

USE OF AI IN CRIMINAL ACTIVITIES AMONG WOMEN

1. Muhammad Mujahid Azeem

M.Phil Scholar, Department of Sociology, Riphah International University, Faisalabad

Email: mujahidazeem3838@gmail.com

2. Dr. Asma Islam

Email: drasmaislam@gmail.com

Abstract

The increasing integration of artificial intelligence (AI) technologies into daily life has created new avenues for criminal activity. While male-dominated narratives of cybercrime persist, emerging patterns suggest a growing involvement of women in AI-facilitated criminal behavior. This study explores the intersection of gender, technology, and crime by examining how women engage in and benefit from AI-enabled criminal activities. Drawing on case studies, academic literature, and criminological theories, this paper investigates the motivations, methodologies, and sociotechnical dynamics that drive women's participation in such offenses. The study also highlights how AI blurs traditional boundaries between victim and perpetrator and challenges law enforcement frameworks. Implications for gender-sensitive policy, digital forensics, and AI governance are discussed. This research aims to provide a nuanced understanding of the gendered dimension of AI crime and contribute to both criminology and AI ethics discourse.

Keywords: Artificial Intelligence, Women and Crime, Cybercrime, Gender and Technology, Digital Criminology, AI Ethics, Female Offenders.

Introduction

In the 21st century, artificial intelligence (AI) has emerged as a transformative force, revolutionizing not only industries and services but also the nature and scope of criminal behavior. AI applications, from machine learning algorithms to natural language processing and facial recognition, have introduced novel tools for both lawful and unlawful purposes. While scholarship has largely focused on male perpetrators in the digital crime landscape, recent developments suggest a quiet yet significant rise in women's involvement in AI-driven criminal activities. This growing trend raises critical questions about how gender intersects with technological evolution in the realm of crime.

Traditionally, criminal justice systems and academic studies have marginalized female offenders, often portraying them as peripheral actors or victims rather than active agents (Chesney-Lind & Pasko, 2013). However, as digital spaces become more accessible and anonymous, women are finding new avenues to engage in cyber-enabled crimes such as identity theft, fraud, surveillance-based blackmail, and AI-assisted deepfake production. Unlike physical crimes, AI-based offenses require less physical strength and more cognitive or technical expertise traits not limited by gender. The blurring of traditional criminological boundaries through AI raises urgent theoretical and practical concerns for policymakers, law enforcement agencies, and gender-focused criminology.

This study addresses an understudied dimension of AI and criminality by focusing on the unique motivations, strategies, and ethical dilemmas associated with women's participation in AI-facilitated criminal acts. It seeks to answer key questions: What types of AI-enabled crimes are women engaging in? What social, psychological, or economic factors drive their involvement? How do these patterns compare with male-driven AI crimes? And what implications do these developments have for AI governance and gender-sensitive justice systems?

The research is grounded in a multidisciplinary framework combining feminist criminology,

routine activity theory, and technological determinism. It draws on global case studies, statistical data, and scholarly analysis to build a comprehensive understanding of the issue. In doing so, it contributes to filling the gap in existing literature on cybercrime, which often overlooks the complexity of female criminality in digital contexts.

By exploring this intersection of gender and emerging technologies, the study aims not only to uncover the patterns and consequences of AI-enabled crimes involving women but also to advocate for inclusive, evidence-based policy interventions. As AI continues to reshape the landscape of opportunity and deviance alike, understanding its gendered dimensions is vital to ensure justice, security, and ethical digital development.

Literature Review

The literature exploring the intersection of artificial intelligence (AI), gender, and criminal behavior remains in its infancy. Existing research has largely focused on the technical aspects of AI-driven crime or the psychological profiles of male perpetrators. However, emerging studies and theoretical frameworks offer valuable insights for understanding women's engagement in AI-enabled criminal activities. This review synthesizes relevant work across criminology, gender studies, and technology to establish the foundation for the present research.

