



Emerging AI Based Crimes & Cybercrime Laws: Addressing Digital Harassment & Ethical Concerns

¹Shalu Mehta, ²Venoo Rajpurohit

¹ Research Scholar, Department of Law, Suresh Gyan Vihar University, Jaipur, India

² Head of the Department, School of Law, Suresh Gyan Vihar University, Jaipur, India

Abstract- In today's world, as we can see, there is rapid advancement in artificial intelligence. It has also introduced many transformative reforms across various industries and given rise to many problems and new complexities in the form of cybercrime, particularly in the area of digital harassment, where one individual can harass another with automated messages. This paper will explore the interaction of AI technology with existing cyber laws, explain the need for new laws, and examine the factors that lead to harassment and the ethical concerns arising from the misuse of technology. This paper outlines the challenges in the existing laws and gives recommendations for updating cyber laws by reforming them and addressing ethical guidelines, including punishment for cyber offenders and protection for victims in the age of AI.

Keywords: Artificial Intelligence; Digital-Harassment; Traditional Laws; Automation; Offence; Offender; Victim; Cyber-crime; Deep fake; Psychology; Accountability; Punishment

1. INTRODUCTION

1.1 Background & Motivation

As we know the technology advances rapidly the AI has also revolutionized in various sectors. Such sectors include healthcare, finance, education and many more. However, all this new techniques and innovations comes with some new adversity and challenges particularly the digital security and ethics has been questioned and one of the most important and emerging issue from that technology in AI is the crimes that are AI based which encompasses of a wide range of illegal activities driven to facilitate by the AI [1]. These crimes are not only a product of hacking techniques but it includes some other forms of Cyber-crime of despite of hacking. Many new crimes emerge that is a digital harassment sometime, fake exploitation and algorithm manipulations can be made and fishing attacks so certain crimes are also immersed with the use of AI [2].

And at the core of this concern digital harassment is increasing day by day which take forms of cyber- crime with the use of AI tools for some malicious purpose or illegal activities. The harassment which are AI driven can imbibe in many forms from

personalized online threads to creation of any harmful content and the content in written showcase the intermediate question and harmful activities towards the individual and this kind of abuse is particularly so automated, scaled in personal life of the victim, making it harder for the traditional (existing) cyber-crime laws to keep this up and on a right track [3].

As, we find the increment in the cyber-crime activities the existing laws and legal frameworks and ethical guidelines are not complete enough to provide punishments for all kind of cyber laws and cyber-crimes and to provide the detailed explanations and complete awareness for the cyber-crime with the use of AI [4-6]. Sometimes it's not easy to find out from where the problem has raised or from where the person is hacked as the connections are not so clearly seems visible and connected that one can identify from where this problem emerge and what is actual root cause of this problem. So, the legal framework for this has to be stronger and faster to match the pace of technology and more ethical guidelines relating to use of AI and cybercrime should be made correctly and the victims should be protected [7-9].

The paper mainly aims to address the issue related to AI based crimes and the digital harassment which an individual face. Paper provides a deep analysis and evaluation of existing



cybercrime laws and suggesting the ways how guidelines can strengthen in the legal responses or any further laws that are need to be made regarding the AI based cybercrime. What problems faced in to-day's digital era? What challenge lies in crafting a regulatory, discipline frame work against AI crimes? What measures government can adapt complexities of AI and for its potential misuse. Also, we have to protect the right of individual and simultaneously the freedom to use the digital landscape without any fear should also be imbibed among the humans and how we can navigate all these concerns regarding AI based crimes and digital harassment that need to be properly evaluated and existing laws should be made stronger with new laws if there is any need to make them.

1.2. Research Gap

This research paper is mainly based on AI based crime particularly addresses the digital harassment which invites about many gaps in current understanding and legal framework. The existing cyber laws design before the adoption of AI in the society. So, the existing laws fail to address the unique characteristics of AI driven harassment and many other in default are found. There automation capability and personalization of harassment. The ethical consideration surrounding AI based harassment mainly individual accountability and psychological impact on the victims remained and unidentified. There is a lack of empirical research on how this leads to digital forms and how these tools can be regulated around the jurisdictions. Additionally, To-days international legal framework is inadequate for managing the borderless nature of such complexities have not yet fully accountable for the misuse of AI technology research. That combine legal technology impact and psychological impact on individuals and ethical guidelines to develop the complete solution. So, addressing this gap is important for evolving and improving the condition of existing laws and punish for the offender's act and following the ethical guidelines. And the society can evolve efficiently without any fear of frauds or any other form of crimes related to AI or AI driven crimes.

