorities and provisions on international cooperation of the Convention on Cybercrime. India has outperformed many other emerging countries in this area. In the year 2000, the Information and Technology Act was passed. The Act's Sections 66E, 67, and 67A outline the penalties and fines for voyeurism and the publication or transmission of pornographic or sexually explicit information online. Additionally, the Indian Penal Code's Sections 354A and 354D establish penalties for cyberbullying and cyberstalking.

The propagation of the various types of violence against women is made possible by technology and the internet. The prosecution process is still challenging because laws may not be keeping up with technology advancements and because law enforcement authorities might not have the necessary resources, training, or tools to help victims.

II. [3] CYBERCRIME AS AN OFFENCE IN THE BROAD SENSE

Any criminal behaviour involving a computer, a networked device, or a network is considered a cybercrime. While most cybercrimes are committed to make money for the perpetrators, some are committed against specific systems or devices to harm or disable them. However, it is important to understand this term beyond face value. Cybercriminals access personal information via computer technology, and they utilise the internet for harassment and

[3] Sharma A and Singh A, "Cyber Crimes against Women: A Gloomy Outlook of Technological Advancement" (2018) 1 www.ijlmh.com

 [ISSN 2581-5369]

exploitation. This includes stalking, blackmailing, and threatening behaviour via emails, morphed photographs, weird comments, etc. In most cases, women are victim in this infamous side of cybercrime. This doesn't pertain to one nation but on a global scale.

III. WOMEN AND CHILDREN BEING TARGETS OF CYBERCRIME

Cyberstalking, harassment, extortion, blackmail, etc. primarily targets women. Many times, because the women and children are not aware of the process for filing a complaint, the criminals have an easier time harassing, abusing, blackmailing, etc. the family. Cybercriminals target women by creating fake identities on Facebook, Twitter, and other social networking sites. This causes great harm to women because of the huge blackmailing, threatening, harassing, and cheating that takes on these sites via email and messenger. Men with bad intentions commit various cybercrimes, such as for financial gain, retaliation, insulting a woman's modesty, extortion, blackmail, sexual exploitation, defamation, inciting hatred against the community, prank satisfaction of taking control, and information theft. Cyber violence against women and girls is a growing concern as more individuals may easily use the internet and social media. Although there is a dearth of statistics, estimates from the EU indicate that one in ten women have been the victim of cyber violence since the age of 15. The impact on women's lives is far more painful than it is on males, according to Jurgita Peciuriene, the programme coordinator for gender-based violence at EIGE. "Women are more likely than men to be victims of serious kinds of cyber assault," she added. Women and girls who have been victims of sexual harassment, stalking, or abuse from an intimate partner "offline" are frequently the same people who perpetrate such crimes "online." Cyber violence, like other forms of violence, has a significant impact on victims' life and can take many different forms.

IV. [4] CYBERCRIMES MOSTLY TARGETED TO WOMEN

1. Sextortion- Blackmail takes the form of "sextortion." Threats to release explicit text, images, or videos about someone are involved. This could be done to demand money or coerce the victim into doing something they don't want to. Often, the victim is not informed or given consent before photos or videos are taken. The criminals begin requesting financial or sexual favours from the victims. They felt emboldened to use their manipulated photographs to intimidate people to extract money from them because they had no money. Recent trends have revealed men to be victims of this crime.

[4] Kumar S and Priyanka, "CYBER CRIME AGAINST WOMEN: RIGHT TO PRIVACY AND OTHER ISSUES" (2019) 5 The Law Brigade (Publishing) Group

 [ISSN 2581-5369]

2. Pornography- Non-con-sensual pornography, also referred to as cyber exploitation or "revenge porn," is the online publication of sexually explicit photos or films without the subjects' knowledge or permission. The perpetrator is frequently an ex-partner who, in retribution for ending a relationship, uses pictures or videos taken over the course of the relationship to publicly humiliate and shame the victim. However, the attackers are not usually current or former partners, and the motivation is not always retribution.

3. Cyberstalking- Cyberstalking is the practise of stalking someone online or via email, text, or other electronic messaging. Repeated episodes that may or may not be harmless on their own, but when added together, erode the victim's sense of security, and generate discomfort, dread, or alarm.

