IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, June 2026
Impact Factor: 8.2

AI-Driven Cyberstalking and Automated Harassment: Challenges Before the Criminal Justice System

Dharshini Dharman
School of Excellence in Law, Chennai

Abstract: *The rapid development and widespread adoption of Artificial Intelligence (AI) have significantly transformed the digital ecosystem, creating both opportunities and challenges for modern society. While AI technologies have enhanced communication, automation, and data processing, they have also facilitated the emergence of sophisticated forms of cybercrime, particularly cyberstalking and automated online harassment. Unlike traditional cyberstalking, which primarily involves direct human conduct through electronic communication, AI-driven cyberstalking utilizes advanced technologies such as generative AI, automated bot networks, deepfake systems, voice cloning, predictive algorithms, and synthetic digital identities to conduct persistent, targeted, and large-scale harassment campaigns with minimal human intervention.*

This article critically examines the growing threat of AI-enabled cyberstalking and automated harassment as an emerging challenge for the criminal justice system. It explores the various methods through which AI technologies are misused to impersonate individuals, disseminate false or manipulated content, invade privacy, spread threats, coordinate harassment across multiple platforms, and inflict psychological and reputational harm upon victims. The study further analyses the limitations of existing legal frameworks in addressing offences committed through autonomous and semi-autonomous technological systems that operate with anonymity, speed, and transnational reach.

Adopting a doctrinal and comparative legal research methodology, the article evaluates the adequacy of existing cybercrime laws, anti-stalking provisions, intermediary liability regimes, and platform governance mechanisms. Particular attention is given to challenges relating to criminal liability, attribution of responsibility, mens rea, evidentiary standards, jurisdictional issues, and the role of digital platforms in preventing and responding to AI-assisted abuse. The study identifies significant legal and procedural gaps that hinder the effective investigation and prosecution of such offences.

The article argues that traditional legal approaches are insufficient to address the complexities of AI-driven misconduct and emphasizes the need for comprehensive legal reforms. It recommends the introduction of updated statutory definitions of cyberstalking, enhanced intermediary accountability, AI traceability requirements, strengthened digital forensic capabilities, victim-centric protection mechanisms, and greater international cooperation. The study concludes that the modernization of criminal justice institutions and legal frameworks is essential to safeguard digital rights, ensure effective victim protection, and combat emerging forms of AI-enabled cyber harassment in the evolving technological era..

Keywords: Artificial Intelligence, Cyberstalking, Automated Harassment, Cybercrime, Deepfakes, Voice Cloning, Digital Evidence, Criminal Liability, Intermediary Liability, Legal Reform, Digital Safety, Criminal Justice System

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, June 2026
Impact Factor: 8.2

I. INTRODUCTION

The rapid evolution of Artificial Intelligence (AI) has fundamentally altered the landscape of cybercrime, giving rise to sophisticated forms of automated digital harassment and cyberstalking. While conventional cyberstalking relied on repetitive, manual actions by human perpetrators via online channels, contemporary AI tools—including generative models, autonomous botnets, deepfake creation, voice cloning, and algorithmic communications—allow bad actors to orchestrate massive, non-stop, and precisely targeted harassment campaigns with virtually no human effort.[1] These AI-powered tactics severely jeopardize personal privacy, mental health, data security, and human dignity, while simultaneously laying bare the critical vulnerabilities in current legal frameworks.[2]

This study offers a critical analysis of AI-mediated cyberstalking and automated abuse as an unprecedented dilemma for the modern criminal justice system. It investigates the ways in which autonomous systems and AI utilities are deployed to broadcast threats, assume victims' identities, alter digital personas, distribute non-consensual deepfakes, and streamline multi-platform harassment.[3] Furthermore, the analysis highlights how traditional cyber regulations and anti-stalking laws fall short when dealing with automated, hyper-fast, and anonymous offenses that easily cross geographic borders.

Using a doctrinal and comparative legal approach, this research evaluates current legislation surrounding cybercrime, stalking, intermediary liability, and the responsibilities of digital platforms. It focuses heavily on how legacy criminal law concepts—such as proving intent (*mens rea*), assigning fault, establishing jurisdiction, meeting evidentiary requirements, and proving a sustained "course of conduct"—falter when confronted with AI-generated malice.[44]The paper also reviews global regulatory models and platform governance rules to measure their efficacy against automated misconduct.

The findings reveal gaping legal voids in investigating and prosecuting AI-assisted cybercrimes, particularly when trying to assign criminal fault among end-users, software developers, hosting platforms, and autonomous systems.[5] The paper contends that the current judicial infrastructure is ill-prepared for such technologically complex, automated harassment. To remedy this, it calls for immediate legislative updates, including redefined statutory concepts of stalking, enforced AI tracking mechanisms, heightened platform liability, advanced digital forensics, and cross-border cooperation to fight global AI crime.[6]

In conclusion, the study warns that without a comprehensive modernization of legal, investigative, and regulatory frameworks by criminal justice bodies, AI-powered harassment will increasingly threaten digital safety and leave victims unprotected in this new technological era.

1.1 CONCEPT OF AI-DRIVEN CYBERSTALKING

Cyberstalking refers to the use of electronic communication technologies to repeatedly monitor, harass, threaten, intimidate, or invade an individual's privacy and security. Traditionally, cyberstalking was carried out directly by human perpetrators through emails, text messages, social media platforms, and other online communication channels.

---

[1] Danielle Keats Citron, *Hate Crimes in Cyberspace* (Harvard University Press, 2014).

[2] Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books, 2019).

[3] Robert Chesney & Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," 107 Calif. L. Rev. 1753 (2019).

[4] Susan W. Brenner, *Cybercrime and the Law: Challenges, Issues, and Outcomes* (Northeastern University Press, 2012).

[5] Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Harvard University Press, 2018).

[6] European Commission, *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)* COM/2021/206 final.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, June 2026 Impact Factor: 8.2

However, the rapid advancement of Artificial Intelligence (AI) has significantly transformed the nature of cyberstalking by enabling automated, scalable, and highly sophisticated forms of digital harassment.

Artificial Intelligence encompasses technologies capable of performing tasks that normally require human intelligence, such as learning, decision-making, language processing, and pattern recognition. Criminals increasingly exploit AI tools, including machine learning systems, generative AI, automated bots, facial recognition, and voice-cloning technologies, to conduct surveillance, gather personal information, impersonate victims, and launch targeted harassment campaigns.

