INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 10 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

THE INTEGRATED ROLE OF CYBER FORENSICS AND INDIAN LAWS TO ENSURE WOMEN'S SAFETY IN DIGITAL AGE AND CHALLENGES

AUTHOR - ISHAN ANAND, STUDENT, B.A.LL.B (VIII SEMESTER), GALGOTIAS UNIVERSITY

BEST CITATION - ISHAN ANAND, THE INTEGRATED ROLE OF CYBER FORENSICS AND INDIAN LAWS TO ENSURE WOMEN'S SAFETY IN DIGITAL AGE AND CHALLENGES, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (10) OF 2025, PG. 991-1004, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

There exists a singular universal truth that holds true across all nations, cultures and communities: the perpetration of violence against women is inherently unacceptable, inexcusable and intolerable[2].

The expanding influence of the Internet, the swift proliferation of information and communication technologies (ICTs) and the widespread use of electronic devices such as mobile phones, computers, tablets, Bluetooth and data storage devices coupled with the extensive reach of social media have introduced novel challenges in addressing violence against women and girls. The trend of physical crime against women has shifted to hybrid crime model leading to rise in threat against women.

The rise of cybercrime has become a global issue with profound implications for societies and economies worldwide. This phenomenon poses threats to the peace and prosperity of individuals, particularly jeopardizing the goals of inclusive and sustainable development underpinned by fundamental human rights that underscore gender equality.

To address these issues Government of India has come up specifically with the I.T Act[3] and D.P.D.P Act [4] along with amendments in IPC[5], CRPC[6] and IEA[7] now BNS[8], BNSS[9] and BSA[10] respectively but these laws would be of no use without the help of cyber forensic which is used to collect concrete evidence against the perpetrator and present an air tight case in the court of law. Computer forensics is defined as the systematic process of identifying, collecting, preserving, analyzing and presenting digital evidence in a manner that is admissible in a court of law.

The paper meticulously explores the current state of Cyber Legislation and integration of Cyber forensics in it, aimed at safeguarding the interests and well-being of women in India. Additionally, it advocates for a heightened and refined Cyber Legislation framework recognizing the imperative need to address multifaceted challenges and intricacies.

Keywords: Cyber Crime, Cyber Forensics, Admissibility of Electronic Evidence

CHAPTER- I

1. INTRODUCTION:

"Digitalisation is a lamp used to illuminate the society but there is a dark beneath the lamp."

Countless women and girls globally endure targeted acts of violence solely based on their gender. The scourge of violence against women and girls (VAWG) transcends geographical borders, traverses racial & cultural divides and disregards distinctions in income groups. This pervasive phenomenon inflicts profound harm upon its victims and impacts society on a holistic scale. The expanding influence of the Internet, rapid proliferation of information and communication technologies (ICTs) and widespread use of electronic devices, coupled with the extensive reach of social media, introduce novel challenges in addressing this

multifaceted issue. The alarming rise of cybercrime on a global scale presents profound implications for societies and economies, thereby jeopardizing the goals of inclusive and sustainable development underscored by fundamental human rights emphasizing gender equality and women's empowerment.

While Government of India responses, notably through legislative measures such as the I.T Act, D.P.D.P Act, BNS, BNSS and BSA aim to mitigate the prevalence of violence against women but there exists a critical gap. The degrees and impacts of violence, trauma, and loss routinely experienced by women, girls, and children often go unreported, prompting the need for a comprehensive analysis of existing frameworks.

A notable case in the realm of women's cybersecurity surfaces on January 1, 2022, with the initiation of a GitHub Pages site under the subdomain "bullibai.github.io." This incident displayed manipulated images of diverse Indian women, including journalists, social workers, students, and prominent personalities, accompanied by derogatory content. These images, allegedly sourced from individual social media accounts, were altered and showcased on the website for auction without their consent, exacerbating the severity of the situation. Strikingly, all targeted women belonged to the Muslim faith, adding a layer of complexity to the incident.

Despite the gravity of such cybercrimes, the legal response raises concerns. On March 29, the court granted bail to the accused, citing humanitarian grounds and emphasizing their status as "first-time offenders."[11]

Nevertheless, a new and complex situation has emerged, requiring updated provisions and strict measures to address the implications of AI and deepfake technologies. While not widely recognized by the general public, the issue gained attention when it involved a deepfake video of a well-known Bollywood celebrity Rashmika Mandhana. The incident made headlines, prompting immediate reactions from several Union Cabinet Ministers including the IT Minister. Unfortunately, numerous cases involving the manipulation of images and videos of women, with added derogatory comments often go unreported or remain pending due to a lack of action.[12]

1.1 Research Methodology:

This research will employ a doctrinal legal methodology. The analytical approach will be used to assess the current state of the law and evaluate its effectiveness. A comparative method will be applied to examine whether evidence obtained through cyber forensics holds the same level of admissibility in court as physical documents.

1.2 Mode of Citation:

Bluebook 20th Edition has been followed throughout this project.

1.2 Research Objective:

(i) To find out the role of cyber forensics in combatting cyber crime against women.

(ii) To find out the intricacies in establishing cyber forensic reports in court of law.