1) Feminist Criminology and the Digital Turn

Feminist criminology has long challenged the male-centric narratives that dominate criminal justice discourse, emphasizing the need to examine female agency, socio-economic motivations, and the contextual nature of women's offenses (Chesney-Lind & Pasko, 2013). As crime moves into digital domains, scholars argue for a reassessment of how gender dynamics manifest in virtual spaces. The internet and AI technologies have offered women not only new tools of empowerment but also novel means of subversion and transgression (Noble, 2018).

A key insight from feminist scholarship is that traditional models of deviance often fail to account for the structural constraints and motivations behind female offending. For instance, economic vulnerability, domestic coercion, or patriarchal marginalization may contribute to women's involvement in AI-enabled fraud, data theft, or extortion. Importantly, the anonymity and accessibility of digital tools challenge stereotypes of women as passive or non-technical, instead presenting them as increasingly competent digital actors.

2) Routine Activity Theory and Technological Crime

Routine activity theory (Cohen & Felson, 1979), which posits that crime occurs when a motivated offender, suitable target, and lack of capable guardianship converge in time and space, has been adapted to explain cybercrime. In AI-driven environments, this convergence is redefined by the virtuality of actors, data, and systems. For example, a woman with access to AI-driven bots may exploit weak cybersecurity protocols to commit fraud or orchestrate phishing schemes from behind anonymous avatars.

Recent adaptations of the theory highlight how AI alters traditional notions of opportunity structure. The low physical risk and high automation of AI tools make them especially attractive to non-traditional offenders, including women (Holt & Bossler, 2016). The theory thus supports the hypothesis that technological changes may reduce the gender gap in certain forms of deviance, particularly where skills and anonymity can substitute for brute force or traditional criminal networks.

3) Technological Determinism and Gendered Access to AI

Technological determinism suggests that technological innovation shapes societal structures and behaviors, including patterns of crime (Chandler, 2000). This theory helps explain how AI's diffusion across sectors like finance, healthcare, and communication has enabled new methods of criminal exploitation. For instance, AI-generated deepfakes have been used in

blackmail cases involving women as both victims and perpetrators (Kietzmann et al., 2020). Gendered access to technology is also evolving. Increasing digital literacy among women globally, especially in developing regions, has opened avenues for both legitimate employment and illicit experimentation with AI tools. While historically excluded from high-tech criminal networks, women now participate in activities such as algorithmic manipulation of financial markets, chatbot-driven scams, and AI-assisted surveillance.

4) Empirical Research on Female Cybercrime Participation

Empirical studies on women in cybercrime remain limited but growing. Leukfeldt et al. (2019) found that while male offenders still dominate the cybercrime landscape, female actors are significantly present in roles requiring social engineering, deception, and content manipulation areas where AI enhances efficacy. Other studies have noted that women are more likely than men to use AI tools in crimes involving relational dynamics, such as revenge pornography, identity theft in intimate relationships, or emotionally manipulative fraud schemes (Maras, 2015).

Moreover, recent law enforcement data indicates an uptick in women apprehended for crimes involving AI-generated fake documents, voice synthesis in impersonation scams, and the use of AI bots in online gambling rings. These developments suggest that the barriers to technical crime participation are eroding and that gendered profiles of offenders must be updated accordingly.

Summary of the Literature Gap:

While existing literature provides theoretical grounding, it lacks a focused analysis of how women specifically engage in AI-enabled crimes, what tools they use, and the unique ethical and policy issues they raise. This study seeks to address this critical gap.

Methodology

This study adopts a qualitative exploratory design aimed at understanding the patterns, motivations, and mechanisms of AI-enabled criminal activities involving women. Given the nascent nature of this research area and the ethical challenges in acquiring direct participant data on criminal behavior, the methodology relies on secondary data analysis, case study evaluation, and thematic synthesis from documented reports, academic literature, and verified media investigations.

1) Research Design

The research utilizes a non-empirical qualitative approach, which is suitable for analyzing underexplored, ethically sensitive domains such as female involvement in AI-assisted crime. This approach emphasizes theoretical development and thematic analysis over numerical generalizability. It draws primarily on:

- Peer-reviewed academic articles
- Digital forensic and law enforcement reports
- NGO and international cybercrime databases (e.g., INTERPOL, Europol)
- Documented legal cases and verified news sources

This design enables the examination of nuanced factors such as social context, identity, and power relations that may be lost in quantitative analysis.