1.3. Objective:

The objective of this paper is to fulfill the emerging concerns related to AI based crime, specially focuses on digital harassment and to weigh the adequacy of current cyber laws as in how they address the new complexities and challenges. This paper identifies the gap in legal frameworks, concerns, guidelines and the impact of AI technology on both victims and

the regulatory framework. Mean-while how impact on society. And provide recommendations through which reforms in current legal structure can be made and guidelines can be issued through proposing the practical solutions, rights and freedom to use the technology based on AI.

2. LITERATURE REVIEW

The interaction of artificial intelligence and cybercrime has increased attention in recent years. There are several studies which highlight the growing concern of AI enable digital harassment research by Council of Europe et al. [10] underscores that how the AI technology particularly in the form of the fake and many other machine alcohol rhythms are being recognized for online efforts create attacks that are difficult to detect. While traditional forms of digital harassment have been well equipped and documented the AI river of many complexities due to it's in accuracy out of reach and many other new challenges for both victims and in legal-reforms. Other, legal scholars including United Nations et al. [11] noted that the existing and emerging cyber laws are not equipped well to handle the AI based offences. These laws basically developed to address more conventional forms of cybercrime suggest identifying that hacking which are different from the unique nature of crimes the difficulty lies in this fact that only facilitate white spread harassment with minimal human and making the enforcement of traditional legal framework increases complexities. Researchers have review that the law which accounts to the evolving digital landscapes particularly required the International corporation attendance attention to address the cross-border AI crimes.

Ethical principles surrounding AI rule in digital harassment have been exploded in many studies scholar such as Scholars such as Zeng, M et al. [12] discuss prominently moral implications of AI ribbon harassment mainly focuses on need for tech companies to take more responsibility for AI to develop and deploy many arguments by AI presents the opportunity for new innovation it create a significant responsive volume and amplification of harmful content and there is the online trust which shall be maintained by developing the discipline and AI guideline platforms.

3. RESEARCH METHODOLOGY

This paper uses a secondary research methodology to evaluate the AI based digital harassment. The methodology involves reviewing various existing literature including many academy articles legal journals, law journals and many industry reports to identify the impact of technology on cyber-crime laws and

Correspondence to: Shalu Mehta, Department of Law, Suresh Gyan Vihar University, Jaipur

Corresponding author. E-mail addresses: shaluyadav593@gmail.com



also to critically examine various case studies from secondary resources to develop the practical application of AI in harassment. Moreover, the paper also acknowledges the current legal framework and their potential to address in today's era. The goal is to identify the gaps in law and takes regarding the AI based harassment. This particular research elaborates about the legal gaps and granting protection to individuals.

Digital Harassment: AI Driven- Scope & Impact

With this paper let us emphasize on AI driven harassments including their scopes and impacts:

AI-Powered Bots

Bot can be used to automate the harassments cyber bullying and includes many online hate speeches across various platforms on social media particularly these bots are highly efficient in targeting the individuals as victims and by analyzing or going through their publicly available data and misuse that data for conducting the offences regarding cyber-crimes.

Deep-fakes

The deep-fake is AI technology that can create highly realistic fake images and fake videos that impersonate the human or the individual which leads to defamation of the individual(victim). Which causes reputational damage and psychological stress to an individual(victim) and to his or her family. For example, the AI generated physical intimate videos have been used as the public figures is misuse of AI technology. Another example, for the deep-fake is our Prime minister himself said one of his speech that his many videos are going viral that he is playing garba (Indian folk dance, originated in the state of Gujarat) on festive occasion but it was not true.

Subjective Harassments

Subjective harassment here means personalized harassment which AI allows for highly target. It is the harassments which is based on victim's online persona, bot generates the abusive messages creating a more damaging and emotional impact in the form of harassment to an individual.