4. Cybersex trafficking- Since there is no physical contact between the victim and the criminal, it differs from physical sex trafficking. The act of broadcasting, recording, or photographing a victim participating in sexual or personal actions from a central place and then selling the content online to sexual predators and customers is known as cybersex trafficking. Women have been coerced, tricked, and threatened into taking part in cybersex trafficking, which is sexual abuse of women.

5. Cyberbullying- This involves making abusive, defamatory, and fraudulent statements about the victims on social networking sites and asking money to have them taken down. Rape and death threats may also be sent to the victim. Additionally, it involves making offensive comments on the victim's posts.

Female callers made up 73% of those to the Revenge Porn Helpline, and 97% of them reported misuse of private images. In contrast, 90% of the 27% of male callers were sextortion victims (2019). A study conducted by University of Exeter revealed that almost 3 out of 4 victims are females, 9 out of 10 women victims suffer intimate image abuse. The research examines the varying experiences of men and women, as well as adults and young people, as victims of intimate image abuse using data from the helplines, both of which are run by the Southwest Grid for Learning. The study's key finding demonstrates that a disproportionately high proportion of victims are women, and that the crime is committed differently depending on the victim's gender.

V. [5] ISTANBUL CONVENTION

The Council of Europe's Committee of Ministers adopted the Istanbul Convention and

[5] Wilk Avan der, "PROTECTING WOMEN AND GIRLS FROM VIOLENCE IN THE DIGITAL AGE" [2021] Council of Europe

accompanying justification report on April 7, 2011. On May 11, 2011, during the 121st Session of the Committee of Ministers in Istanbul, it was made available for signature. 34 states are parties to the convention as of October 2021, one year after it went into effect on August 1st, 2014. Any nation willing to carry out the convention's requirements is welcome to join.

The Istanbul Convention, a historic treaty for women's rights, provides countries with the most complete set of measures for preventing and combating all types of violence against women and domestic violence. Such violence is positioned as a violation of human rights and a form of discrimination against women, and it is strongly linked to the realisation of women's equality with men. The Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse is mentioned in the preamble of the convention (Council of Europe 2011a), along with the European Social Charter, the Council of Europe Convention on Action Against Trafficking in Human Beings, and the Council of Europe Convention on Action against Human Trafficking. The United Nations Convention on the Rights of the Child, the United Nations Convention on the Rights of Persons with Disabilities, and the United Nations Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW) and its subsequently adopted general recommendations are also mentioned in the Istanbul Convention.

The convention is organised on the "4 Ps": co-ordinated policies, prosecution of perpetrators, protection and support of victims, and prevention.

According to the convention's definitions and concepts, violence against women is defined as "a violation of human rights and a form of discrimination against women" (Article 3a) and as a form of gender-based violence that causes "physical, sexual, psychological or economic harm or suffering to women," thus targeting women due to their gender, as well as gendered "socially constructed roles, behaviours, activities and attributes" (Article 3c).

For instance, Article 40, which is defined as "any form of unwanted verbal, non-verbal or physical conduct of a sexual nature with the purpose or effect of violating the dignity of a person, in particular when creating an intimidating, hostile, degrading, humiliating or offensive environment," is applicable to online and technology-facilitated sexual harassment. Because stalking is hereby defined as "the purposeful behaviour of frequently engaging in threatening behaviour directed at another person, causing her or him to fear for her or his safety," the convention's provision on stalking (Article 34) also applies to online and technology-facilitated stalking. The explanatory report to the convention (ibid.) explicitly categorises "the pursuit of any active contact with the victim through any available means of communication, including

 [ISSN 2581-5369]

modern communication tools and ICTs" as unwanted contact within the meaning of the provision, confirming the extension of Article 34's reach to the digital sphere.

VI. [6] BUDAPEST CONVENTION

The first and most important international legally binding convention focusing on cybercrime and electronic evidence is the Council of Europe Convention on Cybercrime (also known as the Budapest Convention).