2) Data Collection

Data was collected from 2015 to 2024 using purposive selection criteria. Sources were included if they:

- Documented involvement of women in crimes involving AI tools or systems
- Provided credible case evidence, such as court proceedings, government investigations, or research studies
- Focused on crimes such as AI-driven fraud, deepfakes, digital impersonation,

phishing, and surveillance

A total of 24 case studies were reviewed across jurisdictions including the United States, the United Kingdom, India, Pakistan, Nigeria, and Russia. Particular attention was paid to regions where women have increasing digital access but weak legal oversight of AI technologies.

3) Analytical Framework

Data was examined through thematic analysis following Braun and Clarke's (2006) methodology. The process involved:

- Familiarization with the data
- Generation of initial codes (e.g., "social engineering," "financial coercion," "AI tool misuse")
- Theme development (e.g., "gendered access to digital tools," "AI as an anonymity enabler")
- Review and refinement of themes in relation to the research questions

The analysis was further informed by feminist criminological theory and routine activity theory, enabling a dual focus on both structural and situational factors contributing to female participation in AI-based crimes.

4) Ethical Considerations

Due to the sensitive and potentially incriminating nature of the topic, this research did not involve direct interaction with individuals or digital forensic tools. All data was drawn from publicly available and ethically approved sources. Anonymity and accuracy of all referenced individuals were ensured based on source documentation.

The study adheres to the ethical guidelines for secondary research in criminology, avoiding the glamorization or trivialization of criminal behavior and ensuring a critical stance toward the use of AI in illegal contexts, regardless of gender.

Findings and Case Analysis

This section synthesizes patterns found in the qualitative data through selected global case studies. The findings reveal three major themes: the use of AI for financial exploitation, manipulation of digital identity, and involvement in AI-generated content crimes such as deepfakes. Each theme is illustrated with representative cases involving women across various socio-economic and national contexts.

1) Financial Fraud and AI-Driven Social Engineering

AI-enhanced social engineering such as automated phishing and voice-cloning scams has become a domain where women are increasingly involved, particularly in financial fraud schemes.

Case 1: India – AI-Generated Voice Scam (2021)

A 29-year-old woman from Delhi was part of a cyber-fraud group that used AI voice synthesis tools to impersonate bank representatives. The group cloned official voices from call recordings using publicly available AI software and targeted elderly customers with fake account warnings. Her role involved crafting emotionally persuasive scripts and handling victims over the phone using the cloned voices. Police investigations revealed the fraud ring generated over ₹1.2 crore (approx. \$150,000 USD) in just three months (Times of India, 2021).

Interpretation:

This case highlights women's participation in technically supported emotional manipulation, an area often linked with female communication strengths and sociolinguistic proficiency. It also underscores how low-cost AI tools can empower non-technical actors to exploit systemic vulnerabilities.

2) Identity Theft and Algorithmic Impersonation

AI tools have enabled the automation and scaling of identity-related crimes. Women have been found engaging in this sphere by targeting victims through dating apps, social media platforms, and virtual service portals.

Case 2: United Kingdom – AI-Assisted Romance Fraud (2019)

A woman in Birmingham was convicted for orchestrating an online romance scam involving AI-generated images and chatbots. Using deep learning tools to create highly convincing fake profiles of men, she lured middle-aged female victims, convincing them to send money for fabricated medical emergencies. She operated at least 10 false identities simultaneously with support from AI chatbots trained to maintain conversation consistency (BBC News, 2020).

Interpretation:

This case illustrates the increasing sophistication with which female offenders exploit trust-based digital relationships. AI enabled the offender to automate deception at scale, suggesting how emotional and technical intelligence converge in emerging digital crimes.

3) Deepfake Creation and Extortion

The production of synthetic media, particularly deepfake images and videos, is a growing field of digital abuse. Although most research focuses on female victims, there is a growing number of cases where women have used deepfake technology for revenge or extortion.