1.4 Research Questions:

a) What are the prevalent forms of cyber crimes affecting women in the internet era and how do they impact their safety?

b) What legislative measures currently exist to safeguard women from cyber crimes and how effective cyber forensic have they been in addressing the challenges?

What are the gaps and shortcomings in the existing legislative framework aimed at protecting women from cyber crimes and what are the implications for their safety and empowerment?

1.5 Research Hypothesis:

Despite having legislative measures, even in 20th century women remain most vulnerable due to multifaceted socio-cultural factors and evolving nature of crime. Consequently, there is

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 10 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

a compelling need for comprehensive reforms and new legislative interventions to tackle the challenges faced by women specifically in this digital era from cyber crime. This research may provide comprehensive re- evaluation of the measures required.

1.6 Literature Review:

1.6.1 Hao K in "Deepfake Porn is Ruining Women's Lives: Now the Law May Finally Ban It," has discussed the severe impact deepfake technology has on women's lives. She has brought into light the need for legal action to ban such non-consensual porn creation which creates great social and psychological problems.

1.6.2 B. Vanlalsiama and Nitesh Jha in "Cyber Forensic: Introducing A New Approach to Studying Cyber Forensic and Various Tools to Prevent Cybercrimes," emphasizes that the cyber forensics need advanced tools and techniques. They stressed that for proper combating of cybercrimes, there is a necessity of specialization, certification and education to professionals.

1.6.3 Dr. Anjani Singh Tomar in "Cyber Forensics in Combating Cyber Crimes," pointed out the importance of gathering, analyzing and using digital evidence in bringing cybercriminals to book. She underscored the need for proper handling and preservation of evidence to be admissible in court.

1.6.4 Saswati Soumya Sahu in "Cyber Forensics: Law and Practice in India," concentrates on the requirement of a robust techno-legal framework in cyber forensics. She reviewed relevant case laws and the existing legal infrastructure for dealing with cybercrimes.

1.7 Chapterisation Scheme:

Chapter 1- Introduction with Research issue, objective, hypothesis, literature review.

Chapter 2- Understanding Cyber Crime and Cyber Forensics Chapter 3- Violence based on Gender

Chapter 4- Connection between online and offline violence Chapter 5- Statutes in India to protect women from Cyber Violence

Chapter 6- Recommendations to Enhance Cyber Security Chapter 7- Conclusion

Chapter 8- Bibliography

CHAPTER-2

UNDERSTANDING CYBER CRIME AND CYBER FORENSICS

2.1 What is Cyber Crime?

Cybercrime refers to criminal activities that are carried out using computers, networks, and the internet. It encompasses a broad range of illicit activities that exploit technology for malicious purposes. Cybercrimes can be committed against individuals, organizations, or governments, and they may involve various forms of unauthorized access, data theft, financial fraud, identity theft, hacking, spreading malware, and other malicious activities conducted in the digital realm.

2.2 Importance of cyber laws specifically aimed at the protection of women in today's world:

1. **Rising Cyber Crimes:** The increasing prevalence of cybercrimes, including online harassment, stalking, and non-consensual sharing of intimate content, necessitates legal frameworks that address these evolving challenges.

2. **Online Gender-based Violence:** Women are disproportionately targeted by cyber violence, and the digital realm has become a space where gender-based violence is perpetuated. Specific laws are needed to combat these offenses and ensure the safety of women online.

3. **Global Connectivity:** The interconnected nature of the internet means that cyber threats can transcend geographical boundaries.

4. **Technological Advancements:** Rapid advancements in technology, such as deepfake technology and AI-driven threats, require laws

that keep pace with these developments.

5. **Preservation of Privacy:** Cyber law play a crucial role in safeguarding the privacy of women online. This includes protection against unauthorized access, online surveillance, and the misuse of personal information.

6. **Promotion of Gender Equality:** To propagate the principles of equal rights and protection for women in both physical and digital spaces.

7. **Accountability and Deterrence:** Having specific laws creates accountability for perpetrators of violence against women. Legal consequences serve as a deterrent, discouraging individuals from engaging in such activities.

2.3 Overview of Cyber Forensics:

Cyber forensics is a branch that integrates law and technology to collect, investigate data and present the credible report in the court from legally disputed computers, networks and storage devices.

2.3.1 Tools Used in Cyber Forensics

Cyber forensic analysts utilize a variety of tools and techniques to analyze data that may be encrypted, deleted, or hidden. These tools are selected based on the specific circumstances and nature of the case.

(a) X-Ways Forensics

X-Ways Forensics is a Windows-based software compatible with both 32-bit and 64-bit systems. It is primarily used for recovering files from digital cameras, corrupted files and deleted data.

(b) The Sleuth Kit

The Sleuth Kit is compatible with both UNIX and Windows systems which offers a comprehensive range of forensic tools. It is particularly effective for analyzing disk images, performing in-depth file system analysis and recovering lost data.

(c) SIFT

It has the ability to convert evidence into read-only files. SIFT has malware analysis capabilities. Moreover, as a free and open-source toolkit it provides investigators with a cost-effective and efficient solution for forensic analysis.

(d) EnCase

EnCase is a versatile forensic tool used to gather and examine data from a variety of devices without altering the original evidence whether it is active, latent or archival.