In November 2001, the Committee of Ministers of the Council of Europe accepted the convention and its justification report. It was made available for signature in Budapest and became operative on July 1st, 2004. 66 states are party to the convention as of June 2021. Any nation willing to put its provisions into practise and participate in international cooperation on cybercrime is invited to join the convention. It acts as a blueprint for any nation creating comprehensive national legislation to combat cybercrime and any other crime involving electronic evidence, and many states have already taken advantage of this chance. The convention mandates that violations of copyright and related rights, as well as offences committed against or using computer data and systems, as well as offences relating to the creation, dissemination, or possession of CAM, be made crimes. Additionally, parties to the convention must strengthen their domestic criminal procedural laws, give their judicial systems the tools to secure electronic evidence related to any crime, and efficiently facilitate international cooperation and mutual legal assistance (MLA) for the investigation and prosecution of cybercrime and other crimes involving electronic evidence.

The primary goals of the convention are to: 1) harmonise the domestic criminal substantive law elements of offences and related provisions in the area of cybercrime; 2) provide domestic criminal procedure law powers necessary for the investigation and prosecution of such offences as well as other offences committed by use of a computer system or evidence in relation to which is in electronic form; and 3) establish a quick and efficient regime of international co-operation (Council of Europe 2001a).

The Budapest Convention's effectiveness and legitimacy can be attributed in large part to the plans for action that successfully balance safeguards for the rule of law with an effective criminal justice response.

[6] Wilk Avan der, “PROTECTING WOMEN AND GIRLS FROM VIOLENCE IN THE DIGITAL AGE” [2021] Council of Europe

 [ISSN 2581-5369]

VII. CYBER VIOLENCE AGAINST WOMEN DURING COVID 19

Domestic abuse, online and ICT-facilitated violence, and other types of violence against women are all present during COVID19. These acts of abuse and violence occur in a climate of widespread, institutionalised prejudice based on gender. In the US, one in two young women between the ages of 18 and 29 who have experienced online sexual harassment report receiving unwanted explicit photographs. While there remains a gender digital divide, women and girls are utilising the internet more frequently than males during the pandemic. According to reports, COVID-19 is the first significant pandemic of the social media era. Users with weak digital abilities are particularly vulnerable to cyberviolence during this time. Concerningly, women and girls are more likely to experience these types of violence because of the digital gender divide.

[7]Internationally, 1 in 3 women had experienced physical or sexual abuse, primarily by an intimate partner, even before the COVID-19 pandemic started. Recent data reveals an increase in calls to domestic abuse hotlines across numerous nations since the COVID-19 outbreak. On the streets, in public places, and online, women continue to experience sexual harassment and other types of assault. Survivors have little access to support services and little knowledge of the support systems that are out there. Some nations have shifted funds and personnel from the fight against violence against women to provide emergency COVID-19 relief. The new front line for violence against women and girls is online, where it has skyrocketed since COVID-19 and the lockdowns. Online abuse of women and girls, including trafficking, is a major source of risk since it crosses generational and intersectional lines. The second vice president of Grevio-CoE and a member of Fondazione Pangea Reama, Ms. Simona Lanzoni, stated that "first, we note the need to highlight the continuum of violence against women and domestic violence offline and online, and GREVIO decided during its 21st plenary meeting to prepare its very first General Recommendation. With the goal of advising state parties to the Istanbul Convention, this work will show the Istanbul Convention's applicability and relevance to online and technologically enabled violence against women. Second, there has been a spike in online aggression during this time of restrictions brought on by the pandemic. Because there are no established methods for stopping violence when it is committed in cyberspace, we must put precise and successful multi-stakeholder-based policies in place.

[7] "Women's - Ohchr.org" (*ochre.org*) <https://www.ohchr.org/sites/default/files/Online_VAW_Statement.pdf> accessed February 5, 2023

