INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW
An International Open Access Double Blind Peer Reviewed, Referred Journal

Volume 5 | Issue 4 | 2026 Art. 50

Shifting Nature of Crime: From Human to Artificial Intelligence

Mahima Raghuwanshi
Law Student, B.A.LL.B. (Hons.),
Institute of Law & Legal Studies, Sage University, Indore

Recommended Citation
Mahima Raghuwanshi, *Shifting Nature of Crime: From Human to Artificial Intelligence*, 5 IJHRLR 725-736 (2026).
Available at www.ijhrlr.in/current-issues/.

Shifting Nature of Crime: From Human to Artificial Intelligence

ABSTRACT

The rise of artificial intelligence (AI) is reshaping our world in ways that go far beyond boosting productivity, transforming healthcare, or changing how we communicate. It's also rewriting the rules of crime. What was once the domain of human-driven offenses—fraud, theft, manipulation—is now evolving into a landscape where AI plays a central role. Increasingly, we're seeing criminal activity that is not only aided by AI but, in some cases, carried out autonomously by it. This paper explores that shift, tracing how crime has moved from traditional human actions into a new era of AI-mediated and AI-powered enterprises. By tracing the historical trajectory of criminal behavior, from pre-digital offenses through the age of cybercrime, and into the contemporary era of machine learning-enabled malfeasance, this paper seeks to illuminate the mechanisms, motivations, and consequences of this transformation. The paper analyzes the key categories of AI-enabled crime, including deepfake fraud, algorithmic manipulation, autonomous cyberattacks, AI-assisted social engineering, and the weaponization of generative AI. It further examines the challenges that AI-driven crime poses to law enforcement agencies, the legal system, and international governance frameworks. Drawing on criminological theory, legal analysis, and technological literature, the paper argues that conventional crime prevention frameworks are fundamentally inadequate to address the speed, scale, and anonymity of AI-facilitated criminal conduct. Critically, this paper proposes a forward-looking framework for addressing the AI crime challenge, encompassing technical countermeasures, legislative reform, international cooperation, and ethical AI development standards. The conclusion asserts that without coordinated, proactive, and interdisciplinary responses, the asymmetry between AI-enabled criminals and law enforcement agencies will continue to widen, posing an existential challenge to public safety and democratic institutions.

KEYWORDS

Artificial Intelligence, Cybercrime, AI-Enabled Crime, Deepfakes, Autonomous Malware, Criminal Justice, Digital Forensics, AI Governance, Machine Learning, Social Engineering

1. INTRODUCTION

1.1 From Human Hands to Machine Minds: The Evolution of Criminal Activity in the Age of Artificial Intelligence

Crime has always changed with new technologies. From counterfeit money made possible by the printing press to wire fraud using the telegraph and online crimes without borders, each wave of technology has reshaped criminal behavior and forced society to rethink its defenses. Today, artificial intelligence marks a change that is not only faster but also fundamentally different. Once confined to research labs, AI is now part of daily life, bringing significant and often ignored effects on crime.

The numbers are staggering. Global cybercrime costs surpassed eight trillion dollars in 2023 and are expected to reach ten and a half trillion annually by 2025. These figures may only hint at what lies ahead. AI introduces abilities like pattern recognition, autonomous decision-making, natural language generation, and predictive modeling that do more than help criminals — they change what is possible. Small groups can now carry out operations that once needed large organizations, while complex tasks that required rare expertise can now be automated. AI-generated synthetic media further blurs the line between truth and fiction.

What makes this moment critical is the growing gap between the rapid pace of AI development and the slow evolution of our responses. Traditional criminology theories, law enforcement tools, and legal frameworks were built for human-driven crimes with clear intent and traceable actions. AI-enabled crime operates at machine speed, crosses borders easily, complicates questions of responsibility, and presents technical challenges that many institutions are not ready to face.

This paper looks at how crime is shifting from mostly human-driven activities to those increasingly influenced or started by artificial intelligence. It traces this change from pre-digital times through cybercrime to the current AI era, creates a classification of AI-enabled offenses, examines the relevance of existing criminology theories, discusses challenges for law enforcement and governance, and suggests a multidisciplinary response framework.

Using evidence from 2015 to 2025 with predictions extending to 2030, the paper acknowledges its focus on English-language sources and adopts a broad definition of AI crime that includes activities ranging from assisted acts to potentially autonomous ones. The key issue is not about precise definitions but whether our institutions can respond with the needed urgency and sophistication to this unfolding reality.