(e) CAINE (Computer Aided Investigative Environment)

CAINE is based on the Ubuntu Linux operating system and integrates a wide range of software and tools which offers a semi-automated process for compiling investigation reports. It conducts investigations in phases such as recovering damaged files, analyzing virus-infected systems and retrieving deleted files.

(f) Forensic Toolkit (FTK)

FTK is used to examine various types of digital information, such as finding deleted emails, extracting content strings, and decrypting encrypted data. It also supports saving digital images in multiple formats and breaks them into segments that can later be reconstructed for further analysis. FTK is known for its powerful capabilities in data processing and forensics.

2.3.2 Standard Phases of Computer Forensic Investigation

Computer forensic investigations typically follow five standardized phases to ensure a systematic and legally compliant approach.

(a) Policy and Procedure Development

Investigators shall adhere to the procedures and protocols set by law enforcement agencies.

(b) Evidence Assessment

This phase involves understanding the nature of the case and determine the type of evidence required. Experts evaluate the specific evidence needed for the crime under investigation to

develop an effective and efficient strategy for data collection.

(c) Evidence Collection

The collection of evidence must be conducted carefully and within legal boundaries to maintain its authenticity and admissibility in court. Experts must ensure the integrity of the data through meticulous planning and adherence to necessary guidelines during acquisition.

(d) Evidence Examination

In this phase, the evidence is analyzed using various tools and techniques to retrieve deleted, encrypted or hidden files. Details such as the time, date and location of data creation or modification are examined to establish a timeline.

(e) Documentation and Reporting

This final phase involves compilation of the findings including the expert opinions into a comprehensive report for the authorities.

CHAPTER-3

CYBER VIOLENCE BASED ON GENDER

3.1 Gender Based Violence:

Gender-based violence is a phenomenon firmly entrenched in gender disparities and remains a conspicuous infringement on human rights across societies. It constitutes acts of violence specifically targeted at individuals based on their gender, affecting both men and women, though women and girls represent the predominant victims. They not only face a higher likelihood of being targeted by cyber violence but also endure severe consequences, encompassing physical, sexual, psychological, or economic harm and suffering.

This encompasses instances of non-consensual intimate image abuse, such as cyber flashing, sextortion, and virtual rape resulting in defamation[13].In my perspective, defamation (or character assassination) is more grave offence than the Homicide because Homicide is assassination of life while defamation is assassination for life.

Research conducted by the World Health Organization reveals that one out of every three women will have encountered some form of violence in her lifetime. Approximately one in ten women are estimated to have already experienced a type of cyber violence from the age of 15 onwards. As internet access becomes essential for economic well-being and is progressively regarded as a fundamental human right, it becomes imperative to guarantee that this digital public space is secure and empowering for everyone, encompassing women and girls[14].

3.2 Challenges In Investigation Of Cyber Violence Against Women And Girls (CVAWG):

1. **Diverse Forms**: CVAWG takes on various forms, with some resembling online extensions of physical world violence, such as cyber harassment or stalking. Additionally, the cybersphere introduces unique forms like non-consensual intimate image abuse or doxing, amplifying the scale of harm compared to physical world violence.

2. **Multiple Cyberspaces:** Perpetrated across various online spaces, CVAWG occurs on social media platforms, messaging apps and discussion sites. The constantly evolving digital environment introduces new technologies, with emerging spaces like the Metaverse becoming platforms for virtual rape and other forms of CVAWG.

3. **Misuse of Information and Communication Technology (ICT) Tools:** A wide array of ICT tools, including smartphones, computers, cameras and other recording equipment are misused for stalking, harassment, surveillance, and control. The broader understanding of technology-facilitated violence includes the entire Internet of Things (IoT), encompassing GPS, smart watches, fitness trackers, smart home devices, spyware and stalkerware.

4. **Varied Perpetrators:** Perpetrators of CVAWG include individuals commonly

associated with gender-based violence, such as relatives, acquaintances, intimate partners, and ex-partners. However, perpetrators can also be anonymous or unacquainted in the online realm for sadism or monetary purposes.

5. Availability of Resources in Open Market: The same resources are used by forensics experts and criminals leading to escape of criminals.

6. **Other:** Race, age, disability, profession, personal beliefs, and sexual orientation are additional factors that can contribute to the experiences of victims of cyber stalking[15].

CHAPTER-4

4.1 THE CONNECTION BETWEEN 'ONLINE' VIOLENCE AND 'OFFLINE' VIOLENCE:

1. **Impact on Victims**

(a) Direct Physical Harm: While digital acts may not always lead directly to physical harm, the emotional and psychological impact on victims can be profound. Online violence can contribute to anxiety, depression, and other mental health issues, which may manifest in offline consequences.

(b) Cyber to Physical Transition: In some cases, online violence may escalate to physical harm. Cyber threats or stalking if left unaddressed then it transits into real-world incidents posing a tangible risk to the safety of victims.[16]

2. Normalization of Violence:

Desensitization: Exposure to online violence can contribute to the normalization of aggressive behaviour, desensitizing individuals to harmful actions. This desensitization may extend to offline interactions, potentially increasing the likelihood of physical violence.

