AI-driven Cyber Crimes against Indian Career Women: Probing Solution in Universal Human Values

Dr Sadhan Kumar Dey[1] & Dr. Alice Dey[2]

Abstract- Artificial Intelligence (AI) has become an unfortunate tool in the hands of 'White Collar Crime' which is better known as Cyber Crime in India. In recent times National Crime Record Bureau of India has recorded an increasing number of Cyber Crimes against women in India Most of these crimes are Artificial Intelligence (AI) -driven. As a result of technological developments in artificial intelligence, with an emphasis on preventing cybercrime and strengthening the laws that protects women's rights. The increasing prevalence of cybercrime poses a multiplicity of challenges for international legal frameworks and law enforcement agencies. India, among the digital economies growing at the fastest pace, needs to fortify its legal defense against cyberattacks promptly. In this respect, technologies powered by artificial intelligence (AI) provide promising substitutes by giving law enforcement agencies state-of-the-art tools for threat detection, evidence processing, and proactive crime prevention. The suggested methodology takes a broad approach, utilizing AI-enabled technologies like data analytics, machine learning, and natural language processing. With the use of these technologies, enormous volumes of data from various sources—such as social media, online forums, and digital communication channels—are analyzed in order to look for trends that can point to cybercrimes directed at women. Criminal administration of Justice has fallen flatten times of need as AI-driven mechanism changes its modus Operandi every time legal measures are made stringent. Even the Stringent laws have failed to control cyber-crimes against women. The present researchers have found hope only in proper teaching of Universal Human Values[3] (hereafter referred to as UHV).

Keywords: AI-driven; Cyber Crimes; Indian Career Women; Finding Solution; Teaching; Universal Human Values (UHV);

I. INTRODUCTION

Cyberspace is the term for the computer-generated environment that is the internet, and cyber laws are the regulations that control it. These laws apply to all drug users in this area since they entail a certain level of global governance. It entails tracking a person's online activities by sending out notifications on boards that they visit, breaking into their converse- apartments, sending them a barrage of emails, and so on. Generally speaking, the snooper has no legitimate reason for communicating and only wants to cause emotional distress to others. The digital age has opened up previously unheard-of avenues for creativity and connectedness, but it has also created a pathway for new kinds of criminal activities, especially in cyberspace.

All India Council of Technical Education (AICTE) and University Grant Commission (UGC) have started teaching UHV in Higher Education. The teaching Modules consist of the following basic domains[4]:

a. "Harmony in the Individual"
b. "Harmony in the Family"
c. "Harmony in the Society"
d. "Harmony in Nature & Existence"

There are different gradations of the course with reference to in depth focus.The present article will showcase a study done as a pilot work to study the Efficacy of teaching UHV. It has been observed that students who had undergone the UHV training Course have grown human -human feelings for maintaining sustainable harmony in the society.

[1] Professor of English, Dept. of Engineering Science and Management.RCCIIT Kolkata India
[2] Assistant Professor, Dept. of Law (IIIJS), University of Engineering & Management,, Kolkata, India
[3] As prescribed by AICTE and UGC for Higher Education in India
[4] Garg et al. Human Values & Professional Ethics. (First Edition) See the Conclusion for application of these Modules in Higher Education in India

II. AI-DRIVEN CYBER CRIMES AGAINST WOMEN IN INDIA

The most usual kind of cAI-driven cybercrime against women in India is revenge porn. It entails the unapproved dissemination of sexually explicit photos or movies, frequently done as a form of blackmail or retaliation. In the last year, the number of revenge porn cases in India has increased by 148%, according to research published by the Cyber Peace Foundation. Pornography that seeks revenge can cause serious psychological and emotional harm in addition to harming a woman's reputation. The ubiquitous character of cybercrime surpasses national boundaries and impacts people, institutions, and even governments. We are depending more and more on technology in our daily lives, which makes us more vulnerable to hacker attacks. Due to its large population and quickly expanding digital infrastructure, hackers frequently target India in their quest to carry out identity theft, data breaches, and other heinous crimes.

