

***Law Audience Journal, Volume 6 & Issue 4, 25th April 2026,
e-ISSN: 2581-6705, Indexed Journal, Impact Factor 5.988, Published at
<https://www.lawaudience.com/volume-6-issue-4-2/>, Pages: 05 to 24,***

***Title: Artificial Intelligence-Driven Cyber Morphing Against Women in India:
Legal Challenges, Evidentiary Issues, and Policy Responses,
Authored By: Dr. Savita Chaudhary, Assistant Professor of Law, Awasthi
College of Law, Solan.
Email ID: savyychaudhary@gmail.com.***



Cite this article as:

DR. SAVITA CHAUDHARY, “*Artificial Intelligence-Driven Cyber Morphing Against Women in India: Legal Challenges, Evidentiary Issues, and Policy Responses*”, Vol.6 & Issue 4, Law Audience Journal (e-ISSN: 2581-6705), Pages 05 to 24 (25th April 2026), available at <https://www.lawaudience.com/artificial-intelligence-driven-cyber-morphing-against-women-in-india-legal-challenges-evidentiary-issues-and-policy-responses>.

***Law Audience Journal, Volume 6 & Issue 4, 25th April 2026,
e-ISSN: 2581-6705, Indexed Journal, Impact Factor 5.988, Published at
<https://www.lawaudience.com/volume-6-issue-4-2/>, Pages: 05 to 24,***

***Title: Artificial Intelligence-Driven Cyber Morphing Against Women in India:
Legal Challenges, Evidentiary Issues, and Policy Responses,
Authored By: Dr. Savita Chaudhary, Assistant Professor of Law, Awasthi
College of Law, Solan.
Email ID: savyychaudhary@gmail.com.***

***| Copyright © 2026 By Law Audience Journal |
(E-ISSN: 2581-6705)***

All Copyrights are reserved with the Authors. But, however, the Authors have granted to the Journal (Law Audience Journal), an irrevocable, non-exclusive, royalty-free, and transferable license to publish, reproduce, store, transmit, display, and distribute it in the Journal or books or in any form and all other media, retrieval systems and other formats now or hereafter known.

No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other non-commercial uses permitted by copyright law.

For permission requests, write to the publisher, subject of the email must be "Permission Required" at the email addresses given below.

*Email(s): lawjournal@lawaudience.com, info@lawaudience.com,
lawaudience@gmail.com.*

Phone (No(s)): +91-8351033361,

Website: www.lawaudience.com.

Facebook: www.facebook.com/lawaudience.

Instagram: www.instagram.com/lawaudienceofficial.

Contact Timings: 10:00 AM to 8:00 PM.

***Title: Artificial Intelligence-Driven Cyber Morphing Against Women in India:
Legal Challenges, Evidentiary Issues, and Policy Responses,
Authored By: Dr. Savita Chaudhary, Assistant Professor of Law, Awasthi
College of Law, Solan.
Email ID: savyychaudhary@gmail.com.***

Disclaimer:

Law Audience Journal (e-ISSN: 2581-6705) and Its Editorial Board Members do not guarantee that the material published in it is 100 percent reliable. You can rely upon it at your own risk. But, however, the Journal and Its Editorial Board Members have taken the proper steps to provide the readers with relevant material. Proper footnotes & references have been given to avoid any copyright or plagiarism issue. Articles published in Volume 6 & Issue 4 are the original work of the authors.

Views or Opinions or Suggestions (if any) expressed or published in the Journal are the personal points of views of the Author(s) or Contributor(s) and the Journal & Its Editorial Board Members are not liable for the same.

While every effort has been made to avoid any mistake or omission, this publication is published online on the condition and understanding that the publisher shall not be liable in any manner to any person by reason of any mistake or omission in this publication or for any action taken or omitted to be taken or advice rendered or accepted on the basis of this work.

All disputes are subject to the exclusive jurisdiction of Courts, Tribunals and Forums at India only.

***Submit your article(s) for Publications at lawaudience@gmail.com, or
lawjournal@lawaudience.com, with subject as "Submission of Paper(s)
for Publication in Law Audience Journal".***

*Law Audience Journal, Volume 6 & Issue 4, 25th April 2026,
e-ISSN: 2581-6705, Indexed Journal, Impact Factor 5.988, Published at
<https://www.lawaudience.com/volume-6-issue-4-2/>, Pages: 05 to 24,*

***Title: Artificial Intelligence-Driven Cyber Morphing Against Women in India:
Legal Challenges, Evidentiary Issues, and Policy Responses,
Authored By: Dr. Savita Chaudhary, Assistant Professor of Law, Awasthi
College of Law, Solan.
Email ID: savyychaudhary@gmail.com.***

Publisher Details:

Law Audience Journal (e-ISSN: 2581-6705),

*Sole Proprietorship of Mr. Varun Kumar, Kharar, District.
S.A.S, Nagar, Mohali, 140301,*

Phone No(s): +91-8351033361 (WhatsApp),

*Email ID(s): lawjournal@lawaudience.com,
info@lawaudience.com or lawaudience@gmail.com.*

Website: www.lawaudience.com.

Contact Timings: 10:00 AM to 8:00 PM.