Forms of Cyber Violence Against Women:

4.1.1. Cyber Stalking: This form of stalking utilizes information and communication technology (ICT) means to harass, intimidate, persecute, spy, establish unwanted communication or contact, and engage in harmful behaviours that induce feelings of threat, distress, or overall insecurity in the victim. A study conducted in the UK revealed that more than half (54%) of cyber stalking cases originated from a first encounter in the physical world[17].

4.1.2. Cyber Harassment: This form of harassment is carried out using information and communication technology (ICT) means to harass, impose, or intercept communication, with the intent or impact of creating an environment that is intimidating, hostile, degrading, humiliating, sexually explicit or offensive for the victim due to their gender or a combination of gender and other factors, including race, age, disability, profession, personal beliefs, or sexual orientation etc. 41 % of responding women who experienced cyber harassment felt that their physical safety was threatened. One in two women have experienced reduced self-esteem or loss of self- confidence, stress, anxiety, or panic attacks because of cyber harassment[18].

4.2.3 Online gender-based hate speech: It refers to content disseminated and shared through information and communication technology (ICT) means that:

a) expresses hatred towards women and/or girls due to their gender or a combination of gender and other factors (such as race, age, disability, sexuality, ethnicity, nationality, religion, or profession); and/or

b) propagates, incites, endorses, or justifies hatred based on gender or a combination of gender and other factors (such as race, age, disability, sexuality, ethnicity, nationality, religion, or profession).

This form of hate speech may also involve the distribution and sharing, through ICT means, of violent content portraying women and girls as sexual objects or targets of violence.

Victims may opt to reduce their frequency of posting, moderate their language to minimize provocation, or even deactivate their accounts. Amnesty International notes that this form of

self-censorship has a 'silencing effect', leading to females refraining from actively participating in online debates and meaningful exchanges. Furthermore, since victims often include prominent female figures like politicians, journalists, or sportswomen, online gender-based hate speech directly influences the presence and activities of potential role models for girls aspiring to pursue careers in traditionally male- dominated industries[19].

4.4.4 Non-consensual intimate image (NCII) or Digital Voyeurism : This type of abuse against women and girls pertains to the dissemination or the threat of dissemination through information and communication technology (ICT) means of intimate, private, and/or manipulated images/videos of a woman or girl without the subject's consent. These images/videos may be acquired without consent, manipulated without consent, or obtained with consent but distributed without consent. Motivations for such actions commonly include sexualizing the victim, causing harm, or negatively impacting the victim's life.

The circulation of such images has the potential to devastate victims' educational and professional opportunities, as well as disrupt their intimate relationships. Victims often experience threats of sexual assault, persistent stalking, harassment, termination from employment, and may be compelled to change schools. Regrettably, some individuals, overwhelmed by the distress caused by these situations, have tragically chosen to commit suicide.[16]

Technological advancements are increasingly facilitating the creation of highly realistic image manipulations. Software such as Photoshop and artificial intelligence (AI) tools can be utilized to generate synthetic media, including deepfakes, which convincingly alter or fabricate visual content[20]. The DPS MMS scandal is a very infamous case of where an MMS clip of a school girl in compromising situation was distributed by Alice Electronics of Kharagpur, West Bengal at Bazee.com[21].

Another example is the Delhi Metro CCTV footage leaks case, involving the unauthorized release of CCTV recordings capturing couples engaging intimately in metro stations. The footage, originally recorded by police security cameras, has been leaked on the internet[22].

5. **Identity Theft:** Unauthorized use of personal information online to impersonate or harm a woman.

The **Ritu Kohli Case** marked a historic moment in India as the first reported incident of cyberstalking and identity theft. Mrs. Ritu Kohli filed a complaint with the police against an individual who had been using her identity to engage in online chat on the website http://www.micro.com/, primarily in the Delhi channel, for four consecutive days. Mrs. Kohli's complaint detailed that the imposter not only used her name but also shared her address and engaged in obscene act during the online interactions. Furthermore, the accused intentionally provided Mrs. Kohli's phone number to other users, encouraging them to call her during unconventional hours. As a result, Mrs. Kohli received nearly 40 calls in three days, causing significant disruption in her personal life. In response to the complaint, the police traced the IP addresses involved, conducted a comprehensive investigation, and subsequently apprehended the offender. A case was registered under Section 509 of the Indian Penal Code (IPC). The accused was later released on bail[23].

In the case of **The State of Tamil Nadu Vs. Suhas Katti[20]**, the accused was charged with posting obscene, defamatory, and annoying messages about a divorcee woman in a Yahoo message group. The accused further forwarded emails to the victim, using a false email account opened in her name. As a consequence of the posted message, the victim received annoying phone calls under the false belief that she was soliciting. The accused was found guilty of offenses under Section 469, 509 IPC, and 67 of

the IT Act 2000. The accused was sentenced to undergo rigorous imprisonment for 2 years under Section 469 IPC, along with a fine of Rs. 500/-. For the offense under Section

509 IPC, the accused was sentenced to undergo 1 year of simple imprisonment and to pay a fine of Rs. 500. Additionally, for the offense under Section 67 of the IT Act 2000, the accused was sentenced to undergo rigorous imprisonment for 2 years and to pay a fine of Rs. 4000, concurrently.