Case 3: United States – Cheerleader Deepfake Scandal (2021)

In Pennsylvania, a woman was arrested for creating deepfake videos of her daughter's cheerleading competitors. She used AI tools to fabricate compromising videos and photos and anonymously sent them to the school administration, intending to discredit the girls and eliminate competition for her daughter (CNN, 2021). The woman used free deepfake applications and basic editing skills.

Interpretation:

The case is significant because it showcases a parent (and woman) using AI tools not for financial gain but for social manipulation and control. It illustrates how AI technologies are accessible enough to be weaponized in petty personal rivalries, extending the range of potential offenders.

4) Surveillance and Coercive Control

AI-based surveillance tools, such as GPS spoofing, facial recognition abuse, and spyware apps, have also been weaponized by women in contexts of interpersonal coercion or custody disputes.

Case 4: Nigeria – AI-Driven Parental Surveillance (2023)

A woman was found using AI-enhanced spyware to track her ex-husband and children's digital behavior amid a bitter custody dispute. The software enabled her to intercept encrypted communications and manipulate digital records to frame her former spouse for negligence. The case drew national attention due to the AI tool's ability to bypass routine encryption barriers and mimic official notifications (Vanguard Nigeria, 2023).

Interpretation:

This case reveals how AI tools may be misused for coercive control, reversing traditional gendered victim-perpetrator roles. It also raises concerns about the ease with which commercial AI software can be deployed in intimate partner disputes with legal consequences.

Summary of Findings

The four cases reveal a spectrum of AI-enabled crimes involving women:

- AI tools reduce barriers to entry, enabling non-technical users to commit sophisticated offenses.

- Female offenders often exploit emotional, social, or relational dynamics enhanced by AI tools.
- Women's involvement is not limited to financial motives but includes reputation-based and interpersonal control strategies.
- Global accessibility of AI tools means such crimes are not restricted to high-tech societies.

Discussion

The findings of this study illustrate the growing intersection of gender, technology, and deviance in the AI era. While female criminality has traditionally been viewed through a narrow lens often limited to either victimhood or minor accomplice roles the cases examined reveal a more complex and active engagement with AI-enabled tools for criminal purposes. This section analyzes these developments through feminist criminology, routine activity theory, and broader legal and ethical frameworks.

1) Rethinking Female Criminality in the Digital Age

Feminist criminology challenges the essentialist portrayal of women as non-criminal or less capable of committing sophisticated crimes. The involvement of women in AI-assisted offenses dismantles traditional binaries of male aggressor versus female victim. In the case of the UK romance scam, for example, the female offender leveraged social trust, AI chatbots, and algorithmic manipulation to engage in deception with technical sophistication.

As Chesney-Lind and Pasko (2013) argue, crime must be understood within the social structures and motivations that shape women's choices. Many female offenders in AI crimes appear to be driven by a blend of economic vulnerability, social pressure, or parental ambition as seen in the cheerleader deepfake scandal. Unlike traditional white-collar crimes dominated by systemic greed, these cases often involve social or emotional motivations augmented by accessible AI tools.

2) AI and Routine Activity Theory: Redefining Opportunity Structures

Routine activity theory (Cohen & Felson, 1979) posits that a motivated offender, a suitable target, and the absence of a capable guardian result in crime. In AI contexts, the "guardian" is typically weak cybersecurity, while the "target" is increasingly abstract such as a person's digital identity or trust.

AI has shifted the opportunity structure by reducing the need for physical presence, technical skill, or criminal networks. This is particularly relevant for female offenders, who may operate in domestic environments while conducting AI-enhanced frauds or surveillance, thereby lowering the threshold of risk and increasing the feasibility of criminal action.

Moreover, AI provides automation, anonymity, and reach three features that allow women with limited traditional power (e.g., physical force or social status) to exert influence through digital means.

3) The Ethics of Empowerment vs. Exploitation

There is a paradox at play: the same AI technologies that empower women economically and socially can also be exploited for deviance. This duality creates an ethical challenge. The Indian voice scam case, for example, demonstrates how democratization of AI tools like voice synthesis originally designed for accessibility and efficiency can be repurposed for manipulation and theft.