In addition, the public's ignorance of cybersecurity and the absence of strong cybersecurity norms render them more vulnerable to cyberattacks. Nevertheless, there are still chances for creativity and teamwork in spite of these obstacles. Initiatives including public-private partnerships, cybersecurity awareness campaigns, and capacity building greatly strengthen India's digital ecosystem's defence against cyberattacks. In a nutshell in order to protect India's digital future, combating the complex nature of cybercrime requires a comprehensive approach that incorporates judicial modifications, technology breakthroughs, and proactive engagement from all parties.

III. RESEARCH METHODOLOGY - USED

In the field of cyber security, research and development are being supported. Working together, academia, research centers, and business sectors promote creativity , cybersecurity technology development, and the identification of cutting-edge defence against online attacks. All of these actions are intended to improve incident response capabilities, fortify India's cybersecurity ecosystem, and establish a safe online space for citizens, companies, and governmental organizations.

To keep abreast of the constantly changing danger landscape of cybercrime, sustained effort, investment, and awareness are crucial. Apart from the traditional approach there are reflections of some data sets collected through-questionnaire and cross-checked with Datasets collected from" National Crime Records Bureau and Statistical" addressing the time frame (2020-2022) to address some innate research questions on women Security, Women empowerment, and Victim safety for accessing easy help with the emergence of Artificial Intelligence and their role in combating these virtual Fraudsters. Reports indicate a significant rise in anonymous complaints about computer-based crimes against women and children in India.

A pilot Survey report has also been consulted for validating the findings of the Effect of UHV training among Computer Science and Information Technology Students of a popular Government University of West Bengal in India. The National Cyber Crime Reporting Portal has seen a surge in such complaints, increasing from 17,460 in 2020 to 56,102 in 2022.

However, due to the anonymity of these complaints, few are followed through with FIRs, leading to a lack of substantial legal action[5]

AI-driven Tools and Techniques - Used for Committing Cyber Crimes against Career Women
The following tools and techniques are being used to induce AI-driven ways to commit cybercrimes against career women in India:

A. Machine Learning: Within the field of artificial intelligence, machine learning is the area of study dedicated to creating models and algorithms that allow machines to learn and make decisions without explicit programming. It entails using a sizable dataset to train a model in order to identify trends and produce precise

[5] Srivastava, Amitabh; "Why are rising anonymous complaints of cybercrime against women, children a worry?" India Today; Published on Feb 27, 2023;

predictions or classifications.

B. Data Analysis: The process of examining, purifying, converting, and structuring data in order to find relevant information, make inferences, and aid in decision-making is known as Data Analysis. It entails obtaining and examining vast amounts of data in order to spot trends, patterns, and anomalies that can be used to comprehend and stop cybercrime.

C. Predictive Modeling: The act of developing a statistical or machine learning model to forecast Future events based on past data is known as predictive modeling. It entails applying algorithms and methodologies to identify trends and forecast probable cybercrime events, allowing for pre-emptive steps to stop Such occurrences from happening.

D. Blockchain technology: Blockchain technology is a digital ledger that may be used to store and transfer data that is transparent, safe, and decentralized. Blockchain technology has the potential to stop online crimes like identity theft and financial fraud. Sensitive data can be safely stored using blockchain technology, preventing data breaches.

E. Two-factor authentication: Online accounts can be kept safe from unwanted access by using two-factor authentication.

F. Encryption: Passwords and other private information can be safeguarded via encryption.

G. Firewalls: It is possible to stop illegal access to computer networks and systems by using firewalls.

H. Anti-malware software: blockchain, artificial intelligence, and machine learning can be employed. It's crucial to remember, though, that technology cannot end computer-based crimes against women on its own. Malware infections can be found and stopped with anti-malware software.[6] [7] India's computer-based crimes against women could be significantly reduced with the use of technology.