Editor(s):

- *Dr. Amit Yadav, Editor-In-Chief at Law Audience Journal,
Associate Professor (Senior Scale) at School of Law, Manipal
University Jaipur.*
- *Adv. Varun Kumar, Founder-CEO-Owner-Publisher-Publishing
Editor at Law Audience Journal.*

Editorial Board Members Details Are Available At:

<https://www.lawaudience.com/editorial-board-members/>

***Title: Artificial Intelligence-Driven Cyber Morphing Against Women in India:
Legal Challenges, Evidentiary Issues, and Policy Responses,
Authored By: Dr. Savita Chaudhary, Assistant Professor of Law, Awasthi
College of Law, Solan.
Email ID: savyychaudhary@gmail.com.***

ABSTRACT:

“The rapid advancement of Artificial Intelligence (AI) has significantly transformed digital interactions and technological innovation; however, it has also intensified emerging forms of cybercrime, particularly cyber morphing targeting women. AI-driven tools such as deepfake technologies, image manipulation software, and generative adversarial networks have enabled the creation of highly realistic morphed images and videos without consent, posing serious threats to privacy, dignity, and the fundamental rights of women in India. This study critically examines the intersection of Artificial Intelligence and cyber morphing, with a specific focus on the legal challenges posed by such technologically sophisticated offences. It evaluates the adequacy and effectiveness of existing legal frameworks, including the Information Technology Act, 2000, relevant provisions of the Indian Penal Code, and emerging data protection regimes, in addressing AI-enabled cyber morphing. The study further explores evidentiary challenges in judicial proceedings, particularly concerning the admissibility, authenticity, and reliability of electronic evidence in cases involving digitally manipulated content.

The study also highlights the psychological, social, and reputational harm suffered by victims, underscoring the gendered nature of such cyber offences. It analyses the role of digital forensics and AI-based detection mechanisms in identifying manipulated media and strengthening the justice delivery system. The research concludes with policy-oriented recommendations, emphasizing the need for AI-specific regulatory frameworks, robust data protection laws, gender-sensitive legal reforms, and increased public awareness. It advocates for a balanced approach that fosters technological advancement while ensuring the protection of individual rights and accountability within the digital ecosystem”.

Keywords: Artificial Intelligence; Cyber Morphing; Women; Digital Evidence; Legal Framework; Deepfakes.

***Title: Artificial Intelligence-Driven Cyber Morphing Against Women in India:
Legal Challenges, Evidentiary Issues, and Policy Responses,
Authored By: Dr. Savita Chaudhary, Assistant Professor of Law, Awasthi
College of Law, Solan.
Email ID: savyychaudhary@gmail.com.***

I. INTRODUCTION:

The digital transformation of society has significantly altered the nature of crime, with cyber offences emerging as a major threat. Among these, cyber morphing—defined as the manipulation of images or videos using digital tools—has increasingly targeted women. With the advent of *Artificial Intelligence (AI)*, cyber morphing has evolved into more sophisticated forms such as deepfakes, making detection and regulation more challenging. In India, where internet penetration is rapidly increasing, women are disproportionately affected by cybercrimes. AI-powered morphing tools allow perpetrators to create realistic fake images or videos, often used for harassment, blackmail, or revenge. These acts not only violate privacy but also undermine dignity and mental well-being. Despite the existence of laws such as the *Information Technology Act, 2000* and provisions under the BNS, the legal framework struggles to address AI-driven crimes effectively. This raises critical questions about authorship, liability, admissibility of digital evidence, and regulatory mechanisms. This study aims to analyze the legal challenges posed by AI-enabled cyber morphing, examine evidentiary issues in prosecuting such crimes, and propose policy reforms for better protection of women in India.

• CONCEPTUAL FRAMEWORK: AI AND CYBER MORPHING:

Artificial Intelligence (AI) refers to the capability of machines and computer systems to perform tasks that typically require human intelligence, such as learning, reasoning, problem-solving, and decision-making. AI systems operate through advanced techniques including machine learning (ML), deep learning, neural networks, and generative adversarial networks (GANs). These technologies enable machines to analyze vast amounts of data, recognize patterns, and generate realistic outputs, including images, audio, and video content (*Russell & Norvig, 2021*). In the context of cybercrime, AI has emerged as a double-edged sword. While it enhances cybersecurity measures, it simultaneously empowers cybercriminals by providing sophisticated tools for committing offences. One of the most concerning developments is the use of GANs, which consist of two neural

***Title: Artificial Intelligence-Driven Cyber Morphing Against Women in India:
Legal Challenges, Evidentiary Issues, and Policy Responses,
Authored By: Dr. Savita Chaudhary, Assistant Professor of Law, Awasthi
College of Law, Solan.
Email ID: savyychaudhary@gmail.com.***

networks—a generator and a discriminator—that work together to create highly realistic synthetic media, commonly known as deepfakes (Goodfellow et al., 2014). AI facilitates cybercrime in several ways. First, it enables the creation of deepfake videos in which a person’s likeness is convincingly replaced with another, often without consent. These deepfakes can be used for harassment, political manipulation, or reputational harm. Second, AI supports automated identity theft by scraping personal data from digital platforms and generating fake identities that appear authentic. Third, AI-driven image processing tools allow for highly realistic image morphing, making it increasingly difficult to distinguish between genuine and manipulated content (Kshetri, 2020). The integration of AI into cybercrime significantly increases the scale, speed, and anonymity of offences. Unlike traditional methods, AI-based tools require minimal technical expertise and are often accessible through open-source platforms, thereby lowering the barrier to entry for cybercriminals. This evolution poses serious challenges for law enforcement agencies, as conventional investigative techniques are often inadequate to detect and prevent AI-enabled crimes.