AI-driven cyberstalking refers to the use of AI technologies and automated systems to monitor, threaten, impersonate, or harass individuals through digital platforms. Unlike traditional cyberstalking, AI enables offenders to automate their activities, increasing the scale, speed, and persistence of harassment while reducing the likelihood of detection. Deepfake technology further aggravates the problem by creating realistic but fabricated images, videos, and audio recordings that can damage reputations, spread misinformation, or facilitate non-consensual content.

The emergence of AI-driven cyberstalking presents significant challenges for the criminal justice system, particularly in relation to offender identification, attribution of liability, jurisdiction, and digital evidence. As existing legal frameworks were designed primarily to address human conduct, they often struggle to regulate AI-enabled misconduct effectively. Consequently, the growing prevalence of AI-driven cyberstalking underscores the need for stronger legal safeguards, advanced digital forensic mechanisms, and updated regulatory frameworks to protect individuals from technology-enabled harassment.

1.2 Meaning of Artificial Intelligence

The ability of robots and computer systems to carry out tasks that often require human intelligence, such as learning, reasoning, problem-solving, decision-making, language comprehension, and pattern recognition, is known as artificial intelligence (AI). AI systems analyse data, find trends, and produce answers with little assistance from humans by using algorithms, data, and computer models.[7]

John McCarthy coined the phrase "Artificial Intelligence" in 1956 and described it as the science and engineering of creating intelligent machines. Machine learning, natural language processing, computer vision, robotics, and generative AI are all included in modern artificial intelligence. With the use of these technologies, computers can effectively carry out difficult tasks and mimic human cognitive processes.[8]

While artificial intelligence (AI) has greatly aided in innovation and technical progress, its abuse has also made it easier for new types of criminality, such as identity theft, deepfake production, cyberstalking, and automated online harassment. Therefore, analysing AI's legal and criminological ramifications in the digital age requires an understanding of the concept.[9]

1.3 Cyberstalking and Automated Harassment: An Overview

The term "cyberstalking" describes the persistent use of internet communication tools to keep an eye on, threaten, intimidate, or harass someone. Cyberstalking, in contrast to traditional stalking, enables offenders to persistently and covertly target victims via social media, emails, messaging apps, and online forums.[10] The use of bots, scripts, or AI-powered systems to carry out extensive harassment campaigns, distribute abusive content, or repeatedly get in touch with victims without the need for human participation is known as automated harassment. Such behaviour may result in serious psychological distress, harm to one's reputation, and invasion of privacy.[11]

---

[7] Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th edn., Pearson Education, 2021) 1.

[8] Margaret A. Boden, *Artificial Intelligence: A Very Short Introduction* (Oxford University Press, 2018) 4.

[9] John McCarthy, "What is Artificial Intelligence?" (Stanford University, 2007) 2.

[10] Paul Bocij and Leroy McFarlane, 'Cyberstalking: The Technology of Hate' (2003) 76(1) *Police Journal* 204.

[11] Danielle Keats Citron, *Hate Crimes in Cyberspace* (Harvard University Press 2014) 28.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, June 2026
Impact Factor: 8.2

1.4 Emergence of AI-Driven Cybercrimes

The integration of AI into digital platforms has facilitated the emergence of sophisticated cybercrimes. AI tools can generate realistic deepfakes, automate phishing attacks, clone voices, create fake identities, and coordinate large-scale harassment campaigns. These technologies enable offenders to target victims more efficiently and anonymously than traditional methods. The accessibility of generative AI tools has further increased the risk of cyber abuse, making detection and attribution more difficult for law enforcement agencies.[12]

1.5 Difference Between Traditional Cyberstalking and AI-Driven Cyberstalking

Basis	Traditional Cyberstalking	AI-Driven Cyberstalking
Nature of Conduct	Performed directly by a human offender	Conducted through AI tools, algorithms, and automated systems
Human Involvement	High level of direct human participation	Minimal human intervention after deployment
Scale of Harassment	Limited by time and effort of offender	Large-scale and continuous harassment possible
Technology Used	Emails, messages, fake profiles, social media	AI bots, machine learning, deepfakes, voice cloning, generative AI
Personalization	Generally manual and limited	Data-driven and highly personalized
Speed and Reach	Relatively slower	Rapid and capable of targeting multiple victims simultaneously
Detection of Offender	Comparatively easier	More difficult due to automation and anonymity
Evidentiary Challenges	Conventional digital evidence	Complex AI-generated evidence and attribution issues
Impact on Victims	Harassment and intimidation	Enhanced psychological harm, reputational damage, and privacy violations
Criminal Justice Response	Existing laws generally applicable	Raises novel legal and regulatory challenges

1.6 Role of Machine Learning, Generative AI, and Automated Systems in Facilitating Cyber Abuse

Cybercrime and online harassment have changed dramatically as a result of the quick development of Artificial Intelligence (AI) technologies. Machine learning, generative AI, and automated systems are some of the most significant advancements that have improved the efficiency, anonymity, and scale of cyber abuse by criminals. Despite the fact that these technologies have valid uses in a number of industries, their abuse has led to the development of sophisticated forms of identity manipulation, cyberstalking, harassment, and digital exploitation.[13]

Without explicit programming, computer systems may learn from data and perform better thanks to machine learning, a subset of artificial intelligence. Machine learning algorithms can assess a victim's online activity, social media interactions, surfing habits, and personal data in the context of cyber abuse in order to spot weaknesses and forecast

[12] World Economic Forum, *Global Risks Report 2024* (WEF 2024) 41.
[13] Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th edn., Pearson Education, 2021) 35.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, June 2026 Impact Factor: 8.2

behavioural trends. These features enable criminals to customise harassment campaigns, monitor victims more efficiently, and carry out highly targeted cyberstalking.[14]

By making it possible to create realistic text, photos, videos, and audio information, generative AI increases the potential for cyber abuse. Deepfakes and voice-cloning software are examples of technologies that can create convincing digital content that mimics people or shows them doing things that never happened. These tools could be used to disseminate false information, produce intimate photos without consent, harm people's reputations, or enable extortion and blackmail. These detrimental actions are now simpler to carry out, even for those with little technical knowledge, because to the growing accessibility of generative AI platforms.

Cyber abuse is also greatly aided by automated systems and AI-powered bots. Large amounts of threatening messages, offensive remarks, or unwelcome communications can be automatically sent across several digital platforms by these technologies. Because automated bots can run constantly, harassers can carry out persistent campaigns without the need for human intervention. Coordinated bot networks are occasionally used to disseminate false narratives, amplify abusive content, or overwhelm victims with widespread online attacks.