VIII. [8]INDIA- A REVOLUTION IN CYBERCRIME LAWS

Sections 66E, 67, 67A, and 67B of the IT Act, as well as Sections 354D, 465, 471, 499, 500, and 509 of the Indian Penal Code, all address numerous instances of cybercrime against women. Sections 14 and 15 of the Protection of Children from Sexual Offences (POCSO) Act, 2012 also apply if the girl is a child. The Information Technology Act of 2000's According to section 66E to this clause, if someone violates someone else's privacy by taking, disseminating, or sending an image of their private area without that person's permission, they could face up to three years in prison, a fine of up to two lakh rupees, or both. Section 67 in The Information Technology Act, 2000[3] covers the electronic transmission or publication of pornographic material. Any content that is lascivious, appeals to the prurient curiosity, or has an effect that tends to deprave and corrupt people is "obscene material" under this document. Section 67A in The Information Technology Act, 2000[4] deals with the electronic publication or transmission of content that contains sexually explicit acts, etc. Following a first conviction, a term of up to seven years in prison and a fine of up to ten lakh rupees is imposed, with a sentence of up to five years in prison for successive convictions. A person who fabricates any fraudulent documents, electronic records, or components thereof with the goal to cause harm or damage is guilty of forgery, according to Penal Code Section 463. The use of fake paper documents or electronic records as authentic is prohibited by Section 471 and is subject to the same penalties as document forgery. Making a false electronic record would include morphing the photographs.

IX. [9]LOOPHOLES

Government should enact severe legislation that apply to Internet Service Providers (ISP), as they are the only ones who have a complete record of all the data that users of the internet have accessed. To stop crimes in their beginnings, ISPs should be required to disclose any suspicious behaviour that any individual engages in.

Legislation must impose stricter regulations on cyber cafes. These businesses must maintain accurate, detailed records of all the clients who use their internet services. Many people use cyber cafes to engage in illegal activities so that their IP addresses are hidden from view during any ensuing investigations.

[8] 8 A, "Cybercrimes and Cyber Laws in India" (*Cybercrimes and Cyber Laws in India | ProBono India*) <https://probono-india.in/blog-detail.php?id=218> accessed February 7, 2023

[9] Joshi P, "Cyber Laws: Loopholes Aplenty" (*Business Standard*January 20, 2013) <https://www.business-standard.com/article/technology/cyber-laws-loopholes-aplenty-111111800098_1.html> accessed February 7, 2023

 [ISSN 2581-5369]

People should be aware of the aspects of their daily lives that cameras are capturing and act modestly when these instances occur. There needs to be greater public understanding of cyber culture and its negative aspects. It's important to educate people about their rights. The most significant barriers to addressing the problem of cybercrimes against women are procedural, such as the conflict of jurisdiction, loss and lack of evidence, absence of a cyber army and a cyber-savvy judiciary. Women online users are hesitant to report cybercrimes right away out of concern that they would be identified in public. Even though there are more of these events, few victims are prepared to file a complaint and demand justice.

X. [10] CONCLUSION

The main issue with cybercrime is the method of operation and the persistence of the cybercriminal. To stay one step ahead of such offenders, the judiciary should be strengthened with contemporary web-based apps, together with the police force and the investigative agencies. Women are increasingly the easy targets in a world that depends more and more on electronic and online platforms for criminal activity. The law must go above and beyond to punish such criminals with severe measures. Governments have the power to enact laws that guarantee the protection of human rights, particularly those of women, both online and in real-world settings. At the same time, people need to develop their online and offline smarts; they need to know how to be cautious online and how to take legal action if their rights are abused. Cybercrimes like email spoofing and morphing lack a moral foundation in society and are therefore treated leniently. Therefore, it is imperative to improve women's knowledge of the need to use caution when utilising internet resources and to receive correct assistance if they are ever a victim of cybercrime so they can speak out against it.

(A) [11] Suggestions

Any state is very concerned about the rising number of crimes against women, but cybercrime makes the situation even more difficult because it gives criminals the chance to create false identities before engaging in illicit activity. To combat this, the government should enact stronger rules that apply to Internet Service Providers (ISP), as they are the only ones that have a complete record of all the data that users of the internet have accessed. ISPs should be required to report any suspicious behaviour that a user engages in; this will help to stop crimes before they start. Cybercrime cases should be dealt by not disclosing the names and personal details of

[10] Sharma A and Singh A, "Cyber Crimes against Women: A Gloomy Outlook of Technological Advancement" (2018) 1 www.ijlmh.com

[11] Kumar S and Priyanka, "CYBER CRIME AGAINST WOMEN: RIGHT TO PRIVACY AND OTHER ISSUES" (2019) 5 The Law Brigade (Publishing) Group

 [ISSN 2581-5369]

the victims as this will give them the confidence to approach the police or concerned authorities as it defeats the stigma around the issue. Therefore, essential steps must be taken to foster the rights of the women and children.

*****

 [ISSN 2581-5369]