• **CYBER MORPHING AGAINST WOMEN:**

Cyber morphing refers to the digital manipulation or alteration of images, videos, or other media to create misleading, deceptive, or harmful representations. When directed against women, cyber morphing becomes a form of gender-based cyber violence, often intended to harass, humiliate, exploit, or extort the victim. One of the most common forms of cyber morphing involves superimposing a woman’s face onto explicit or pornographic content using editing software or AI tools. This creates false and defamatory material that can severely damage the victim’s reputation and psychological well-being. Another prevalent practice is the creation of fake social media profiles using morphed images, which are then used to impersonate victims and engage in fraudulent or abusive activities. Additionally, perpetrators often circulate morphed images or videos through messaging platforms or social media to blackmail victims or seek revenge, a phenomenon commonly referred to as image-based sexual abuse (Citron & Franks, 2014).

***Title: Artificial Intelligence-Driven Cyber Morphing Against Women in India:
Legal Challenges, Evidentiary Issues, and Policy Responses,
Authored By: Dr. Savita Chaudhary, Assistant Professor of Law, Awasthi
College of Law, Solan.
Email ID: savyychaudhary@gmail.com.***

The advent of AI has significantly intensified cyber morphing practices. AI-powered tools can produce highly realistic and nearly undetectable manipulated content, making it difficult for victims to prove that the content is fabricated. This technological advancement not only increases the scale of victimization but also complicates legal and evidentiary processes. Moreover, the viral nature of digital platforms ensures rapid dissemination of such content, amplifying the harm caused to victims. Cyber morphing against women must therefore be understood not merely as a technological issue but as a serious violation of fundamental rights, including the right to privacy, dignity, and equality. It reflects broader societal issues of gender discrimination and misuse of technology, necessitating a comprehensive legal and policy response.

II. REVIEW OF LITERATURE

A review of existing literature reveals significant scholarly contributions in the fields of Artificial Intelligence, cybercrime, and digital rights:

- **Russell & Norvig (2021)** discuss the foundational concepts of Artificial Intelligence and its applications, highlighting both its benefits and risks.
- **Goodfellow et al. (2014)** introduced Generative Adversarial Networks (GANs), which form the technological basis of deepfake creation.
- **Kshetri (2020)** examines the role of emerging technologies in cybercrime, emphasizing the challenges posed by AI-driven offences.
- **Danielle Keats Citron (2019)** explores online harassment and image-based abuse, particularly focusing on gendered cyber violence.
- **Citron & Franks (2014)** analyze non-consensual pornography and its legal implications.
- **Casey (2011)** highlights the importance of digital forensics and evidentiary integrity in cybercrime investigations.
- **Reddy (2022)** critically evaluates Indian cyber laws and their limitations in addressing AI-based crimes.

***Title: Artificial Intelligence-Driven Cyber Morphing Against Women in India:
Legal Challenges, Evidentiary Issues, and Policy Responses,
Authored By: Dr. Savita Chaudhary, Assistant Professor of Law, Awasthi
College of Law, Solan.
Email ID: savyychaudhary@gmail.com.***

III. RESEARCH GAP:

Most existing studies focus either on AI technology or cybercrime independently. Limited research integrates AI, cyber morphing, and gender-specific legal analysis in the Indian context, thereby justifying the present study.

IV. OBJECTIVES OF THE STUDY:

The present study aims to achieve the following objectives:

- 1. To examine the role of Artificial Intelligence in transforming cyber morphing into a technologically advanced form of cybercrime.*
- 2. To analyze the nature and extent of cyber morphing offences targeting women in India.*
- 3. To evaluate the adequacy and effectiveness of existing legal frameworks, including the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023, in addressing AI-enabled cyber morphing.*
- 4. To identify key legal challenges such as attribution of liability, jurisdictional issues, and lack of AI-specific legislation.*
- 5. To examine evidentiary challenges related to admissibility, authenticity, and reliability of digital evidence in cyber morphing cases.*
- 6. To assess the socio-psychological impact of cyber morphing on women.*
- 7. To propose policy reforms and legal measures for effective prevention and regulation of AI-driven cyber offences.*

V. SCOPE OF THE STUDY:

The scope of the study is confined to:

- The intersection of Artificial Intelligence and cyber morphing, particularly in the Indian context.*
- Analysis of AI tools such as deepfakes and image manipulation technologies used in*

***Title: Artificial Intelligence-Driven Cyber Morphing Against Women in India:
Legal Challenges, Evidentiary Issues, and Policy Responses,
Authored By: Dr. Savita Chaudhary, Assistant Professor of Law, Awasthi
College of Law, Solan.
Email ID: savyychaudhary@gmail.com.***

cyber offences.

- Examination of legal frameworks in India, including IT Act, BNS, and relevant judicial decisions.
- Study of evidentiary issues under the Indian Evidence Act, 1872 (Section 65B).
- Focus on cyber morphing against women as a form of gender-based digital violence.

VI. LIMITATIONS:

- The study does not extensively cover technical algorithmic development of AI.
- Comparative international analysis is limited.
- Rapid technological changes may outpace legal developments discussed.

VII. HYPOTHESIS OF THE STUDY:

Existing legal frameworks in India are inadequate to effectively address AI-enabled cyber morphing offences against women.