Furthermore, gendered use of AI raises distinct ethical concerns. Women are disproportionately represented as victims of deepfake pornography (Chesney & Citron, 2019), yet the same tools are being used by women for extortion or control. This dual positioning complicates policy interventions that often assume clear-cut victim-perpetrator roles.

4) Law Enforcement Blind Spots and Gender Bias

Another key concern is that law enforcement and digital policy often suffer from gendered blind spots. Female offenders may go unnoticed longer due to stereotypes of women as “less threatening” or non-technical. As Maras (2015) notes, this bias affects both investigation priorities and sentencing outcomes.

Additionally, legal systems are still adapting to AI-related crimes. Many jurisdictions lack specific legislation to address synthetic identity crimes, AI voice cloning, or deepfake misuse. This legal lag allows both male and female offenders to exploit regulatory gray areas. However, without a gender-sensitive understanding, efforts to combat such crimes may fail to account for the unique ways women both perpetrate and experience AI-driven criminality.

5) Toward a Gender-Sensitive AI Governance Framework

To address these challenges, gender must be integrated into digital crime policy and AI governance. A few key recommendations include:

- Inclusion of gender analytics in AI risk assessments
- Gender-aware digital forensics training for law enforcement
- Creation of public awareness campaigns on non-physical forms of AI-based abuse
- Legal reform that criminalizes AI misuse comprehensively, with safeguards against biased profiling
- Only through such integrated frameworks can justice systems effectively respond to the new gender dynamics of AI-driven crime.

Challenges and Ethical Considerations

The integration of artificial intelligence (AI) into criminal activities especially those involving female perpetrators raises a host of challenges and ethical dilemmas for law enforcement, policy makers, and society. These complexities are compounded by the dual-use nature of AI tools, the anonymity of cyberspace, and longstanding gender biases in criminal justice systems.

1) Legal and Regulatory Gaps

One of the foremost challenges is the absence of comprehensive legislation addressing AI-specific crimes. While cybercrime laws exist in many jurisdictions, they often fail to account for the autonomous, scalable, and adaptive nature of AI tools. For example, existing identity theft statutes do not cover the use of AI-generated deepfakes or voice clones, leading to prosecutorial loopholes. This is especially problematic in transnational contexts where data, victims, and perpetrators often reside in different countries.

Women involved in AI-based crimes may exploit these legal gray zones, particularly in regions with weak cyber governance. In the Nigerian parental surveillance case, existing child custody laws and cyber security statutes proved insufficient to address the digital manipulation involved.

Ethical concern: How can legal systems maintain fairness while rapidly adapting to technical innovation? Rapid lawmaking without due diligence may result in over-criminalization or biased surveillance of female users, especially in patriarchal societies.

2) Attribution and Anonymity

AI-based crimes pose significant challenges in attribution. Many crimes are committed using avatars, bots, or anonymized email addresses, which hinders proper identification. This issue is compounded when female offenders operate behind male digital identities or vice versa, making gender-based analyses even more complex.

Additionally, automated AI tools such as generative chatbots or algorithmic trading bots can operate independently once activated. If a woman programs an AI tool to run scams autonomously, is she responsible for each act? These questions blur ethical lines of intent,

agency, and culpability core principles of criminal law.

3) Victim-Perpetrator Duality

Women in AI-related crimes may simultaneously embody both victim and perpetrator roles. A woman may be coerced by a partner or financial desperation to engage in AI fraud, or she may have previously been a victim of AI-based surveillance and now uses similar tools to retaliate. This duality complicates legal adjudication and ethical judgments.

As Noble (2018) observes, the digital sphere does not operate on binary moral frameworks. The same tool such as a facial recognition application may be used to find a missing child or stalk an estranged spouse. Ethical decisions about AI misuse cannot be made in isolation from context, especially gendered context.

4) Technological Accessibility and Misuse

The low barrier to entry for AI tools is a significant ethical concern. With the rise of open-source machine learning models and user-friendly deepfake apps, even individuals with limited technical knowledge can engage in harmful activities. Women with basic smartphone skills can now produce synthetic media, automate phishing emails, or manipulate financial data actions that once required entire teams of hackers.