6. **Doxing:** Publishing private or identifying information about a woman online without her consent, leading to potential harm.

7. **Online Exploitation:** Exploitative practices online, including trafficking, pornography, or other forms of abuse targeting women.

4.2 Reasons Behind Cyber Crimes Against Women in India:

1. Era of digitalisation
2. Lack of knowledge to join cyber community
3. The transcendental jurisdiction of Internet
4. Allow other to use own account
5. Lack of privacy
6. Not using safety tips
7. Connect with strangers
8. Share personal information and emotion
9. Compare Digital world with Real World
10. Non-reporting due to sociological reasons
11. Unreported cases and underreported degrees of violence
12. Lack of comprehensive legal responses to emerging technologies (AI and deepfakes)

4.3 Proposed remedies to protect women against cyber crimes in India:

(i) Awareness and reporting about cyber crimes

(ii) Grievance Redressal Mechanism and Speedy Investigation

(iii) Strict Statutes

(iv) Hard Punishments

(v) NGOs for therapy and rehabilitation

CHAPTER-5

STATUTES IN INDIA TO PROTECT WOMEN FROM CYBER CRIME:

5.1 Bharatiya Nyaya Sanhita 2023, erstwhile Indian Penal Code, 1860

(i) Section 75 erstwhile 354A: If a man engages in any of the actions of soliciting or asking for sexual favours; displaying pornography without the woman's consent; or making sexually coloured remarks, he shall be held accountable for the offense of sexual harassment. The potential penalties may include rigorous imprisonment for a duration extending up to three years, a fine, or both. For the initial two infractions, the imprisonment or fine may stretch to one year, or both, at the court's discretion.

(ii) Section 77 erstwhile 354 C: 'Voyeurism' is the act of capturing the image of a woman involved in a private act and/or disseminating said image without her consent. To qualify as 'Voyeurism,' the circumstances must be such that the woman would typically expect not to be observed, either by the perpetrator or any other person acting on behalf of the perpetrator. A person convicted under this section is subject to punishment, including fines and imprisonment up to three years for the first conviction and seven years for subsequent convictions.

(iii) Section 78 erstwhile 354D: It introduced a provision addressing stalking which also includes cyber stalking. Stalking is defined as an act where a man follows or contacts a woman despite clear indications of her disinterest in such contact or monitors the cyber activity or use of the Internet or electronic communication

of a woman. A man committing the offence of stalking could face imprisonment for up to three years for the first offence, and shall also be subject to fines. For any subsequent conviction, the individual would be liable for imprisonment up to five years and fines.

(iv) Section 356 erstwhile 499: Defaming a person involves doing an act with the intention of harming the reputation of that individual. Defamation by publishing visible representations of an imputation concerning a woman, when done with the intention to harm her reputation, is punishable with imprisonment for a term that may extend to two years, or with a fine, or both.

(v) Section 351 erstwhile 503: Criminal Intimidation occurs when someone threatens another person with harm to their person, reputation, or property, or to the person or reputation of someone in whom that person is interested. The intent behind the threat is to cause alarm to the individual, compel them to perform an act they are not legally obligated to do, or refrain from doing an act they are legally entitled to do.

(vi) Section 79 erstwhile 509: Any person who utters any word, makes any sound or gesture, or exhibits any object with the intention that such word, sound, gesture, or object be heard or seen by a woman to insult her modesty or intrude upon her privacy may be charged under this section. 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.

5.2 Information Technology Act, 2000

(i) Section 66C of the IT Act establishes identity theft as a punishable offense, encompassing instances of cyber hacking. This provision dictates that individuals who fraudulently or dishonestly use the electronic signature, password, or any other unique identification feature of another person may face imprisonment for a term extending up to three years and may be liable to a fine of up to one lakh rupees.

(ii) Section 66E of the IT Act addresses the violation of a person's privacy. Offenses such as capturing, publishing, or transmitting images of a private area of any person without consent, under circumstances violating their privacy, can result in imprisonment for up to three years and/or a fine.

(iii) Section 67 of the IT Act prohibits and penalizes the publication, transmission, and causing of transmission of obscene content. For a first conviction, the punishment includes imprisonment for up to three years and a fine, while for a second conviction, it extends to imprisonment for up to five years and a fine.

(iv) Section 67A makes the publication, transmission, or causing of transmission of sexually explicit material punishable. For a first conviction, the punishment involves imprisonment for up to five years and a fine, and for a second conviction, it extends to imprisonment for up to seven years and a fine.

(v) Section 67B deals with the publication or transmission of sexually explicit content depicting children. On the first conviction, the offender may face imprisonment for a term up to five years and a fine of up to ten lakh rupees. In the event of a second or subsequent conviction, the penalty may include imprisonment for a term up to seven years and a fine of up to ten lakh rupees.

(vi) Section 72: Penalty for Breach of confidentiality and privacy.

5.3 The Indecent Representation of Women (Prohibition) Act, 2012,

is designed to regulate and prohibit the indecent portrayal of women in various media forms such as advertisements and publications. Additionally, the distribution of material under this Act extends to online platforms, encompassing the portrayal of women over the internet.