1. *AI technologies have significantly increased the complexity and scale of cyber morphing crimes.*
2. *Evidentiary challenges weaken the prosecution and reduce conviction rates in such cases.*
3. *Lack of AI-specific legislation leads to ambiguity in liability and enforcement.*
4. *Strengthening legal and technological mechanisms can significantly improve victim protection and justice delivery.*

VIII. NEED OF THE STUDY:

This study is necessary due to the following reasons:

- Rapid advancement of Artificial Intelligence technologies has created new forms of cybercrime.
- Increasing incidents of cyber morphing and deepfake-based exploitation of women.

***Title: Artificial Intelligence-Driven Cyber Morphing Against Women in India:
Legal Challenges, Evidentiary Issues, and Policy Responses,
Authored By: Dr. Savita Chaudhary, Assistant Professor of Law, Awasthi
College of Law, Solan.
Email ID: savyychaudhary@gmail.com.***

- Lack of specific legal provisions addressing AI-driven crimes in India.
- Growing evidentiary challenges in courts related to digital and AI-generated content.
- Need to protect fundamental rights such as privacy, dignity, and equality.
- Absence of sufficient academic research focusing on AI and gender-based cybercrime in India.

IX. LEGAL FRAMEWORK IN INDIA:

The Information Technology Act, 2000 (IT Act) is the primary legislation in India governing cyber activities and offences. Enacted to facilitate electronic commerce and address cybercrime, the Act provides a legal framework for regulating digital conduct. However, it was drafted at a time when Artificial Intelligence (AI) and advanced technologies such as deepfakes were not prevalent, resulting in significant limitations when applied to contemporary cyber offences like AI-driven cyber morphing. Section 66E of the IT Act deals with the violation of privacy. It criminalizes the intentional capturing, publishing, or transmission of images of a private area of any person without their consent. In cases of cyber morphing, especially where a woman's image is manipulated and circulated without consent, this provision may be invoked. However, the section primarily addresses unauthorized capture of real images rather than AI-generated or synthetically altered content, thereby creating ambiguity in its application to deepfake technologies (Government of India, 2000).

Section 67 of the IT Act penalizes the publication or transmission of obscene material in electronic form. It is often used in cases involving morphed images circulated online with the intent to harass or defame women. Similarly, Section 67A provides stricter punishment for the publication or transmission of sexually explicit material. These provisions are relevant in addressing the dissemination of morphed or deepfake pornographic content. Nevertheless, they focus on the nature of the content rather than the technological process

***Title: Artificial Intelligence-Driven Cyber Morphing Against Women in India:
Legal Challenges, Evidentiary Issues, and Policy Responses,
Authored By: Dr. Savita Chaudhary, Assistant Professor of Law, Awasthi
College of Law, Solan.
Email ID: savyychaudhary@gmail.com.***

used to create it and thus fail to address the unique challenges posed by AI-generated media (Bansal, 2016). A major limitation of these provisions is their inability to adequately address issues of authorship, intent, and liability in AI-based offences. For instance, in cases involving deepfake content, it may be difficult to identify the original creator, especially when such content is generated using automated tools or widely available applications. Furthermore, the IT Act does not explicitly define or regulate emerging technologies like AI, machine learning, or synthetic media, which limits its effectiveness in prosecuting modern cybercrimes (Reddy, 2022). Additionally, the Act does not provide clear guidelines for the admissibility and authentication of AI-generated digital evidence, thereby complicating judicial proceedings. Law enforcement agencies also face challenges in investigation due to the lack of technical expertise and infrastructure required to trace and analyze AI-driven offences. In conclusion, while the IT Act, 2000 offers a foundational framework to address cyber offences, its provisions are not adequately equipped to deal with the complexities of AI-enabled cyber morphing. This highlights the urgent need for legislative reforms to incorporate technology-specific definitions and mechanisms to effectively combat emerging cyber threats.

X. JUDICIAL APPROACH:

The Indian judiciary has played a significant role in recognizing and addressing issues related to cyber harassment, privacy violations, and digital rights. A major turning point in this regard was the landmark judgment in ***Justice K.S. Puttaswamy vs. Union of India (2017)***, wherein the Supreme Court of India unequivocally recognized the right to privacy as a fundamental right under Article 21 of the Constitution. The Court emphasized that privacy includes the protection of personal autonomy, dignity, and informational self-determination, all of which are directly implicated in cases of cyber morphing and digital exploitation. This judgment has far-reaching implications for cybercrimes against women, particularly those involving the unauthorized use, manipulation, and dissemination of personal images. In cases of cyber morphing, where a woman's image is altered and

***Title: Artificial Intelligence-Driven Cyber Morphing Against Women in India:
Legal Challenges, Evidentiary Issues, and Policy Responses,
Authored By: Dr. Savita Chaudhary, Assistant Professor of Law, Awasthi
College of Law, Solan.
Email ID: savyychaudhary@gmail.com.***

circulated without her consent, the violation extends beyond mere defamation to an infringement of her fundamental right to privacy and dignity. The recognition of privacy as a fundamental right provides a constitutional basis for victims to seek legal remedies against such abuses (*Puttaswamy vs. Union of India, 2017*).