2. HISTORICAL EVOLUTION OF CRIME

2.1 The Roots of Digital Wrongdoing: A Historical Journey from Pre-Industrial Crime to the Rise of Organized Cybercrime

Crimes have never stayed constant. Crime has evolved in response to the technological, economic, and social conditions of its time. In pre-industrial society, most offences were local and personal. They involved physical contact and had a direct interaction with another individual. The industrial period saw an increase in fraud, espionage, and other financial crimes. Deception became more prominent after the introduction of the telegraph because of the time differences in message transmission.

Crime throughout history was a human activity. Law enforcement could easily identify and trace offenders since there is always a human factor to crimes. With the digital age, many challenges have emerged in identifying crimes and tracking them. Beginning in the 1970s, computer networking and the internet eliminated the need for proximity. Crimes could now be automated, mass-produced for virtually no cost, and committed against new forms of digital assets such as data and electronic cash.

Cybercrimes initially required personal initiative, as shown by the Morris worm and Kevin Mitnick attacks. The late nineties marked a transition in criminal conduct from individual initiatives and efforts to a business model. The internet commercialisation allowed for the development of data markets, exploit kits, and crime-as-a-service models, including ransomware. Organised groups developed sophisticated structures, and nation-states blurred the lines between crime and espionage, as demonstrated by Stuxnet in 2010.

By the early 2020s, the human role in crime had become more distributed and mediated through technology. This set the stage for artificial intelligence to introduce an even more profound shift in criminal capability.

3. UNDERSTANDING AI AND ITS CRIMINAL POTENTIAL

3.1 Intelligence as a Weapon: Understanding How Artificial Intelligence is Being Exploited for Criminal Purposes

Artificial intelligence refers not to one tool, but rather a suite of many tools. These tools include machine learning for recognizing patterns, deep learning for advanced pattern recognition, natural language processing for understanding and producing text and speech, computer vision for analyzing visuals and videos, and generative AI for

synthesizing realistic imagery, audio, and video.

All types of AI do not have equal applications for committing crimes. In particular, those AI functions most relevant for committing crime involve the synthesis of media, automation, optimization, vulnerability discovery, and the analysis of personal information.

AI can be viewed as both a tool used by the human user to augment criminal activity and an autonomous actor, which at the moment remains unlikely, though increasingly possible. The former will serve as the focus of the present paper.

Machine learning offers great utility to criminals, since it can recognize patterns and optimize outcomes in ways that are highly effective in committing certain crimes. ML offers great benefits in terms of fraud through the synthesis of content, personalization of phishing, and adversarial methods for outwitting security measures. The emergence of generative AI has lowered the bar of entry and allows non-specialists to quickly synthesize realistic-looking media.

4. TAXONOMY OF AI-ENABLED CRIMES

4.1 Faces, Lies, and Algorithms: The Expanding Landscape of AI-Enabled Criminal Threats

Among other concerning innovations in artificial intelligence crimes, the development of deepfake technology stands out. Modern deep learning techniques allow criminals to generate incredibly realistic synthetic videos, audios, and images of people, thus destroying the very idea of trusting our senses.

Deepfakes are primarily created and circulated in the context of non-consensual intimate imagery, which accounts for more than 95 percent of deepfake videos uploaded in 2023. The victims, predominantly women and minors, suffer tremendous psychological, social, and emotional damage. In politics, deepfakes may forge videos featuring political leaders and affect the course of elections. Moreover, the "liar's dividend" increases because people become inclined to reject any evidence of their existence, regarding it as potential deepfaking.

Another way in which AI has been transformative is through its use in malware, which has become increasingly adaptive by allowing itself to adapt on the go and even identify weaknesses automatically while launching attacks. Social engineering tactics have become incredibly powerful with the use of personalized phishing emails and realistic interactions by AI. AI has been used in mass propaganda and radicalization by terrorist organizations.

Some of the future challenges posed by AI include the creation of bioweapons and attacks against AI itself through adversarial data inputs and poisoning of data.

5. CRIMINOLOGICAL THEORIES APPLIED TO AI CRIME

5.1 Old Theories, New Realities: Applying Classical Criminological Frameworks to the Age of AI-Enabled Crime

Crime has been explained through various criminological theories since ancient times. Three of such theories, namely Routine Activity Theory, Rational Choice Theory, and Social Learning Theory, continue to be relevant; however, these theories show certain flaws when analyzing AI-related criminal activity.

The Routine Activity Theory posits that there is crime only when an interested party commits it on an available victim in the absence of appropriate guardianship. With regard to AI, these factors change due to the expansion of interested parties (as a result of lower technical requirements), ease of finding the victim, and poor guardianship due to speed and efficiency of the attacks.

According to Rational Choice Theory, crimes are made through a calculation process where the offender weighs the pros and cons. In case of AI, it becomes easy for offenders to gain from their activities and minimize risks associated with them. However, the theory does not account for autonomous artificial intelligence.