5.4 The Digital Personal Data Protection Act, 2023:

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 10 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

This Act is designed to facilitate the processing of digital personal data in a manner that upholds the right of individuals to safeguard their personal information. Simultaneously, it acknowledges the imperative to process such data for lawful purposes. The act also addresses matters connected to or incidental to these primary objectives.

5.5 Bhartiya Sakshya Adhiniyam, 2023

(i) Section 57 includes electronic and digital records in the definition of "primary evidence".

(ii) Section 63(1): **Electronic Records as Documents** Information in an electronic record (printed, stored, or recorded electronically) is deemed a document if certain conditions are met. It is admissible in evidence without needing the original.

(iii) Section 63(2): **Conditions for Admissibility**

(a) The computer/device was regularly used to create or process information for lawful activities during the relevant period.

(b) The information was fed into the device in the ordinary course of business.

(c) The device functioned properly or any malfunction did not affect the accuracy of the record.

(iv) **Certification for Evidence** (Section 63(4)):

(a) A certificate shall accompany the electronic record, stating:

(b) Identification and production details of the record.

(c) Details of devices involved.

(d) Compliance with the conditions of Section 63(2).

5.6 Bharatiya Nagarik Suraksha Sanhita:

(a) Section 176(3): It mandates a forensic expert to collect evidence at the crime scene for offenses that carry a punishment of minimum seven years.

(b) Section 94: Any court or police station incharge may demand the production of electronic communication that may contain digital evidence.

In State (NCT of Delhi) v. Navjot Sandhu,2[24] Hon'ble Supreme Court initially ruled that electronic records could be admitted as evidence even without a certificate under Section 65B(4) of the Indian Evidence Act. However, this decision was later overruled in Anvar PV v. PK Basheer [25]which reinstated the mandatory requirement of Section 65B certificate for the admissibility of electronic records.

CHAPTER-6

RECOMMENDATIONS TO ENHANCE CYBER LAWS IN ORDER TO PROSECUTE CRIMINALS AND ADMISSIBILITY OF CYBER FORENSIC EVIDENCE

1. **Strengthening Laws Against Cyber Stalking and Harassment:** Introduce more stringent penalties for cyber stalking and harassment, considering the psychological and emotional impact on victims. Clearly define and include specific provisions addressing cyber stalking, making the legal framework more comprehensive.

2. **Stricter Measures for Non-consensual Image Sharing:** Enhance penalties for the unauthorized sharing of intimate images without consent, commonly known as revenge porn or non-consensual intimate image abuse Broaden the definition of such offenses to encompass various forms of digital media and technological advancements.

3. **Heightened Punishments for Online Gender-based Hate Speech:** Introduce specific provisions to tackle online gender-based hate speech, recognizing the harmful impact it has on the targeted individuals. Collaborate with online platforms to monitor and remove content that incites hatred based on gender, race, or other factors.

4. **Inclusion of Cyber Education in School Curriculum:** Integrate cyber education into the school curriculum to empower young individuals with the knowledge and skills needed for responsible and safe online behaviour. Foster awareness about the consequences of cybercrimes and the importance of respecting others' digital rights.

5. **Establishment of Cyber Cells Dedicated to Women's Safety:** Create specialized cyber cells within law enforcement agencies focused on addressing cybercrimes against women. Provide training to law enforcement personnel on handling cybercrime cases with sensitivity and understanding of gender-related issues.

6. **Streamlining Reporting Mechanisms:** Develop user-friendly and accessible online portals for reporting cybercrimes against women, ensuring swift and efficient action. Facilitate a victim-friendly environment during investigations, minimizing re-traumatization.

7. **International Collaboration for Cybercrime Prevention:** Strengthen collaborations with international agencies to address cross-border cybercrimes, especially those targeting women. Participate in information sharing and joint efforts to apprehend and prosecute offenders operating beyond national boundaries.

8. **Regular Updates and Amendments:** Establish a mechanism for regular review and updates to cyber legislation, ensuring it remains adaptive to evolving cyber threats and technologies. Consider input from experts, advocacy groups, and affected individuals during the amendment process.

(a) Integration of Innovative Cyber Crimes:

The landscape of cybercrime has undergone a significant transformation, rendering the prevailing modus operandi from 2008 obsolete. Section 43 of the IT Act addresses certain cybercrimes, such as hacking, introduction of malicious programs, malware attacks, and source code breaches. However, Section 43 imposes civil penalties, lacking effective criminal deterrence. Although Section 66 penalizes specific cybercrimes mentioned in Section 43, the prescribed punishment is only three years of imprisonment, rendering the offense bailable. Contemporary cybercrime includes ransomware attacks, sextortion, privacy infringements by malicious programs, cyber warfare on critical infrastructure, malicious campaigns on social media, Darknet crimes, online cryptocurrency-related offenses, online gambling syndicates, spoofing, scamming, skimming attacks, etc.

These emerging cybercrimes are not explicitly addressed in the Information Technology Act. It is crucial to introduce separate sections for each category of cybercrime in the amended Act, making them cognizable and non-bailable, with a minimum punishment exceeding seven years. This step aims to prevent the application of pre-arrest notices under Section 41 CRPC to aid cybercriminals, fostering a forward-looking and visionary ITA that aligns with contemporary challenges and serves as a deterrent to modern cybercrime syndicates.