II. FORMS OF AI-DRIVEN HARASSMENT

By enabling automated, scalable, and sophisticated online abuse techniques, artificial intelligence has greatly increased the capabilities of cybercriminals. AI-driven harassment, in contrast to traditional types of cyber harassment, makes use of cutting-edge technologies to more successfully target victims while hiding the identity of those who engage in it. The most prevalent types of AI-driven harassment include the following.

2.1 AI-Powered Chatbots Used to Repeatedly Contact Victims

AI-powered chatbots are automated software applications that use machine learning and natural language processing to create dialogues that resemble those of a human. Although chatbots are frequently used for communication and customer service, they can also be abused to harass, threaten, or repeatedly contact people. Chatbots can be used by criminals to transmit persistent messages, threats, or unwelcome interactions on various digital sites. These automatic exchanges have the potential to overwhelm victims and produce a long-lasting atmosphere of psychological discomfort and terror.[15]

2.2 Automated Social Media Harassment Campaigns

The development and management of automated social media accounts, or "bots," is made possible by artificial intelligence. Without the need for human intervention, these bots may communicate with users, exchange material, and leave comments. Coordinated bot networks are frequently used by cybercriminals to initiate extensive harassment operations against specific targets. These efforts may include online intimidation, trolling, false information, and harsh remarks. Because these attacks are automated, their offenders can target several individuals at once while remaining anonymous.[16]

2.3 Voice Cloning and Impersonation

AI-generated pictures, movies, or audio recordings that accurately portray statements or events that never happened are known as "deepfakes." Offenders can produce extremely convincing fake content involving victims by using generative adversarial networks (GANs) and machine learning. Character assassination, non-consensual intimate imagery, political manipulation, and internet harassment are common uses of deepfakes. Deepfakes are especially dangerous

[14] United Nations Office on Drugs and Crime (UNODC), *Artificial Intelligence and Crime: Emerging Challenges and Policy Responses* (United Nations Publication, 2024) 10.
[15] Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th edn., Pearson Education, 2021) 45.
[16] Danielle Keats Citron, *Hate Crimes in Cyberspace* (Harvard University Press, 2014) 67.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, June 2026 Impact Factor: 8.2

because of their lifelike appearance, which can cause victims to experience social humiliation, emotional distress, and reputational harm.[17]

2.4 AI-Generated Fake Profiles and Identities

Realistic profile images, biographical data, and online personalities that don't match actual people can be produced by generative AI algorithms. Such fictitious identities are commonly used by cybercriminals to trick victims, penetrate online communities, or carry out cyberstalking operations. These made-up personas could be used to track victims, obtain personal data, or launch coordinated harassment campaigns while hiding the real identities of perpetrators. Cloning and Impersonating Voices[18]

2.5 Automated Dissemination of Defamatory or Abusive Content

Large amounts of material can be quickly created and distributed across digital channels thanks to artificial intelligence. AI systems have the ability to automatically produce false accusations, nasty remarks, defamatory claims, and misleading information about specific people. Automation increases the impact on victims and makes content removal more challenging by spreading damaging content repeatedly and concurrently across several websites and social media platforms

2.6 AI-Assisted Doxxing and Privacy Violations

Doxxing is the term used to describe the unapproved gathering and public release of a person's personal data. The ability of criminals to collect, evaluate, and compile personal information from various internet sources is greatly improved by AI technologies. Sensitive information including addresses, phone numbers, workplace details, and personal relationships can be revealed by criminals thanks to machine learning algorithms' ability to find patterns and connections in publicly accessible data. Victims of these privacy infractions may face physical harm, threats, and harassment.

These types of AI-driven harassment show how AI has changed traditional cyber abuse into more complex and challenging crimes. Their increasing frequency emphasises the necessity of strong legal frameworks, efficient digital forensic tools, and improved regulatory monitoring to shield people from the negative effects of AI.[19]

III. IMPACT ON VICTIMS

Victims of AI-driven cyberstalking and automated harassment suffer severe repercussions that affect their social, professional, and personal lives in addition to the digital realm. Automated bots, deepfakes, voice cloning, and data analytics are examples of artificial intelligence technologies that allow harassers to carry out persistent and highly targeted types of harassment. Victims frequently suffer severe psychological, social, financial, and reputational damage as a result. The consequences of such behaviour underscore the critical need for strong institutional and legal protections.

3.1 Psychological Trauma and Emotional Distress

Psychological trauma is one of the most direct effects of AI-driven cyberstalking. Because of ongoing surveillance and harassment, victims often suffer from anxiety, tension, despair, dread, humiliation, and emotional insecurity.[20] A

[17] Europol, *Facing Reality? Law Enforcement and the Challenge of Deepfakes* (Europol Innovation Lab Report, 2022) 7.

[18] United Nations Office on Drugs and Crime (UNODC), *Artificial Intelligence and Crime: Emerging Challenges and Policy Responses* (2024) 12.

[19] Danielle Keats Citron, *Hate Crimes in Cyberspace* (Harvard University Press, 2014) 89.

[20] Danielle Keats Citron, *Hate Crimes in Cyberspace* (Harvard University Press, 2014) 28.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, June 2026
Impact Factor: 8.2

chronic sense of vulnerability is created by the automated nature of AI-enabled abuse, which enables perpetrators to attack victims repeatedly and persistently. By generating embarrassment, social isolation, and a lack of confidence, deepfake content, impersonation, and coordinated harassment campaigns can exacerbate emotional misery. Prolonged exposure to internet harassment can, in extreme circumstances, cause psychological breakdowns and mental health illnesses.[21]

3.2 Reputational Harm

The production and distribution of inaccurate or deceptive content, which can gravely harm a person's reputation, are made possible by AI technology. False impressions about a victim's behaviour or character can be produced by deepfake videos, altered photos, fake social media postings, and AI-generated false material.[22] Correction or removal of such content may be challenging due to its quick dissemination across digital media. Professional jobs, educational chances, and interpersonal connections can all suffer from reputational harm. Victims may still experience social shame and a decline in public trust even after incorrect information is subsequently refuted.[23]

3.3 Invasion of Privacy

Privacy is one of the most significant interests threatened by AI-driven cyberstalking. Machine learning algorithms and automated systems can collect, analyse, and exploit large amounts of personal information obtained from social media platforms, online databases, and digital communications.[24] Offenders may monitor a victim's activities, track locations, gather personal data, or reveal sensitive information without consent. Such actions interfere with the individual's right to privacy and personal autonomy. The misuse of personal data through AI technologies raises serious concerns regarding informational privacy and data protection in the digital age.[25]