Indian courts have also, in various cases, acknowledged the seriousness of online harassment and image-based abuse. For instance, judicial interventions have emphasized the responsibility of digital platforms to remove objectionable content and protect users from harm. However, these decisions have largely been based on existing legal provisions under the Information Technology Act, 2000 and the Indian Penal Code (now Bharatiya Nyaya Sanhita, 2023), rather than addressing the technological nuances of AI-driven offences. Despite these developments, there remains a significant gap in jurisprudence specifically dealing with Artificial Intelligence and AI-generated morphing, such as deepfakes. Courts have yet to develop clear legal standards regarding issues such as authorship of AI-generated content, liability of developers or users of AI tools, and evidentiary standards for proving the authenticity or falsity of digitally manipulated media. The absence of precedents in this area creates uncertainty in legal interpretation and enforcement (Reddy, 2022). Furthermore, the rapid evolution of AI technologies has outpaced judicial responses, making it difficult for courts to effectively adjudicate cases involving sophisticated digital manipulation. The lack of technical expertise and standardized forensic tools further complicates the judicial process. In conclusion, while the Indian judiciary has made significant progress in recognizing privacy and addressing cyber harassment, there is an urgent need for judicial innovation and jurisprudential development to specifically tackle AI-enabled cyber morphing. This requires not only interpretation of existing laws in light of technological advancements but also the establishment of clear legal principles to guide future cases.

XI. LEGAL CHALLENGES:

***Title: Artificial Intelligence-Driven Cyber Morphing Against Women in India:
Legal Challenges, Evidentiary Issues, and Policy Responses,
Authored By: Dr. Savita Chaudhary, Assistant Professor of Law, Awasthi
College of Law, Solan.
Email ID: savyychaudhary@gmail.com.***

- **ABSENCE OF SPECIFIC AI LEGISLATION:**

One of the most significant challenges in addressing AI-enabled cyber morphing in India is the absence of a comprehensive legal framework specifically governing Artificial Intelligence. Existing laws, such as the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023, were enacted without anticipating the complexities introduced by AI technologies like deepfakes and generative models. This legislative gap creates ambiguity in determining liability. For instance, it is unclear whether responsibility lies with the creator of the AI tool, the user who deploys it, or the platform that hosts the content. Such uncertainty weakens legal accountability and complicates enforcement. Moreover, the lack of statutory definitions for concepts like “AI-generated content” or “deepfakes” further hinders effective prosecution, as courts must rely on outdated provisions that may not adequately capture the nature of the offence (Reddy, 2022). The absence of AI-specific legislation also affects preventive regulation. Without clear guidelines, there is limited scope for regulating the development, distribution, and misuse of AI tools, thereby allowing cyber morphing practices to proliferate unchecked.

- **ATTRIBUTION OF LIABILITY:**

Attribution of liability is a critical issue in cases of AI-driven cybercrime. Identifying the perpetrator behind morphed or deepfake content is inherently difficult due to the anonymity provided by the internet. Offenders often use encrypted networks, virtual private networks (VPNs), and fake identities to conceal their identity, making it challenging for law enforcement agencies to trace them. Additionally, the use of automated AI tools further complicates attribution. In many cases, content is generated through pre-existing algorithms or software applications, raising questions about whether liability should be attributed to the developer, the user, or both. The decentralized and automated nature of AI systems blurs traditional notions of mens rea (criminal intent) and actus reus (criminal act), which are fundamental to criminal liability (Yar & Steinmetz, 2019). This complexity often results in delayed investigations and low conviction rates, thereby undermining the deterrent

***Title: Artificial Intelligence-Driven Cyber Morphing Against Women in India:
Legal Challenges, Evidentiary Issues, and Policy Responses,
Authored By: Dr. Savita Chaudhary, Assistant Professor of Law, Awasthi
College of Law, Solan.
Email ID: savyychaudhary@gmail.com.***

effect of the law.

- **JURISDICTIONAL ISSUES:**

Cybercrimes, including AI-enabled cyber morphing, frequently transcend national boundaries, creating significant jurisdictional challenges. A single act of cyber morphing may involve multiple jurisdictions—for example, the perpetrator may be located in one country, the victim in another, and the digital platform hosted in a third. Such cross-border elements complicate both investigation and enforcement. Indian law enforcement agencies often face difficulties in obtaining data from foreign service providers due to differences in legal systems and lack of effective international cooperation mechanisms. Mutual Legal Assistance Treaties (MLATs), while available, are often time-consuming and inefficient in addressing fast-paced cyber offences. Furthermore, jurisdictional ambiguity can delay legal proceedings and hinder victim redressal. The absence of harmonized international standards for regulating AI and cybercrime exacerbates these challenges, making it imperative for India to strengthen global cooperation and adopt transnational legal frameworks (Kshetri, 2020).

- **INADEQUATE PUNISHMENTS:**

Another critical issue is the inadequacy of existing punishments in addressing the severity of harm caused by AI-generated cyber morphing. While the IT Act and related criminal laws prescribe penalties for offences such as obscenity and privacy violations, these punishments may not proportionately reflect the psychological, social, and reputational harm suffered by victims, particularly women. AI-generated content, such as deepfake pornography, can have long-lasting and irreversible consequences due to its realism and rapid dissemination across digital platforms. Despite this, the penalties under existing laws are relatively limited and may not serve as an effective deterrent for offenders. Moreover, the absence of graded penalties based on nature and impact of AI-driven offences results in a lack of proportionality in sentencing. This undermines the principles of justice and fails to adequately recognize the seriousness of emerging cyber threats (Citron, 2019).