9. The Information Technology Act, in its current form, exhibits a centralized structure with limited devolution of authority to State Governments. Sections 67-C, 69A, and 69B of the IT Act grant exclusive authority to the Central Government in matters of preservation, retention of information, blocking offensive content, and monitoring internet data for cybersecurity. To address contemporary needs, powers for blocking offensive content, monitoring internet data and accessing information necessary for investigating cognizable offenses should be devolved to authorized State Government agencies as well. This decentralization will enhance intelligence collection, improve cybercrime investigation and align authority with the responsibilities entrusted to state governments.

10. The IT Act's current structure places excessive emphasis on higher- ranked officers for investigating offenses. Sections 78 and 80

stipulate that only officers of the rank of inspector and above can investigate cyber offenses and exercise powers of search and seizure. This provision poses challenges due to the shortage of higher-ranked officers, while younger sub inspectors are often better trained in investigating cybercrimes. Therefore, authorizing police officers of the rank of sub-inspectors and above to investigate cyber offenses is strongly recommended.

11. Law enforcement agencies dealing with cybercrime face a significant challenge – non co-operation from various intermediaries such as social media platforms, banks, crypto exchanges, server owners, etc. The reluctance of intermediaries to provide relevant information hampers investigations. It is essential to establish lawful standard operating principles (SOPs) and incorporate legal provisions in the IT Act, making it mandatory for intermediaries to cooperate with law enforcement agencies. Although Section

69 of the ITA mandates intermediaries to assist the government in interception, monitoring, or decryption, it is often flouted. Clarifying that providing relevant information to law enforcement agencies in a prescribed format is a lawful duty of the intermediary, free from personalized yardsticks, will expedite the acquisition of information for cybercrime investigations.

12. Cybercrime has become the primary organized crime syndicate globally. For a stronger deterrence, more stringent provisions should be introduced in the Information Technology Act. Currently, many cybercrimes specified in the IT Act are bailable, with a maximum imprisonment not exceeding three years. Offenses like hacking, pornography, malware attacks, identity theft, online cheating, impersonation and privacy breaches lack sufficient deterrence. Therefore, all cybercrimes should be made cognizable and non-bailable to proactively prevent their commission.[26]

CHAPTER-7

7.1 Conclusion: Countless women and girls globally face targeted gender- based violence, transcending geographical, racial and cultural divides. The Internet's pervasive influence, coupled with the rise of technology hasintroduced new challenges and these are being addressed by India through legislative acts like the I.T Act, BNS, BNSS, BSA and D.P.D.P Act effectively. But new incident like "bullibai.github.io" displayed manipulated images of Indian women highlighting the need for updated provisions amidst AI and deepfake threats. Hence, to effectively address the challenges posed by cybercrimes, it is imperative to enhance the existing cyber laws and cyber forensic mechanisms. Strengthening the legal framework with stringent penalties, decentralized powers, mandatory cooperation from intermediaries and regular amendments to legislation will provide a robust system for combating modern cyber threats. Moreover, integrating specialized training, user-friendly reporting mechanisms and international collaboration in filed of cyber forensics will empower law enforcement to efficiently investigate and prosecute cybercrimes. By adopting these measures, the justice system can ensure a safer digital environment and act as a strong deterrent against the evolving landscape of cyber offenses particularly victimising women.

7.2 Bibliography:

A. Books, Articles, Journals, Research Papers, Speech, Interview

1. Ban Ki-moon, U.N SECRETARY GENERAL, 2008, available at https://en.unesco.org/sites/default/files/genderreport2015final.pdf

2. European Institute for Gender Equality, https://eige.europa.eu/sites/default/files/cyber_violence_against_women_and_girls_key_terms_and_concepts.pdf

3. Council for Europe, https://rm.coe.int/grevio-rec-no-on-digital-

violence- against-women/1680a49147

4. European Institute for Gender Equality,https://eige.europa.eu/gender- based-violence/cyber-violence-againstwomen

5. Sugiura, L. (2021). The Incel Rebellion: The Rise Of The Manosphere And The Virtual War Against Women, Emerald Group Publishing Bingley, https://www.emerald.com/insight/publication/doi/10.1108/9781839822544

6. Short, E., Linford, S., Wheatcroft, J. M., and Maple, C. (2014), 'The

impact of cyberstalking: the lived experience – a thematic analysis', Studies in Health Technology and Informatics, Vol. 199, pp. 133–137 available at

http://dx.doi.org/10.3233/978-1-61499-401-5-133

7. Maple, C., Short, E., and Brown, A. (2011), Cyber Stalking in the United Kingdom: An analysis of the ECHO pilot survey, University of Bedfordshire, U.K., https://uobrep.openrepository.com/handle/10547/270578

8. Amnesty International (2017), Amnesty reveals alarming impact of online abuse against women, https://www.amnesty.org/en/latest/press-release/2017/11/amnestyreveals-alarming-impact-of-online-abuseagainst-women/

9. Amnesty International (2018), Amnesty International, London,

https://www.amnesty.org/en/latest/news/2018/03/online-violence-against-women- chapter-2