Social Impact and Psychological Stress

Correspondence to: Shalu Mehta, Department of Law, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: shaluyadav593@gmail.com

This AI driven harassments causes a severe mental health issues and psychological imbalance in the mind of individual who is and victim for such AI driven harassments. Psychological harassments include anxiety depression, PTSD and causes a long- term reputational harm due to permanency of digital content. Whether the content made was right or wrong despite of that the society judges of the person on the basis of that particular digital content which is wrong but as we know we are in India and Indian society works on such realms and on such notions.

Intensity of Harm

It's beyond imagination that at what intensity the harm is caused to the victim as an individual through AI powered harassment. Rapidly, spread through social networking sites increasing its reach and making it more complex and difficult for a victim to escape from such kind of harassments or recover from such kind of harassment, as it destroys the life of an individual. As, reputation take time & good will, take time to build and it takes a second to destroy.

Legal Gaps, Complexities and Challenges: In Addressing AI-Based Harassment

Below points mentions the legal gaps complexities and challenges which needs to be acknowledged in AI based harassment:

Superannuated Cyber Laws

Many cybercrime laws deal with hacking identity, many other problems but the existing acts like Information Technology Act 2000 & Bharatiya Sakshya Adhiniyam 2023. There is no version of cyber-crime immersed as AI specific offences like the pictures and automated messages of harassment. This leads to a problem that when AI offences take place, where to punish the offender and give relief to victim is still a question.

Trans-Jurisdictional

As the AI crimes are committed all over the world and they are global in nature. It complicates the enforcement of legal reforms because the offenders can operate across or through various jurisdiction often without facing any legal consequences and punishment for the crimes that they have committed.



Ambiguity in Definition:

As in law no-where the AI based harassment has specifically defined (no clear definition has been provided. Its challenging as during the time punishing the offender what to prosecute against the offender's. As, applying existing laws to AI generated content is not complete and significantly right. As, the harm is done beyond these existing laws and considering the same it's not right full that the punishment should be less than the offence committed. Punishment shall always meet the criteria for which the offence has been committed and no existing law or act provides the clear definition of AI based harassments or AI based offences.

Complexities in Ethical Issues

As the current laws are not capable to address many concerns same relates with AI technology which raises a concern of privacy traditionally previously laws often fail to account for the ways that AI uses various way and methods. AI uses to manipulate the individual or how many individual targeted. So, these complexities have not been resolved till date and needs an immediate attention.

Ethical Concerns and Corporate Social Responsibility in AI Development

Accountability

No one can be held accountable because in many cases AI system operates autonomously and it makes extreme difficult to recognize and assign responsibility for the malicious action and to identify the offender the creators or developers or the individuals who misuse the technology may not always be held accountable for offences that they have done. As, on currently based system it is not easy to identify the offender.

Consent & Privacy

AI driven harassments are often the collection of the data which is available of an individual on online platforms and on social media's so the consent for collecting such kind of data is not required and it is easily targetable by the offender's and make victim to fall prey, for AI based offences.

Strengthening Harmful Stereotypes

AI based technology specially, deep fake generators can create harmful stereotypes such as misleading public opinion or spread misinformation about any general or sensitive topic and contribute to evading of trust in the digital content and of social online platforms.

Corporate Social Responsibility

Now, it is responsibility of tech companies that they must provide and generate the integrated ethical guidelines in their product development. And shall design the AI system in such a way that it safeguards the individual's rights and privacy content. Preventing the misuse of AI based technology by establishing monitoring the systems to detect and prevent the AI based harassments.

Transparency and Reporting System

Companies should ensure transparency in AI operations and AI methods. Providing a clear reporting mechanism to victims for harassment. They must also actively engage in preventing AI tools so that victims cannot be exploited for malicious purpose. Proper, complaint procedure shall be established. The offenders shall be made easily identifiable. It is the necessity of modern era.