***Title: Artificial Intelligence-Driven Cyber Morphing Against Women in India:
Legal Challenges, Evidentiary Issues, and Policy Responses,
Authored By: Dr. Savita Chaudhary, Assistant Professor of Law, Awasthi
College of Law, Solan.
Email ID: savyychaudhary@gmail.com.***

XII. EVIDENTIARY ISSUES:

• ADMISSIBILITY OF DIGITAL EVIDENCE:

The admissibility of digital evidence in India is primarily governed by Section 65B of the Indian Evidence Act, 1872, which lays down specific conditions for the acceptance of electronic records in judicial proceedings. According to this provision, any electronic evidence must be accompanied by a proper certification to establish its authenticity and integrity. In cases involving AI-generated cyber morphing, significant challenges arise in satisfying these requirements. First, authenticating AI-generated content becomes difficult because such content may not have an identifiable original source. Deepfake images or videos are often created using complex algorithms that leave minimal traceable metadata, making verification problematic. Second, proving originality is equally challenging, as the manipulated content may closely resemble genuine media, thereby blurring the distinction between authentic and fabricated material (Kshetri, 2020). These issues create hurdles in establishing evidentiary credibility, often weakening the prosecution's case and affecting the administration of justice.

• DEEPAKE DETECTION DIFFICULTIES:

One of the most pressing evidentiary concerns in AI-driven cyber morphing is the difficulty in detecting deep-fake content. Advances in machine learning and generative adversarial networks (GANs) have enabled the creation of hyper-realistic media that is often indistinguishable from genuine content. This raises critical issues relating to the burden of proof. Victims may find it difficult to prove that the content is fake, while accused persons may exploit this ambiguity to evade liability. Additionally, the reliability of forensic tools used to detect deepfakes remains a concern, as such tools are still evolving and may not always produce conclusive results (Whittaker et al., 2018). The absence of standardized forensic methodologies further complicates the evidentiary process, leading to inconsistencies in judicial outcomes.

***Title: Artificial Intelligence-Driven Cyber Morphing Against Women in India:
Legal Challenges, Evidentiary Issues, and Policy Responses,
Authored By: Dr. Savita Chaudhary, Assistant Professor of Law, Awasthi
College of Law, Solan.
Email ID: savyychaudhary@gmail.com.***

- **CHAIN OF CUSTODY:**

Maintaining the chain of custody is essential to ensure the integrity and reliability of digital evidence. However, in the context of cyber morphing, this process becomes highly complex. Digital content can be easily duplicated, altered, or transmitted across multiple platforms within seconds, making it difficult to track its origin and movement. Data manipulation is another significant concern, as even minor alterations can compromise the evidentiary value of digital records. Ensuring that the evidence presented in court is the same as that originally collected requires robust technical safeguards and documentation procedures, which are often lacking in practice (Casey, 2011). These challenges undermine the credibility of digital evidence and may lead to its rejection in court.

- **EXPERT TESTIMONY:**

Given the technical nature of AI-generated content, courts increasingly rely on expert testimony to interpret digital evidence. Experts play a crucial role in explaining the functioning of AI systems, identifying manipulated content, and validating forensic findings. However, the lack of adequately trained experts in the field of AI and digital forensics poses a significant challenge. Inconsistent expertise and absence of standardized procedures can lead to conflicting opinions, thereby hindering judicial decision-making. Moreover, the judiciary itself may lack sufficient technical understanding, further complicating the evaluation of expert evidence (Reddy, 2022). To address these issues, there is a need for capacity building and the establishment of uniform forensic standards.

- **IMPACT ON WOMEN:**

Cyber morphing has profound and far-reaching consequences for women, extending beyond legal violations to deeply affect their psychological and social well-being. Victims often experience severe psychological trauma, including anxiety, depression, and emotional distress, as a result of the unauthorized use and circulation of their images. Social stigma is another significant impact, particularly in the Indian socio-cultural context, where issues related to reputation and honor are highly sensitive. Morphed or explicit content can lead to

***Title: Artificial Intelligence-Driven Cyber Morphing Against Women in India:
Legal Challenges, Evidentiary Issues, and Policy Responses,
Authored By: Dr. Savita Chaudhary, Assistant Professor of Law, Awasthi
College of Law, Solan.
Email ID: savyychaudhary@gmail.com.***

victim-blaming, isolation, and damage to personal and professional relationships. The reputational harm caused by such content is often irreversible due to its rapid and widespread dissemination on digital platforms (Citron, 2019). Furthermore, many victims hesitate to report such crimes due to fear of social backlash, lack of awareness, and mistrust in the legal system. This underreporting exacerbates the problem and allows perpetrators to act with impunity.

- **POLICY REFORMS AND RECOMMENDATIONS:**
- **ENACTMENT OF AI-SPECIFIC LEGISLATION:**

To effectively combat AI-enabled cyber morphing, India must enact comprehensive legislation specifically addressing Artificial Intelligence and its misuse. Such laws should define and regulate deepfakes, synthetic media, and AI-generated content, while clearly establishing liability for creators, users, and intermediaries.

- **STRENGTHENING CYBER LAWS:**

Existing laws, particularly the Information Technology Act, 2000, should be amended to incorporate provisions dealing explicitly with cyber morphing and AI-driven offences. Penalties should be enhanced to reflect the severity of harm caused, ensuring a stronger deterrent effect.