3.4 Threats to Personal Safety

Cyberstalking and doxxing can reveal personal information, putting victims at risk for physical damage and threats. AI-assisted tracking technologies raise the possibility of physical assault, intimidation, and stalking by disclosing a person's address, place of employment, daily activities, or contact information. Fearing for their own safety, victims frequently change their daily routines, limit their social interactions, or implement extra security measures. Online abuse can turn into offline criminal activity in severe circumstances, posing serious hazards to one's life and safety.[26]

3.5 Gender-Based Online Violence

AI-driven cyberstalking and online harassment disproportionately harm women and girls. AI is often abused to produce sexually explicit content, deepfake pornography, non-consensual intimate photos, and gender-targeted abuse. Coordinated online attacks aimed at intimidating or silencing female journalists, activists, professionals, and public leaders are especially dangerous. Such behaviour weakens women's engagement in public and digital settings and

---

[21] Brian H. Spitzberg and Gregory Hoobler, "Cyberstalking and the Technologies of Interpersonal Terrorism" (2002) 4(1) *New Media & Society* 71.

[22] Europol, *Facing Reality? Law Enforcement and the Challenge of Deepfakes* (Europol Innovation Lab Report, 2022) 7.

[23] Susan W. Brenner, *Cybercrime and the Law: Challenges, Issues and Outcomes* (Northeastern University Press, 2012) 93.

[24] Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th edn., Pearson Education, 2021) 45.

[25] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

[26] Thomas J. Holt, Adam M. Bossler and Kathryn C. Seigfried-Spellar, *Cybercrime and Digital Forensics: An Introduction* (Routledge, 2018) 125.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, June 2026 Impact Factor: 8.2

perpetuates already-existing gender disparities. Therefore, gender-based violence enabled by AI constitutes a serious human rights issue that calls for targeted legislative and policy solutions.[1]."

3.6 Chilling Effect on Freedom of Expression

Persistent online abuse can deter victims from using digital platforms, voicing their ideas, or taking part in public discourse. People frequently self-censor their words and restrict their online activity out of fear of abuse, threats, reputational attacks, and privacy violations.[11] Known as the "chilling effect," this phenomenon limits the free flow of ideas and erodes democratic participation. By expanding the scope and reach of abusive behaviour, the use of AI technology to amplify harassment exacerbates this effect even more. As a result, AI-driven harassment threatens not just specific victims but also more general democratic freedoms and principles. "

In conclusion, the consequences of AI-powered automated harassment and cyberstalking extend far beyond the internet. Psychological hardship, reputational harm, privacy violations, physical safety threats, gender-based abuse, and restrictions on their right to free expression are all possible outcomes for victims. These consequences demonstrate the necessity of comprehensive legal protections, effective law enforcement mechanisms, and victim-centered tactics to stop AI-enabled cyber abuse.

IV. LEGAL FRAMEWORK IN INDIA

The Indian legal system is facing new difficulties as a result of the quick development of artificial intelligence, especially with regard to identity theft, deepfakes, cyberstalking, online harassment, and privacy violations. A number of constitutional clauses, criminal laws, cyber laws, and court rulings offer protection against such detrimental acts even though India does not currently have a specific statute governing AI-driven cyberstalking.[27] The legal framework aims to provide accountability for digital malfeasance while protecting individual liberty, privacy, dignity, and reputation.[28]

4.1 Constitutional Protection of Privacy and Dignity

A number of fundamental rights guaranteed by the Indian Constitution are pertinent to the fight against automated harassment and cyberstalking caused by artificial intelligence. According to court interpretation, the rights to privacy, dignity, reputation, and mental health are all protected by Article 21's protection of the right to life and personal liberty. These constitutionally protected interests are immediately interfered with by AI-enabled surveillance, internet stalking, deepfake generation, and unapproved personal information collecting.

While freedom of speech and expression is protected by Article 19(1)(a), equality before the law is guaranteed under Article 14. Such freedom, however, cannot be utilised as a cover for damaging AI-generated content or online abuse or harassment. Thus, the constitutional framework necessitates striking a balance between individual rights protection in digital domains and freedom of expression.[29]

4.2 Bharatiya Nyaya Sanhita, 2023

Criminal law provisions against AI-driven cyberstalking and automated harassment are available in the Bharatiya Nyaya Sanhita, 2023 (BNS). While there is no explicit mention of artificial intelligence in the act, a number of its clauses deal with behaviour that is frequently linked to abuse of AI.

When AI tools are used to enable harassment, the regulations pertaining to stalking, criminal intimidation, defamation, identity-related offences, publication of obscene information, and offences harming people's reputation and dignity may

[27] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[28] *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.
[29] Bharatiya Nyaya Sanhita, 2023.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, June 2026 Impact Factor: 8.2

be used.[30] If the use of AI-generated deepfakes, false identities, and automated threats leads to intimidation, damage to one's reputation, or breach of privacy, it may be illegal. As a result, the BNS is a crucial legal tool for pursuing criminals who abuse AI technologies.

4.3 Information Technology Act, 2000

The major piece of legislation controlling cybercrimes in India is still the Information Technology Act, 2000. The Act establishes sanctions for certain types of cyber misbehaviour and gives legal validity to electronic records. In situations involving AI-driven cyber harassment, a number of clauses are especially pertinent.[31]

Offenders who use AI technologies for cyberstalking or harassment may be prosecuted under sections pertaining to identity theft, cheating by personation through computer resources, invasion of privacy, unauthorised access to computer systems, and publication or transmission of objectionable material. Additionally, the Act gives law enforcement organisations the authority to look into cybercrimes and gather digital evidence that is required for prosecution.[32]

The Information Technology Act still plays a crucial role in combating cybercrimes due to the growing usage of AI-generated information, but academics contend that its rules need to be updated to handle new AI-related risks.[33]

4.4 Intermediary Guidelines and Platform Obligations

The main channels by which AI-driven harassment takes place are digital platforms including social media networks, messaging apps, and content-sharing websites. As a result, intermediaries play a crucial role in stopping and dealing with dangerous internet behaviour.[34]

Intermediaries are subject to due diligence requirements under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. These responsibilities include eliminating illegal content, setting up grievance procedures, assisting law enforcement, and taking appropriate steps to stop platform misuse.[35]

Upon receiving legitimate complaints or directives from the government, intermediaries may be obliged to remove offensive content in circumstances involving AI-generated deepfakes, impersonation, cyberstalking, and automated harassment campaigns. As a result, platform accountability is now a crucial part of India's digital governance strategy.