Ethically, this raises the issue of responsibility in tool design. Should developers be held accountable for the misuse of AI products? How much user education or safeguards are necessary to prevent abuse? These questions remain largely unresolved, creating ethical ambiguity for both creators and users of AI tools.

5) Gender Bias in AI Governance and Enforcement

AI governance frameworks often lack gender-sensitive safeguards. Technologies like predictive policing and facial recognition have been shown to exhibit racial and gender bias, disproportionately misidentifying women and people of color (Buolamwini & Gebru, 2018). In the context of AI crimes committed by women, there is a risk of either overlooking female suspects due to stereotypes or over-policing women under assumptions of emotional instability or social deviance.

This underscores the need for ethical AI governance that includes diverse voices in AI development, equity audits, and transparent accountability measures to prevent both technological and judicial bias.

Summary

The ethical and legal challenges of women's involvement in AI-enabled crimes demand urgent interdisciplinary attention. These issues cannot be resolved through criminal law alone but require reforms in technology development, AI education, digital ethics, and gender policy.

Conclusion

The growing use of artificial intelligence in criminal activities marks a new chapter in the evolution of deviance, one where traditional boundaries of gender, space, and intent are being fundamentally reshaped. This study has sought to explore a relatively under-investigated dimension of this phenomenon: the role of women in AI-enabled criminal behavior. Through a synthesis of theoretical frameworks and global case studies, it has demonstrated that female offenders are not only active participants but, in many cases, are redefining the typologies and tactics of digital crime.

Feminist criminology reveals how systemic inequalities and socio-emotional motivations often drive women's engagement in crime, while routine activity theory helps explain how AI has lowered barriers to entry and altered opportunity structures. The selected case analyses from romance frauds in the UK to deepfake manipulation in the US and AI surveillance in Nigeria highlight the global, multifaceted nature of this issue.

The ethical and regulatory challenges that emerge from this research are considerable.

Women's involvement in AI-assisted crime complicates conventional narratives of offender and victim, especially in digital environments where identity is malleable and accountability is diffuse. The dual-use nature of AI tools, combined with inadequate legal frameworks and technological accessibility, allows women like their male counterparts to exploit both systemic and interpersonal vulnerabilities with increasing sophistication.

To address these challenges, it is imperative to develop gender-inclusive digital crime policies, comprehensive AI legislation, and ethical oversight mechanisms that reflect the complexities of technological crime in the 21st century. Without this, both enforcement and prevention strategies risk being incomplete, ineffective, or unjust.

This study contributes to the ongoing discourse in criminology and AI ethics by offering a gender-focused perspective on digital deviance. It invites further empirical research into the socio-technical factors that influence female participation in AI-related crimes and calls for cross-disciplinary collaboration to develop responses that are not only effective but equitable and informed by lived realities.

References

- BBC News. (2020, February 14). Woman jailed for £250k romance scam using fake online identities. <https://www.bbc.com/news/uk-england-birmingham-51493700>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp063oa>
- Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, 81, 77–91.
- Chandler, D. (2000). Technological or media determinism. LSE Media Research.
- Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107(6), 1753–1819. <https://doi.org/10.2139/ssrn.3213954>
- Chesney-Lind, M., & Pasko, L. (2013). *The female offender: Girls, women, and crime* (3rd ed.). SAGE Publications.
- Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588–608. <https://doi.org/10.2307/2094589>
- Holt, T. J., & Bossler, A. M. (2016). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Routledge.
- Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C. (2020). Deepfakes: Trick or treat? *Business Horizons*, 63(2), 135–146. <https://doi.org/10.1016/j.bushor.2019.11.006>
- Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2019). Cybercrime and the organization of offending: Scripts, networks, and coordinated activities. *Trends in Organized Crime*, 22, 1–12. <https://doi.org/10.1007/s12117-018-9336-6>
- Maras, M. H. (2015). *Cybercriminology*. Oxford University Press.
- Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. NYU Press.
- Times of India. (2021, November 15). Cyber fraud gang used AI tools to dupe elderly. <https://timesofindia.indiatimes.com>
- Vanguard Nigeria. (2023, July 28). AI surveillance used in bitter custody dispute, woman arrested. <https://www.vanguardngr.com>