- **CAPACITY BUILDING:**

There is a pressing need to strengthen institutional capacity by:

- Training law enforcement agencies in handling AI-based cybercrimes
- Developing advanced forensic infrastructure for detecting manipulated content

Such measures would improve investigation and prosecution efficiency.

- Awareness Campaigns

Public awareness initiatives are essential to educate women about:

- Cyber safety practices
- Available legal remedies

**Title: Artificial Intelligence-Driven Cyber Morphing Against Women in India:
Legal Challenges, Evidentiary Issues, and Policy Responses,
Authored By: Dr. Savita Chaudhary, Assistant Professor of Law, Awasthi
College of Law, Solan.
Email ID: savyychaudhary@gmail.com.**

Empowering victims with knowledge can encourage reporting and reduce vulnerability to cyber exploitation.

- **PLATFORM ACCOUNTABILITY:**

Social media and digital platforms must be held accountable for the content they host.

They should:

- Implement AI-based detection tools to identify and remove harmful content
- Establish quick grievance redressal mechanisms

Proactive platform regulation is crucial in preventing the spread of morphed content.

- **INTERNATIONAL COOPERATION:**

Given the transnational nature of cybercrime, India must strengthen international cooperation through:

- Bilateral and multilateral agreements
- Efficient data-sharing mechanisms

Global collaboration is essential for effective investigation and enforcement in AI-driven cyber offences (Kshetri, 2020). Artificial Intelligence has fundamentally transformed the landscape of cybercrime, converting cyber morphing into a highly sophisticated and potent tool for harassment, exploitation, and gender-based digital violence, particularly against women in India. The emergence of deepfake technologies and AI-driven content generation has amplified the scale, realism, and impact of such offences, making them more difficult to detect, regulate, and prosecute. While existing legal frameworks, including the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023, provide a foundational basis to address cyber offences, they remain inadequate in dealing with the unique challenges posed by AI-enabled crimes.

- **SUGGESTIONS AND RECOMMENDATIONS:**

1. Introduce AI literacy programs for law enforcement and judiciary.

**Title: Artificial Intelligence-Driven Cyber Morphing Against Women in India:
Legal Challenges, Evidentiary Issues, and Policy Responses,
Authored By: Dr. Savita Chaudhary, Assistant Professor of Law, Awasthi
College of Law, Solan.
Email ID: savyychaudhary@gmail.com.**

2. Encourage public awareness campaigns on cyber safety for women.
3. Promote research and development in AI detection tools.
4. Strengthen victim support systems, including counseling and legal aid.

RECOMMENDATIONS

Legal Reforms:

- Enact AI-specific legislation defining deepfakes and synthetic media.
- Amend the Information Technology Act, 2000 to include AI-based offences.
- Introduce strict penalties for cyber morphing and deepfake exploitation.

Technological Measures:

- Develop AI-based detection and forensic tools.
- Establish national digital forensic laboratories.

Institutional Measures:

- Provide specialized training for police, cyber cells, and judiciary.
- Create fast-track courts for cybercrime cases involving women.

Platform Accountability:

- Mandate social media platforms to:
 - Remove harmful content quickly
 - Implement AI detection systems
 - Ensure grievance redressal mechanisms

International Cooperation:

- Strengthen cross-border legal frameworks
- Improve data-sharing mechanisms with global agencies

CONCLUSION:

The study highlights that legal ambiguity, particularly in relation to liability and authorship, significantly undermines the effectiveness of current laws. Additionally, evidentiary

***Title: Artificial Intelligence-Driven Cyber Morphing Against Women in India:
Legal Challenges, Evidentiary Issues, and Policy Responses,
Authored By: Dr. Savita Chaudhary, Assistant Professor of Law, Awasthi
College of Law, Solan.
Email ID: savyychaudhary@gmail.com.***

challenges—such as authentication of digital content, deepfake detection, and maintenance of the chain of custody—further complicate judicial processes. The lack of specialized forensic infrastructure and trained personnel exacerbates these issues, often resulting in delayed justice or low conviction rates. Furthermore, the absence of comprehensive policy frameworks specifically addressing Artificial Intelligence limits the ability of regulatory bodies to respond effectively to evolving technological threats (Reddy, 2022; Kshetri, 2020). Beyond legal and procedural concerns, cyber morphing has profound socio-psychological implications for women, including trauma, reputational harm, and social stigma. The reluctance of victims to report such crimes due to fear of victim-blaming and societal backlash further highlights the need for a more supportive and victim-centric approach.

In light of these challenges, it is imperative for India to adopt a comprehensive and multi-dimensional strategy. This includes enacting AI-specific legislation, strengthening existing cyber laws, enhancing forensic and investigative capacities, and promoting digital literacy and awareness among citizens. Equally important is the role of digital platforms in ensuring accountability through proactive monitoring and swift removal of harmful content. Given the transnational nature of cybercrime, international cooperation and harmonization of legal standards are essential for effective enforcement. In conclusion, safeguarding women in the digital age requires not only robust legal reforms but also a coordinated effort involving technology, policy, and society. A proactive, adaptive, and inclusive approach is necessary to ensure that technological advancements do not come at the cost of fundamental rights, dignity, and justice.