4.5 Judicial Recognition of Privacy Rights

The expansion of legal protections against digital harms has been greatly aided by the Indian judiciary. The Supreme Court acknowledged privacy as a basic right under Article 21 of the Constitution in its historic ruling in Justice K.S. Puttaswamy (Retd.) v. Union of India. The Court stressed that personal data security and informational privacy are crucial components of personal autonomy and dignity[36].

In a similar vein, the Supreme Court emphasised the significance of striking a balance between protection against the abuse of digital platforms and freedom of expression in Shreya Singhal v. Union of India. Court rulings have constantly acknowledged that constitutional rights should not be compromised by technological improvements and that new types of cyber abuse require the evolution of legal protections.

---

[30] Ryan Abbott, *The Reasonable Robot: Artificial Intelligence and the Law* (Cambridge University Press, 2020) 45.
[31] Information Technology Act, 2000, ss. 66C, 66D, 66E and 67
[32] Apar Gupta and Ujwala Uppaluri, "Privacy and Surveillance in India" (2018) 53(16) *Economic and Political Weekly* 34.
[33] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
[34] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[35] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
[36] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, June 2026 Impact Factor: 8.2

These court rulings offer a solid constitutional basis for combating automated harassment and cyberstalking caused by AI. They uphold the idea that people have a right to be shielded from online intrusions that jeopardise their security, privacy, dignity, and reputation.

In conclusion, even though India does not currently have a comprehensive legal framework that specifically regulates AI-driven cyberstalking, the country's current constitutional protections, criminal laws, cyber laws, intermediary regulations, and judicial precedents all work together to provide strong safeguards against such behaviour. However, the growing sophistication of harassment enabled by AI emphasises the necessity of specific law reforms and more robust enforcement procedures.

V. CHALLENGES BEFORE THE CRIMINAL JUSTICE SYSTEM

Artificial Intelligence (AI) has revolutionised cybercrime by making advanced types of automated harassment and cyberstalking possible. The distinctive features of AI technology pose serious problems to the criminal justice system, even while current criminal laws offer a framework for dealing with cyber offences. Investigation and prosecution are frequently made more difficult by problems with offender identity, criminal culpability, digital evidence, jurisdiction, and legal regulation. As a result, courts and law enforcement must deal with intricate legal and technological issues that were not foreseen by conventional criminal law frameworks.

5.1 Difficulty in Identifying Anonymous Offenders

Finding the perpetrators of AI-driven cyberstalking is one of the biggest obstacles in the fight. To hide their identities, cybercriminals often use proxy servers, automated bot networks, virtual private networks (VPNs), encrypted communication platforms, and false identities.[37] The [38]adoption of AI-powered tools makes attribution much more difficult because automated systems may engage in destructive behaviour without constant and direct human intervention.

It can be challenging for law enforcement to track down the source of an incident since criminals frequently use several internet platforms spread across several jurisdictions. Thus, cyberspace's anonymity continues to be a significant barrier to successful criminal investigation and conviction.[39]

5.2 Attribution of Criminal Liability Where AI Systems Are Involved

The foundation of traditional criminal law is the idea that criminal responsibility results from human behaviour combined with a guilty mind (mens rea). However, when destructive actions are carried out by autonomous or semi-autonomous systems, AI-driven cybercrimes pose complicated considerations about who is responsible.[40]

When AI systems independently create information, make judgements, or carry out activities that cause harassment or harm, it becomes especially challenging to assign blame. The question of whether the developer, programmer, platform operator, user, or any other party connected to the AI system should be held liable may come up. There is doubt in the criminal justice system since current legal frameworks typically do not offer definitive answers about accountability for crimes caused by AI.[41]

---

[37] Thomas J. Holt, Adam M. Bossler and Kathryn C. Seigfried-Spellar, *Cybercrime and Digital Forensics: An Introduction* (Routledge, 2018) 118.

[38] Information Technology Act, 2000.

[39] Susan W. Brenner, *Cybercrime and the Law: Challenges, Issues and Outcomes* (Northeastern University Press, 2012) 95.

[40] Information Technology Act, 2000.

[41] Ryan Abbott, *The Reasonable Robot: Artificial Intelligence and the Law* (Cambridge University Press, 2020) 45.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, June 2026 Impact Factor: 8.2

5.3 Collection and Preservation of Digital Evidence

The availability of trustworthy digital evidence is crucial for the successful prosecution of cybercrimes. Electronic communications, social media posts, metadata, server logs, deepfake content, and AI-generated outputs can all be used as evidence in situations involving AI-driven harassment. There are many technical and practical difficulties in gathering and preserving such evidence.[42]

In a short amount of time, digital evidence can be changed, removed, encrypted, or manipulated. AI-generated content may also be altered often, which makes it challenging to verify authenticity and uphold the chain of custody necessary for legal admissibility. Therefore, to properly preserve and interpret electronic evidence, investigating agencies need sophisticated digital forensic capabilities.[43]

5.4 Cross-Border Nature of Cyber Offences

Cybercrimes often cross international borders. A criminal from one nation may target victims who live in another by using servers located in a different jurisdiction. AI-driven cyberstalking frequently involves cloud-based services, globally accessible digital networks, and international communication platforms.[44]

Because these crimes are transnational in nature, law enforcement agencies face significant challenges when trying to obtain evidence, identify suspects, and secure cooperation from other countries. International investigations are made more difficult by variations in legal standards, procedural requirements, and data protection regulations.[45]

5.5 Jurisdictional Conflicts

Another significant obstacle facing the criminal justice system is jurisdictional concerns. While cybercrimes sometimes entail actions that take place concurrently in several jurisdictions, traditional criminal law is mostly territorial in scope. As a result, it might be very difficult to decide whether court has the jurisdiction to look into, prosecute, and decide an AI-driven cybercrime.[46]

When the perpetrator, victim, digital platform, and data storage facilities are situated in different nations, conflicts may occur. Criminal proceedings frequently experience delays and procedural challenges due to the lack of consistent international norms defining cybercrime jurisdiction.[47]

5.6 Rapid Technological Evolution Outpacing Legislation

Legislative reform frequently advances more slowly than technological innovation. Artificial intelligence technologies are developing at a never-before-seen rate, giving rise to new types of cyber abuse that may not have been anticipated when current legislation was passed.[48]

Current criminal and cyber laws may not sufficiently handle new dangers like deepfakes, synthetic identities, voice cloning, and autonomous cyberattacks, even while they offer certain rights against harassment and privacy abuses. Offenders may take advantage of regulatory gaps created by legal frameworks' incapacity to keep up with technological advancements.[49]”

---

[42] Information Technology Act, 2000.