Table 1. Brief elaboration in the below given table for emerging Crime based on- AI and Cybercrime Laws:

Emerging AI-Based Crimes and Cybercrime Laws	
Category	Details
1. Kind of AI-Based Crimes	a. AI-Driven Phishing: Use of AI to create influencing fake websites and e-mails.
	b. Technology of Deep-fake: Generating false media to impersonate individual's (victim-targeted resource person) for doing digital harassment and fraud.
	c. AI-Generated Malware: AI use to generate an adaptive malware.
	d. Autonomous Cyber Attacks: AI-based systems efficient enough to autonomously target attacks on systems.
2. Legal Frameworks Addressing Cybercrime Ethical Principles	a. Cybersecurity Laws (e.g., GDPR, CCPA): Protecting the individual's personal data from offender's and preventing unauthorized use of AI-driven access.
	b. Intellectual Property Laws: Regulate AI's efficiency to facilitate infringement on copyrights or patents.
	c. AI Regulation Bills (e.g., EU AI Act): Frameworks to ensure AI develops under is ethical guidelines principle and secure individual rights and freedom against the offender.
	d. National and International Cybercrime Laws (Cross-border laws): E.g., Computer Fraud and Abuse Act (CFAA) in the U.S. & IT Act, 2000 & other cyber security laws in India.

4. RECOMMENDATIONS OF PAPER

1. Current cyber laws required to be updated with AI driven offences including deep fakes, automated bully and algorithm manipulation.
2. An International corporation shall be strengthened by the global corporation and coordination among the countries to create a unified legal standard for AI related crimes.
3. To implement the ethical guidelines for AI development to ensure the fairness, transparency, accountability and make it a safe platform that minimizes the misuse, particularly in digital harassment.

4. Developing AI specific reporting and protection mechanism which facilitate for the victim to report the harassment incident easily and see the legal address for AI based harassments on digital platforms.
5. Promoting more public awareness and making the public education compulsory regarding AI based cyber-crimes and encouraging everyone to be responsible and careful while using the technology.

5. CONCLUSION

In conclusion, the rise of AI driven digital harassment makes significant challenge for both existing legal frameworks and ethical guidelines as the AI technology evolve new forms of



online abuse are also evolving making law such a way that they should be measurable offenders shall be punished and without failure. The reports of such AI based harassment or regarding the complaining for the same can be made. This calls for urgent reform to address these challenges. The paper highlighted the need for the legal framework that addresses the AI based crimes it is important that co-operation shall be made cross- border. For cross border offences and corporate social responsibility should be made to ensure AI technology. Although there are tremendous opportunities for innovation its misuse the digital platforms and requires the immediate attention from governments, that tech companies and civil society must come together and collaborate to develop and legal framework after considering the current scenario and provide technical safeguards through the proactive measures adoption ensure that a AI technology could rather use for better development of individual than becoming just a misused, un-trust platform in digital space.

REFERENCES

- [1] Anderson, R. (2020). *Cybercrime and AI: The evolving threats and legal challenges*. Oxford University Press.
- [2] Binns, R. (2018). On the ethics of artificial intelligence and data privacy. *Journal of Technology Ethics*, 34(2), 65-78. <https://doi.org/10.1234/jte.2018.0101>
- [3] Elish, M. C., & Hwang, S. (2021). The ethics of AI in online spaces: Responsibility, transparency, and accountability. *AI & Society*, 36(1), 97-115. <https://doi.org/10.1007/s00146-020-01009-7>
- [4] Goodwin, M. (2021). Deep-fakes and the law: Combating AI-driven harassment. *Law and Technology Review*, 44(3), 220-245. <https://doi.org/10.2113/ltr.2021.0522>
- [5] Hwang, J., & Kim, Y. (2020). *AI and cybersecurity: Understanding the impact of artificial intelligence on cybercrime*. Springer.
- [6] Mc Stay, A. (2018). *The right to be forgotten: AI, privacy, and the ethics of digital harassment*. Routledge.
- [7] Robertson, M., & Goodwin, H. (2021). Addressing the legal and ethical challenges of AI in digital harassment. *International Journal of Cybersecurity*, 29(4), 403-417. <https://doi.org/10.1109/IJC.2021.05410>
- [8] Smith, C. (2019). AI-driven harassment: Legal remedies and ethical dilemmas. *Cyberlaw Journal*, 56(1), 75-92.
- [9] European Union. (2020). *General Data Protection Regulation (GDPR)*.
- [10] Council of Europe. (2021). *The Budapest Convention on Cybercrime*.

- [11] United Nations. (2019). *Artificial intelligence and the law: Global frameworks and ethical considerations*. UN Office on Drugs and Crime.
- [12] Zeng, M., & Zhang, L. (2020). *Legal aspects of AI and digital privacy: Emerging issues in cybersecurity*. Springer Nature