***Title: Artificial Intelligence-Driven Cyber Morphing Against Women in India:
Legal Challenges, Evidentiary Issues, and Policy Responses,
Authored By: Dr. Savita Chaudhary, Assistant Professor of Law, Awasthi
College of Law, Solan.
Email ID: savyychaudhary@gmail.com.***

References:

- Citron, D. K. (2019). *Hate crimes in cyberspace*. Harvard University Press.
- Government of India. (2000). *Information Technology Act, 2000*.
- Government of India. (2023). *Bharatiya Nyaya Sanhita, 2023*.
- Kshetri, N. (2020). *The economics of deepfakes*. *IT Professional*, 22(2), 73–77.
<https://doi.org/10.1109/MITP.2020.2976092>
- Reddy, G. S. (2022). *Artificial intelligence and legal liability: Emerging issues*.
Indian Journal of Law and Technology, 18(1), 89–110.
- Whittaker, M., Crawford, K., Dobbe, R., et al. (2018). *AI Now Report 2018*. New York University.
- Citron, D. K., & Franks, M. A. (2014). *Criminalizing revenge porn*. *Wake Forest Law Review*, 49, 345–391.
- Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). *Generative adversarial nets*. *Advances in Neural Information Processing Systems*, 27, 2672–2680.
- Kshetri, N. (2020). *The economics of deepfakes*. *IT Professional*, 22(2), 73–77.
<https://doi.org/10.1109/MITP.2020.2976092>
- Russell, S., & Norvig, P. (2021). *Artificial intelligence: A modern approach (4th ed.)*. Pearson.
- Bansal, A. (2016). *Cyber laws in India: An analysis of the Information Technology Act, 2000*.
International Journal of Law and Legal Jurisprudence Studies, 3(2), 1–10.
- Government of India. (2000). *Information Technology Act, 2000*.
- Reddy, G. S. (2022). *Artificial intelligence and legal liability: Emerging issues*.
Indian Journal of Law and Technology, 18(1), 89–110.
- Agarwal, S., & Sharma, R. (2021). *Cybercrime against women in India: Issues and challenges*.

***Title: Artificial Intelligence-Driven Cyber Morphing Against Women in India:
Legal Challenges, Evidentiary Issues, and Policy Responses,
Authored By: Dr. Savita Chaudhary, Assistant Professor of Law, Awasthi
College of Law, Solan.
Email ID: savyychaudhary@gmail.com.***

Journal of Cyber Law, 5(2), 45–60.

- Citron, D. K. (2019). *Hate crimes in cyberspace*. Harvard University Press.
- Government of India. (2000). *Information Technology Act, 2000*.
- Government of India. (1872). *Indian Evidence Act, 1872*.
- Kshetri, N. (2020). *The economics of deepfakes*. *IT Professional*, 22(2), 73–77.
- *Putta swamy v. Union of India*, (2017) 10 SCC 1.
- Reddy, G. S. (2022). *Artificial intelligence and legal liability: Emerging issues*. *Indian Journal of Law and Technology*, 18(1), 89–110.
- West, S. M. (2019). *Data capitalism: Redefining the logics of surveillance*. *Business & Society*, 58(1), 20–41.
- Whittaker, M., et al. (2018). *AI Now Report 2018*. New York University.
- Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and society*. Sage Publications.
- *Puttaswamy v. Union of India*, (2017) 10 SCC 1.
- Reddy, G. S. (2022). *Artificial intelligence and legal liability: Emerging issues*. *Indian Journal of Law and Technology*, 18(1), 89–110.
- Government of India. (1950). *Constitution of India*.
- Citron, D. K. (2019). *Hate crimes in cyberspace*. Harvard University Press.
- Kshetri, N. (2020). *The economics of deepfakes*. *IT Professional*, 22(2), 73–77.
<https://doi.org/10.1109/MITP.2020.2976092>
- Reddy, G. S. (2022). *Artificial intelligence and legal liability: Emerging issues*. *Indian Journal of Law and Technology*, 18(1), 89–110.
- Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and society (3rd ed.)*. Sage Publications.
- Casey, E. (2011). *Digital evidence and computer crime (3rd ed.)*. Academic Press.
- Citron, D. K. (2019). *Hate crimes in cyberspace*. Harvard University Press.
- Government of India. (1872). *Indian Evidence Act, 1872*.
- Kshetri, N. (2020). *The economics of deepfakes*. *IT Professional*, 22(2), 73–77.
<https://doi.org/10.1109/MITP.2020.2976092>

***Title: Artificial Intelligence-Driven Cyber Morphing Against Women in India:
Legal Challenges, Evidentiary Issues, and Policy Responses,
Authored By: Dr. Savita Chaudhary, Assistant Professor of Law, Awasthi
College of Law, Solan.
Email ID: savyychaudhary@gmail.com.***

- Reddy, G. S. (2022). *Artificial intelligence and legal liability: Emerging issues. Indian Journal of Law and Technology, 18(1), 89–110.*
- Whittaker, M., Crawford, K., Dobbe, R., et al. (2018). *AI Now Report 2018. New York University.*
- Kshetri, N. (2020). *The economics of deepfakes. IT Professional, 22(2), 73–77.*
<https://doi.org/10.1109/MITP.2020.2976092>
- Reddy, G. S. (2022). *Artificial intelligence and legal liability: Emerging issues. Indian Journal of Law and Technology, 18(1), 89–110.*