[43] Thomas J. Holt, Adam M. Bossler and Kathryn C. Seigfried-Spellar, *Cybercrime and Digital Forensics: An Introduction* (Routledge, 2018) 126.

[44] UNODC, *Comprehensive Study on Cybercrime* (2013) 145.

[45] Council of Europe, *Convention on Cybercrime (Budapest Convention)*, 2001.

[46] Susan W. Brenner, *Cybercrime Jurisdiction and International Law* (Oxford University Press, 2014) 72.

[47] UNODC, *Comprehensive Study on Cybercrime* (2013) 151.

[48] Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th edn., Pearson Education, 2021) 53.

[49] Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th edn., Pearson Education, 2021) 53.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, June 2026 Impact Factor: 8.2

5.7 Lack of Specialized Cyber Investigation Expertise

Investigating AI-driven cybercrimes calls for extremely specialised technological expertise. Digital forensics, artificial intelligence systems, cybersecurity, data analytics, and electronic evidence management are all critical areas of competence for law enforcement organisations. But many investigating organisations still struggle with a lack of technology resources and qualified staff.[50]

The intricacy of AI technologies could make it more difficult for investigators to comprehend how crimes were done, pinpoint the culprits, and successfully present technical evidence in court. Therefore, ongoing training and capacity-building programs are crucial for bolstering cybercrime enforcement systems.

5.8 Admissibility and Authenticity of AI-Generated Evidence

Investigating AI-driven cybercrimes calls for extremely specialised technological expertise. Digital forensics, artificial intelligence systems, cybersecurity, data analytics, and electronic evidence management are all critical areas of competence for law enforcement organisations. But many investigating organisations still struggle with a lack of technology resources and qualified staff.[51]

The intricacy of AI technologies could make it more difficult for investigators to comprehend how crimes were done, pinpoint the culprits, and successfully present technical evidence in court. Therefore, ongoing training and capacity-building programs are crucial for bolstering cybercrime enforcement systems.

There are particular evidentiary difficulties in criminal procedures because to the growing use of AI-generated content. Courts must decide whether digital evidence created or altered by AI systems is legitimate, trustworthy, and admissible. Even though they are phoney, deepfake movies, artificial intelligence-generated documents, and synthetic audio recordings may look real.

AI systems' capacity to produce convincingly false evidence raises questions about procedural justice and evidentiary integrity. Expert testimony and sophisticated forensic methods may be needed by courts to confirm the legitimacy of electronic evidence. Because AI-generated content is becoming more and more common, it is necessary to establish clear criteria for evidence and procedural protections.[1]."

In conclusion, the criminal justice system faces hitherto unheard-of difficulties due to AI-driven cyberstalking and automated harassment. The limitations of current legal frameworks are highlighted by issues with offender identification, attribution of liability, digital evidence, jurisdiction, technical innovation, investigative expertise, and evidential dependability. Comprehensive legislative changes, improved digital forensic capabilities, international collaboration, and specialised institutional procedures capable of successfully combating AI-enabled cybercrime are all necessary to address these issues.[52]

VI. COMPARATIVE PERSPECTIVE

Many countries and regional organisations have devised creative ways to regulate online harms, platform responsibility, data protection, and artificial intelligence, even though no country has yet created a comprehensive legal framework for addressing AI-driven cyberstalking. Comparing these frameworks offers insightful information for enhancing India's legal response to cybercrime aided by AI.

6.1 United States Approach to Cyberstalking

The US has one of the most comprehensive legal systems in place to deal with internet harassment and cyberstalking. Both federal and state laws make cyberstalking illegal. 18 U.S.C. Section 2261A, the federal cyberstalking legislation,

[50] UNODC, *Artificial Intelligence and Crime: Emerging Challenges and Policy Responses* (2024) 18.
[51] Europol, *Facing Reality? Law Enforcement and the Challenge of Deepfakes* (2022) 7.
[52] Ryan Abbott, *The Reasonable Robot: Artificial Intelligence and the Law* (Cambridge University Press, 2020) 81.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, June 2026
Impact Factor: 8.2

forbids using electronic communication systems to harass, threaten, intimidate, or cause another person significant emotional distress.[53]

The detrimental effects of online harassment are becoming more widely acknowledged by American courts, who have interpreted cyberstalking legislation extensively to take into account new technical techniques. Specific laws addressing identity theft, revenge pornography, online harassment, and digital impersonation have been passed by some states.[54]

Legislative efforts to control synthetic media and shield people from digital impersonation have been spurred in recent years by worries about deepfakes and AI-generated content. The US strategy highlights how crucial it is to combine criminal penalties with victim protection and platform accountability.[55]

6.2 European Union Regulations on AI Governance

Because of its rights-based approach to digital governance, the European Union has become a global pioneer in AI legislation. When it comes to the creation and application of AI systems, the EU places a high priority on privacy, data security, accountability, and openness.

Strong protection against the illegal collection, processing, and misuse of personal data is offered by the General Data Protection Regulation (GDPR). Unauthorised surveillance, profiling, and data exploitation are common components of AI-driven cyberstalking, which may be against GDPR regulations. [56]

The AI Act, which creates a risk-based regulatory framework for artificial intelligence, was also adopted by the European Union. The law places requirements on AI systems concerning accountability, transparency, human oversight, and risk management. The AI Act's regulatory approach aims to prevent the misuse of AI technologies and safeguard fundamental rights, even though it does not expressly target cyberstalking.

In order to address emerging AI-related risks, proactive legislation and preventive measures are crucial, as demonstrated by the European model.

6.3 United Kingdom Online Safety Framework

Through the Online Safety Act, the United Kingdom has implemented a comprehensive approach to address online hazards. Digital platforms are required by law to safeguard users against dangerous and illegal content, such as cyberstalking, harassment, and abuse.

This framework mandates that online service providers create content moderation systems, conduct risk assessments, and collaborate with regulatory bodies. Additionally, the law improves processes for eliminating hazardous content and fortifies protections for vulnerable consumers.[57]

The UK strategy highlights shared accountability between governments, tech firms, and consumers while acknowledging the critical role platform operators play in stopping AI-driven harassment. As a result, the framework offers a helpful model for enhancing intermediary accountability in digital settings.

6.4 International Best Practices in Combating AI-Enabled Harassment

Best practices for dealing with AI-enabled cyber abuse have been recognised by a number of international organisations. These methods place a strong emphasis on a multidisciplinary strategy that combines international collaboration, institutional capacity-building, technical safeguards, and legal control.