IV. SURVEY OF RECENT STUDIES RELATED TO AI-DRIVEN CYBER CRIMES AGAINST INDIAN WOMEN

To avoid and lessen computer-based crimes, technology technologies such as

Mark Austin Walters, Jessica Tumath in The Modern Law Review, Vol. 77, stated “While social media and the internet are undoubtedly beneficial to individuals and society at large, they also serve as a particularly strong breeding ground for remarks that could be considered defamatory.”[8]

Lisa Sharland at Genevieve Feely Australian Strategic Policy Institute (Jun. 1, 2019) stated “Email is a wonderfully efficient and user-friendly form of communication. Instead of being textual interaction, it is quite similar to spoken discussion.”[9]

“Pornography has the most potent power to completely ruin a person, their intellect, their future, their potential, and society.” -Kamlesh Vaswani, Activist.[10]

RAVI KRISHNANI in the World Policy Journal, pointed out that “Cybercrime against women started to increase in frequency. Since the entire nation was under lockdown, criminals were unable to physically harm the victim; instead, they started to torture them mentally and emotionally.”[11]

[6] Canadian Centre for Justice Statistics. (2021). Cybercrime.
[7] Canadian Survey of Cyber Security and Cyber Crime-2023
[8] Bector P, Professor A, BPR College, et al. The Harmful Effects of Cyberbullying on Teenagers – A common study. *Global Journal for Research Analysis* 2012; 3: 1–3.
[9] Sheinov VP, Belarusian State University. Cyber Bullying in youth environment: Origins and effects. *The Herzen University Studies: Psychology in Education*. DOI: 10.33910/herzenpsyconf-2019-2-73.
[10] Call to curb rise in violence against women. *Human Rights Documents Online*. DOI: 10.1163/2210-7975_hrd-9943-2016039
[11] Mansfield-Devine S. Significant rise in cybercrime against public sector organisations. *Computer Fraud & Security* 2012; 2012: 1–3

Sanjay Goel stated "Relationships because during this time period, the majority of women used social media websites and one or more online platforms for occupational, recreational, and educational purposes."[12] [13]

Brandon Gaskew in *Third Way*: "Criminals have benefited from the fact that most women during this time were using social media websites and one or more online platforms for recreational, professional, and educational objectives."[14]

Gandhi (2012) examined a variety of online crimes and determined the most common categories, including hacking, phishing, vishing, cross-site scripting, cyberstalking, and bot networks.

Goyal (2012) concentrated on the various ethics involved in cybercrimes and explored how all ethics, including those related to business, law, biotechnology, medicine, engineering, and computers, that apply to all related crimes also apply to cybercrimes.

Vinit Kumar Gunjan, Amit Kumar and Sharda Avdhanam (2013) provides an overview of cybercrimes and criminals in India, concluding that these crimes are more terrible and destructive than traditional crimes, and every country needs to be aware of the laws, criminal psychology, and cybercrime regulations that are related to them.

Impact on Career Women Victims due to Cyber Crimes

The digital era has made cybercrime a growing menace to people. People are more susceptible to financial loss, identity theft, mental distress, and reputational harm as a result of the sophistication of cyberattacks.

Financial loss or loss of income: Financial loss is one of the most typical consequences of cybercrime on people. Cybercriminals frequently employ a variety of techniques, including phishing, hacking, and malware, to obtain a person's financial data, including passwords, bank account information, and credit card numbers. Unauthorized transactions may lead to the loss of money, from which it may be impossible to recoup.

Identity theft: A major aftereffect of cybercrime on people is identity theft. Social security numbers, driver's license numbers, and dates of birth are examples of stolen personal information that cybercriminals can use to register new accounts, obtain loans, and carry out other fraud schemes in the names of real people. Financial loss as well asserious legal and administrative difficulties in regaining the person's identification may arise from this.