10. Hao, K. (2021), 'Deepfake porn is ruining women's lives. Now the law may finally ban it', MIT Technology Review,

https://www.technologyreview.com/2021/02/12/1018222/deepfake-revenge-porn-coming- ban/

B. News and links

1. THE STATESMAN, https://www.thestatesman.com/india/can-be-taken- to-court-on-rashmika-mandhanasdeep-fake-video-it-minister-warns-online- platforms-1503238316.html

2. https://en.wikipedia.org/wiki/DPS_MMS_scandal

3. Yashashvi Yadav, https://timesofindia.indiatimes.com/blogs/voices/anachronistic- cyberlegislation-related-to-cyber-crimes-needs-upgradation/

C. Acts of India:

1. Indian Penal Code, Act No. 45 of 1860 (India)

2. Information and Technology Act,2000.

3. The Digital Personal Data Protection Act, 2023

D. Cases:

1. Aumkareshwar Thakur vs NCT of Delhi, W.P.(Crl.) No.-000027 / 2022 (SC)

2. Ritu Kohli Case

3. The State of Tamil Nadu Vs. Suhas Katti

LIST OF CASE:

Aumkareshwar Thakur vs NCT of Delhi, W.P.(Crl.) No.-000027 / 2022 (SC).

Ritu Kohli Case

E. The State of Tamil Nadu Vs. Suhas Katti, C No. 4680 of 2004

ENDNOTES

2 Ban Ki-moon, U.N SECRETARY GENERAL, 2008,(last visited Feb 25, 2024) available at https://en.unesco.org/sites/default/files/gender report2015final.pdf .

3 The Information Technology Act, No. 21, Acts of Parliament,2000 (India).

4 The Digital Personal Data Protection Act, No. 22, Acts of Parliament,2023 (India).

5 Indian Penal Code, Act No. 45 of 1860

6 Criminal Procedure Code,1973, No. 2, Acts of Parliament, 1974 (India)

7 Indian Evidence Act, Act No.1 of 1872

8 Bharatiya Nyaya Sanhita, No. 45, Acts of Parliament,2023 (India)

9 Bharatiya Nagarik Suraksha Sanhita, No. 46, Acts of Parliament,2023 (India)

10 Bharatiya Sakshya Adhiniyam, No. 47, Acts of Parliament,2023 (India)

11 Aumkareshwar Thakur vs NCT of Delhi, W.P.(Crl.) No.-000027 / 2022 (SC).

12 THE STATESMAN, https://www.thestatesman.com/india/can-be-taken-to-court-on- rashmika-mandhanasdeep-fake-video-it-minister-warns-online-platforms-1503238316.html (last visited November 6,2024)

13 Council for Europe, https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147 (last visited March 4, 2024)

14 European Institute for Gender Equality,https://eige.europa.eu/gender-based- violence/cyber-violence-againstwomen (last visited March 3, 2024)

15 Sugiura, L. (2021). The Incel Rebellion: The Rise Of The Manosphere And The Virtual War Against Women. Emerald Group Publishing Bingley,

https://www.emerald.com/insight/publication/doi/10.1108/9781839822544

16 Short, E., Linford, S., Wheatcroft, J. M., and Maple, C. (2014), 'The impact of cyberstalking: the lived experience – a thematic analysis', Studies in Health Technology and Informatics, Vol. 199, pp. 133–137 available at http://dx.doi.org/10.3233/978-1-61499-401- 5-133

17 Maple, C., Short, E., and Brown, A. (2011), Cyber Stalking in the United Kingdom: An analysis of the ECHO pilot survey, University of Bedfordshire, U.K., https://uobrep.openrepository.com/handle/10547/270578 (last visited March 2, 2024)

18 Amnesty International (2017), Amnesty reveals alarming impact of online abuse against women, https://www.amnesty.org/en/latest/press-release/2017/11/amnestyreveals-alarming-impact-of-online-abuseagainst-women/ (last visited March 2, 2024)

19 Amnesty International (2018), Amnesty International, London,

https://www.amnesty.org/en/latest/news/2018/03/online-violence-against-women- chapter-2 (last visited March 2, 2024)

20 Hao K. (2021), 'Deepfake porn is ruining women's lives. Now the law may finally ban it', MIT Technology Review,

https://www.technologyreview.com/2021/02/12/1018222/deepfake-revenge-porn-coming- ban/ (last visited March 2, 2024)

21 https://en.wikipedia.org/wiki/DPS_MMS_scandal (last visited March 2, 2024)

22 http://zeenews.india.com/news/nation/porn-mmses-from-delhi-metro-

cctvfootage_860933.html (last visited March 1, 2024)

23 Dr. Sapna Sukrut Deo, CYBERSTALKING AND ONLINE HARASSMENT: A NEW CHALLENGE FOR LAW ENFORCEMENT,

https://docs.manupatra.in/newsline/articles/Upload/FDF5EB3E-2BB1-44BB-8F1D-9CA06D965AA9.pdf (last visited March 1,2024)

20 CC No. 4680 of 2004

24 2005 INSC 333

25 AIR 2015 SUPREME COURT 180

26 Yashashvi Yadav, https://timesofindia.indiatimes.com/blogs/voices/anachronistic- cyberlegislation-related-to-cyber-crimes-needs-upgradation/ (last visited on March 2,2024)