---

[53] 18 U.S.C. § 2261A (Federal Cyberstalking Statute, United States).

[54] Danielle Keats Citron, *Hate Crimes in Cyberspace* (Harvard University Press, 2014) 112.

[55] Ryan Abbott, *The Reasonable Robot: Artificial Intelligence and the Law* (Cambridge University Press, 2020) 98.

[56] European Commission, *White Paper on Artificial Intelligence: A European Approach to Excellence and Trust* (2020) 3.

[57] UK Department for Science, Innovation and Technology, *Online Safety Act Guidance* (2024).

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, June 2026 Impact Factor: 8.2

Enhancing digital forensic ability to recognise AI-generated content and verify electronic evidence is a crucial best practice. Another is creating specialised cybercrime units with knowledge of digital investigations, cybersecurity, and artificial intelligence[58]."

Additionally, international organisations have stressed the significance of victim-centered support mechanisms, quick removal of harmful content, transparency in AI systems, and platform responsibility. Programs for digital literacy and public awareness are equally crucial in lowering susceptibility to harassment caused by AI.[59]

Because cyberstalking typically involves perpetrators, victims, and digital infrastructure situated in other jurisdictions, cross-border cooperation is still crucial. International cooperation in the investigation and prosecution of cybercrimes is encouraged by instruments like the Budapest Convention on Cybercrime.[60]

Strong legal safeguards, technology regulation, platform responsibility, specialised investigative processes, and international cooperation are all necessary for effective responses to AI-driven cyberstalking, as the comparative analysis shows. While creating a thorough framework capable of handling the particular difficulties presented by AI-enabled cyber harassment, India may learn important lessons from these strategies.[61]

VII. NEED FOR LEGAL REFORMS

The current legal frameworks controlling cybercrime are facing unprecedented problems due to the rapid growth of artificial intelligence. Although existing laws offer some safeguards against identity theft, cyberstalking, harassment, and privacy infringement, they were mostly created prior to the development of advanced AI technologies like voice cloning, deepfakes, autonomous bots, and generative AI systems. Legal reforms that may protect fundamental rights, encourage responsible technical innovation, and address the particular concerns posed by AI-enabled cyber exploitation are therefore desperately needed.

7.1 Specific Legislation Addressing AI-Generated Harms

There is currently no comprehensive legal framework in India that particularly regulates the harms created by artificial intelligence. Certain effects of AI abuse may be addressed by current criminal and cyber laws, but they fall short in addressing problems like deepfake production, artificial media manipulation, AI-generated impersonation, and automated harassment campaigns.[62]

AI-generated damages should be precisely defined by dedicated legislation, which should also establish criminal culpability for harmful use of AI technologies and offer victims appropriate remedies. These laws should also include provisions for risk assessment, transparency, and protections against the abuse of generative AI systems.

7.2 Enhanced Accountability of AI Developers and Platforms

There are significant concerns about accountability raised by the growing role of AI systems in enabling cyber abuse. Legal changes should clearly define the obligations of IT firms, digital platforms, and AI developers whose technologies are used to support illegal activity.[63]

It should be mandatory for platform owners to put in place strong content moderation procedures, identify harmful content produced by AI, react quickly to complaints, and assist law enforcement. In a similar vein, engineers ought to be urged to include ethical and safety precautions in AI systems to reduce the possibility of abuse.

---

[58] UK Department for Science, Innovation and Technology, *Online Safety Act Guidance* (2024).

[59] United Nations Office on Drugs and Crime (UNODC), *Artificial Intelligence and Crime: Emerging Challenges and Policy Responses* (2024) 20.

[60] Interpol, *Global Cybercrime Strategy* (2022) 15.

[61] OECD, *Artificial Intelligence in Society* (2019) 78.

[62] Ryan Abbott, *The Reasonable Robot: Artificial Intelligence and the Law* (Cambridge University Press, 2020) 98.

[63] OECD, *Artificial Intelligence in Society* (OECD Publishing, 2019) 78.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, June 2026
Impact Factor: 8.2

7.3 Stronger Digital Forensic Infrastructure

There are significant concerns about accountability raised by the growing role of AI systems in enabling cyber abuse. Legal changes should clearly define the obligations of IT firms, digital platforms, and AI developers whose technologies are used to support illegal activity.[64]

It should be mandatory for platform owners to put in place strong content moderation procedures, identify harmful content produced by AI, react quickly to complaints, and assist law enforcement. In a similar vein, engineers ought to be urged to include ethical and safety precautions in AI systems to reduce the possibility of abuse.

7.4 Specialized Cybercrime Units

The intricacy of cybercrimes enabled by AI demands certain investigating skills. Crimes utilising machine learning algorithms, automated systems, and sophisticated digital technologies may be too complex for traditional policing techniques to handle.[65]

It is necessary to create and bolster specialised cybercrime units manned by professionals in cybersecurity, digital forensics, artificial intelligence, and data analytics. To guarantee that investigators, prosecutors, and judicial officers stay up to date on new technological advancements, ongoing professional training programs must to be implemented.

7.5 International Cooperation Mechanisms

Offenders, victims, servers, and digital platforms situated in many jurisdictions are often involved in AI-driven cyberstalking. Therefore, robust international cooperation structures are necessary for effective enforcement.[66]

India should improve cooperation with foreign law enforcement agencies, take an active part in international cybercrime initiatives, and fortify mutual legal aid agreements. To effectively combat cross-border cybercrimes, identify suspects, and gather digital evidence, international cooperation is crucial.

7.6 Victim-Support and Protection Measures

AI-driven harassment frequently causes serious psychological, social, and reputational harm to its victims. Therefore, victim-centered legal reforms that emphasise protection, assistance, and access to justice should be adopted.[67]

Confidential reporting systems, counselling services, legal aid initiatives, quick removal of offensive content, and improved privacy protections are a few examples of possible measures. In order to reduce the long-term effects of cyber harassment and encourage victims to report incidents, effective victim-support services are crucial.

7.7 Public Awareness and Digital Literacy Initiatives

In addition to legal regulation, raising public knowledge of digital threats and online safety procedures is necessary to prevent AI-driven cyber abuse. Many people are still ignorant about the potential dangers of deepfakes, impersonation, and automated harassment, as well as the possibilities of AI technologies.[68]

Governments, academic institutions, and civil society organisations should support digital literacy initiatives that teach people how to use technology responsibly, protect their privacy, and spot false information produced by artificial intelligence. Increased public knowledge can improve overall cyber resilience and dramatically lower susceptibility to cyber abuse.