Emotional trauma: Cybercrime not only involves money loss and identity theft, but it can also result in emotional distress. Cybercrime victims frequently experience dread and anxiety because they feel violated and unprotected.
An individual's mental health may be negatively impacted for some time by this, particularly if they feel alone and unable to get assistance.

Loss of reputation: Last but not least, cybercrime can harm a person's reputation. Cybercriminals may publish embarrassing or harmful content online using information they have stolen, which damages their credibility and undermines public confidence. Reputational harm can have particularly negative implications in professional contexts, such as job loss or trouble finding new employment.

Increase in cyberbullying and harassment: Cyberbullying and harassment can rise as a result of cybercrime. Cybercriminals can target individuals and organizations by disseminating offensive remarks and destructive content via technology. Relationship and reputational harm as well as emotional and psychological distress may arise from this. In addition

[12] Mansfield-Devine S. Significant rise in cybercrime against public sector organisations. *Computer Fraud & Security* 2012; 2012: 1–3

[13] Choudhary R. Cyberspace and Women- Dimensions of Cybercrime against Women in India. *Design Engineering* 2022; 73–80

[14] Rai K, Kaur B, Sardana S. Awareness of Cybercrime against Women among Students of Higher Educational Institutes in Delhi. *Performance Management* 2020; 163–174

to harming mental health, Cyberbullying and harassment can cause anxiety and sadness.
Furthermore, disinformation can be disseminated by cybercrime, which can have detrimental social and political effects.

V. LAWS NECESSARY TO COMBAT THE EVOLVING THREAT OF CYBER CRIMES

A legislative framework to combat cybercrimes against women has been developed in India as a result of the increase in these crimes. To begin with, the Indian legal framework consists of a number of laws and regulations, such as the Information Technology Act of 2000, the Indian Penal Code, or the Bhartiya Nyaya Sanhita. Let's examine these rules and legislation in more detail.

VI. CONSTITUTIONAL LIABILITY

It is a gross breach of someone's right to privacy to break into their private property or take their creative works. The "right to privacy" is one of the essential rights granted to Indian people, although it is not expressly stated in the constitution; rather, it is protected by the Indian Penal Code.
Every human being has a fundamental desire for privacy, which is to set boundaries around oneself that prevent others from entering.
Interference or intrusion into another person's private life is forbidden by the right to privacy. The Indian Supreme Court[15]t has unequivocally stated in its rulings that the right to privacy is a basic freedom protected by Article 21 of the Indian Constitution.
Therefore, the right to privacy falls under the broad provisions of Article 21 of the Indian Constitution.
Thus, in the event of cybercrime involving an individual's private property or personal belongings, the accused may be accused of violating Article 21 of the Indian Constitution, and the required penalty may be applied against the accused.

CONCLUSION

India is experiencing an increase in cybercrimes targeting women, hence it is critical that women take precautions to avoid becoming victims. a few recommended actions that women should adhere to in order to shield themselves against cybercrimes. Digital Media often suggest the ways for preventing AI-driven attacks as shown below:

Using Strong Passwords: Using secure passwords is one of the easiest yet most effective strategies to defend yourself against online fraud. Make sure your passwords contain a combination of capital and lowercase letters, digits, and special characters, and that they are at least 12 characters long. Steer clear of using obvious passwords like your birthdate, pet's name, or your name.

Keeping Personal Information Private: When disclosing personal information online, especially on social media, exercise caution. Don't post your home address, phone number, or other private information online. Phishing emails and phone calls requesting personal information should also be avoided.

Using Social Media with Diligence: The use of social media might have drawbacks. It might assist you in maintaining relationships with friends and family, but it can also serve as a haven for cybercriminals. Being wary of the people one adds as friends and refrain from posting private or delicate images online.[16]

Using Two-Factor Authentication: One's online accounts are further secured by two-factor authentication, which requires two forms of authentication in addition to your password—for example, a code delivered to your phone. This feature is available on a wide range of well-known internet services, such as social media sites and email providers.