---

[64] Europol, *Facing Reality? Law Enforcement and the Challenge of Deepfakes* (Europol Innovation Lab Report, 2022) 12.

[65] Interpol, *Global Cybercrime Strategy* (2022) 15.

[66] United Nations Office on Drugs and Crime (UNODC), *Comprehensive Study on Cybercrime* (2013) 151.

[67] Danielle Keats Citron, *Hate Crimes in Cyberspace* (Harvard University Press, 2014) 124

[68] United Nations Office on Drugs and Crime (UNODC), *Artificial Intelligence and Crime: Emerging Challenges and Policy Responses* (2024) 24.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, June 2026
Impact Factor: 8.2

VIII. CONCLUSION

Artificial Intelligence has significantly transformed the digital environment, but its misuse has also enabled sophisticated forms of cyberstalking and automated harassment. Technologies such as deepfakes, voice cloning, automated bots, and synthetic identities have increased the scale, anonymity, and impact of online abuse, posing serious threats to privacy, reputation, dignity, and personal security.

The study finds that victims of AI-driven cyberstalking often experience severe psychological, social, and financial consequences arising from persistent surveillance, privacy violations, and reputational harm. It further reveals that although the Indian legal framework provides protection through the Bharatiya Nyaya Sanhita, 2023, the Information Technology Act, 2000, and intermediary regulations, these laws are not specifically designed to address AI-enabled offences. Challenges relating to offender identification, attribution of liability, digital evidence, and jurisdiction continue to hinder effective enforcement.

A comparative analysis of international regulatory approaches demonstrates the importance of stronger platform accountability, data protection measures, and technological oversight in combating AI-assisted harms. The study concludes that existing legal mechanisms are inadequate to address the evolving nature of AI-driven cyberstalking. Therefore, India must adopt comprehensive reforms, including AI-specific legislation, enhanced digital forensic capabilities, specialized cybercrime investigation units, stronger intermediary obligations, and greater international cooperation. Such measures are essential to safeguard fundamental rights and ensure that technological innovation develops in accordance with the principles of justice, human dignity, and the rule of law

8.1 Suggestions

1. Educational institutions should incorporate digital literacy and cyber safety awareness programs into their curricula to educate individuals about AI-related risks.
2. Public awareness campaigns should be conducted to inform citizens about cyberstalking, deepfakes, online impersonation, and methods for reporting cyber offences.
3. Technology companies should adopt ethical AI principles and implement safeguards to prevent misuse of their products and services.
4. Researchers and policymakers should continuously monitor emerging AI technologies and assess their potential impact on privacy, security, and human rights.
5. Collaboration between government agencies, academia, industry stakeholders, and civil society organizations should be encouraged to formulate effective responses to AI-enabled cyber threats.
6. Further empirical and interdisciplinary research should be undertaken to understand the evolving nature of AI-driven cybercrime and its social consequences.
7. Citizens should be encouraged to adopt responsible online practices, including protecting personal information, verifying digital content, and reporting suspicious activities promptly.
8. Future policy initiatives should seek to balance technological innovation with the protection of constitutional values, individual dignity, and digital rights.

BIBLIOGRAPHY

A. Books

1. Abbott, Ryan, *The Reasonable Robot: Artificial Intelligence and the Law* (Cambridge University Press, 2020).
2. Boden, Margaret A., *Artificial Intelligence: A Very Short Introduction* (Oxford University Press, 2018).
3. Brenner, Susan W., *Cybercrime and the Law: Challenges, Issues and Outcomes* (Northeastern University Press, 2012).
4. Citron, Danielle Keats, *Hate Crimes in Cyberspace* (Harvard University Press, 2014).
5. Holt, Thomas J., Bossler, Adam M. and Seigfried-Spellar, Kathryn C., *Cybercrime and Digital Forensics: An Introduction* (Routledge, 2018).

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, June 2026 Impact Factor: 8.2

6. Russell, Stuart and Norvig, Peter, *Artificial Intelligence: A Modern Approach* (4th edn., Pearson Education, 2021).
7. Brenner, Susan W., *Cybercrime Jurisdiction and International Law* (Oxford University Press, 2014).

B. Journal Articles

1. Bocij, Paul and McFarlane, Leroy, "Cyberstalking: The Technology of Hate" (2003) 76(1) *The Police Journal* 204–221.
2. Spitzberg, Brian H. and Hoobler, Gregory, "Cyberstalking and the Technologies of Interpersonal Terrorism" (2002) 4(1) *New Media & Society* 71–92.
3. Gupta, Apar and Uppaluri, Ujwala, "Privacy and Surveillance in India" (2018) 53(16) *Economic and Political Weekly* 34–40.
4. Citron, Danielle Keats, "Cyber Civil Rights" (2009) 89 *Boston University Law Review* 61–125.

C. Statutes and Legislative Materials

1. Constitution of India, 1950.
2. Bharatiya Nyaya Sanhita, 2023.
3. Information Technology Act, 2000.
4. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
5. Digital Personal Data Protection Act, 2023.
6. General Data Protection Regulation (EU) 2016/679.
7. 18 U.S.C. § 2261A (Federal Cyberstalking Statute, United States).
8. Online Safety Act, 2023 (United Kingdom).

D. Cases

1. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
2. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
3. *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.
4. *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.

E. International Reports and Documents

1. United Nations Office on Drugs and Crime (UNODC), *Comprehensive Study on Cybercrime* (2013).
2. United Nations Office on Drugs and Crime (UNODC), *Artificial Intelligence and Crime: Emerging Challenges and Policy Responses* (2024).
3. Europol, *Facing Reality? Law Enforcement and the Challenge of Deepfakes* (Europol Innovation Lab Report, 2022).
4. Interpol, *Global Cybercrime Strategy* (2022).
5. OECD, *Artificial Intelligence in Society* (OECD Publishing, 2019).
6. European Commission, *White Paper on Artificial Intelligence: A European Approach to Excellence and Trust* (2020).
7. United Nations Women, *Online Violence Against Women and Girls* (2020).
8. Council of Europe, *Convention on Cybercrime (Budapest Convention)* (2001).

F. Web Sources

1. United Nations Office on Drugs and Crime (UNODC), Official Website.
2. Europol, Official Website.
3. Interpol, Official Website.
4. European Commission, Official Website.
5. Ministry of Electronics and Information Technology (MeitY), Government of India.
6. National Cyber Crime Reporting Portal, Government of India.
7. Supreme Court of India Official Website