Keeping Software Up-to-Date: Maintain the most recent versions of all of the software/s, including one's operating system and antivirus programs. Security patches that fix vulnerabilities that cybercriminals

[15] Dey, Sadhan Kumar & Dey. Alice. Legacy of Empowering Indian Women: Scrutinizing Major Constitutional Provisions and Legislations on Women's Rights in Context. Viswabharati (2023)

[16] Gupta, S., & Kapoor, M. (2018). Cyber Crime in India: An Empirical Study on Cyber Crime Awareness among Women. International Journal of Management Studies, 5(4), 106-111.

could exploit are frequently included in software updates.

Using Antivirus Software: Malware and other dangerous software can be detected and prevented from infecting one's device with the aid of antivirus software. Installing and Maintaining up-to-date reliable antivirus software is important.

Reporting Incidents: It is essential that one should report the authorities of any cybercrime that you are a victim of. Reporting events can assist law enforcement in finding and apprehending cybercriminals as well as aid in the prevention of future crimes.[17]

Let us refer once again how the major Modules have been made teachable and practically available for experiential validation:

Harmony in the Individual: Harmony is referred to the state of happiness and bliss that is ever present in the individuality of the students and the teacher.
Once such happiness is reached through the method of discovery of the 'inner Self" of the teacher and taught in higher education.
Harmony in the Individual can be maintained through a balanced approach towards maintenance of co-existence between the 'Self' and the 'Body'.

Harmony in the Family: Harmony in the Family can be maintained through a balanced approach towards maintenance of co-existence between/among all the 'Individual Members' of a given family.

"Harmony in the Society: Harmony in the Society can be maintained through a balanced approach towards maintenance of co-existence among all the 'Families living in a given Society.

Harmony in Nature & Existence: Harmony in the Nature & Existence can be maintained through a balanced approach towards maintenance of co-existence among all the Societies
Thus, the set of Universal Human Values (UHV) is the only option open to technical brains of India. for providing "Guidance" to the youth so that they can understand the implications of value-based education and value-based living. Once the youth understand that value-based living can guarantee Peaceful co-existence the tendency of misusing Ai-driven gadgets for committing cybercrimes against career women in India will wither away.

[17] *Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector; UNODC* /CCPCJ/EG.4/2013/2*;*

REFERENCES

[1] Dey, Sadhan Kumar & Dey. Alice. Legacy of Empowering Indian Women: Scrutinizing Major Constitutional Provisions and Legislations on Women's Rights in Context. Viswabharati (2023)

[2] Gupta, S., & Kapoor, M. (2018). Cyber Crime in India: An Empirical Study on Cyber Crime Awareness among Women. International Journal of Management Studies, 5(4), 106-111.

[3] Mansfield-Devine S. Significant rise in cybercrime against public sector organisations. *Computer Fraud & Security* 2012; 2012: 1–3

[4] Rai K, Kaur B, Sardana S. Awareness of Cybercrime against Women among Students of Higher Educational Institutes in Delhi. *Performance Management* 2020; 163–174

[5] Garg et al. Human Values & Professional Ethics. (First Edition) See the Conclusion for application of these Modules in Higher Education in India

[6] Choudhary R. Cyberspace and Women-Dimensions of Cybercrime against Women in India. *Design Engineering* 2022; 73–80

[7] Srivastava, Amitabh; "Why are rising anonymous complaints of cybercrime against women, children a worry?" India Today; Published on Feb 27, 2023

[8] Dey, Sadhan Kumar & Dey. Alice. Leveraging AI in Prevention and Protection of Women Against Cybercrime in India: A Paradigm Shift of Criminal Law in the Making. Springer Nature Singapore Pte Ltd. 2025

[9] Dey, Sadhan Kumar. Pedagogic Dynamics of Peace Strategies in Economic Development: Applying Universal Human Values in Conflict Management. Emerald Publishing Limited UK 2025