Social Learning Theory explains how criminal knowledge spreads through social networks. AI goes further by actively generating new criminal knowledge and acting as a personalized tutor, making sophisticated techniques accessible to beginners and accelerating the spread of harmful capabilities.

These theories highlight both continuities and the need for fresh thinking in addressing AI crime.

6. LAW ENFORCEMENT AND LEGAL CHALLENGES

6.1 Beyond Human Reach: The Legal, Forensic, and Jurisdictional Challenges of Prosecuting AI-Enabled Crime

A functioning criminal justice system fundamentally depends on its ability to clearly identify who is responsible for harmful acts. Without reliable attribution, effective prosecution and deterrence become nearly impossible.

Traditional crime investigations rely on physical evidence, witnesses,

and records. While cybercrime already made attribution difficult through proxies and anonymity tools, AI-enabled crime pushes these challenges to a new level. Criminals can now use automated networks, synthetic identities, and adaptive machine learning to obscure their tracks and create convincing false trails that mislead investigators.

Jurisdictional complexities grow even more severe when attacks span multiple countries, with AI systems, infrastructure, victims, and money flows distributed globally. Evidentiary problems are equally troubling, as the "black box" nature of many AI systems makes it hard to link human intent to specific outcomes, and deepfakes increasingly undermine the reliability of video and audio evidence.

Current legal frameworks, designed decades ago, struggle particularly with questions of criminal intent when AI operates with growing autonomy. This creates serious liability gaps that weaken deterrence and demand urgent legal reform.

Social Learning Theory accounts for the diffusion of criminal information among social networks. On the other hand, AI technology not only disseminates but also creates criminal knowledge, becoming an intelligent tutor that simplifies sophisticated skills and hastens their dissemination among novices.

Both theories emphasize both continuity and innovation in solving the problem of AI crime.

7. GOVERNANCE, POLICY, AND INTERNATIONAL RESPONSE

7.1 Multi-Level Strategies for Governing AI-Enabled Crime

Efforts to combat AI crimes need to be carried out in concert by the government, international community, and private businesses. Such an approach is necessary due to the rapid development of AI technology.

Europe has shown leadership in this domain with the EU's 2024 AI Act, which regulates AI in a risk-based manner and requires such qualities as transparency, responsibility, and human oversight. In the US, there is a rather slow process with the implementation of the 2023 Executive Order and regulations regarding deepfakes. China has strong legislation regarding generative AI and deepfakes, whereas India and Singapore are still developing their regulatory strategies.

Internationally, there is the Budapest Convention, which needs to be updated. Technology firms participate in this process with voluntarily implemented safety measures. However, additional regulations from the government are crucial.

8. COUNTERMEASURES AND PROPOSED FRAMEWORK

8.1 Comprehensive Countermeasures Against AI-Enabled Crime: Technical, Legal, Educational, and Integrated Approaches

Successful strategies against crimes enabled by AI need to include a balanced approach that combines technological innovation, legislative updates, public enlightenment, and collaboration.

Technologically, advanced AI-based cybersecurity technologies have a vital part to play in crime prevention by analyzing patterns, recognizing attack signatures, and anticipating future cyber threats at an unprecedented speed compared to human capabilities. These technologies should continually update their features to keep up with new strategies employed by criminals. Tools such as C2PA can authenticate the source of digital files using cryptography and differentiate between legitimate content and artificial intelligence generated content. Privacy preserving technologies such as homomorphic encryption and zero-knowledge proof ensure data confidentiality while minimizing their attractiveness to criminals.

Legally, legislative measures are essential in creating clear legal standards for human accountability for AI-generated activities, including those under human control and more autonomous AI operations. Legislation can include offenses such as non-consensual deepfake creation, AI-based fraudulent activities, illicit data access, and interference in the electoral process. Developers of artificial intelligence should conduct tests for criminal misuse of their technologies, document associated risks, and report any incidents while enjoying protection from liability.

Both education and social initiatives are still essential. High levels of digital and media literacy will help citizens defend themselves against any phishing attacks, deep fakes, and manipulation. Continuous training for law enforcement is also required, along with dedicated teams and international cooperation, as well as educational initiatives in schools.

This type of approach should be based on four key principles: flexibility, coordination, responsibility, and proportionality. All of these elements together form a flexible, adaptable, and effective system of protection.

9. FUTURE TRAJECTORIES AND EMERGING THREATS

Prediction of the future of crimes enabled by artificial intelligence should be done considering the rapid development of AI technologies, methods adopted by criminals, and the ability of law enforcement agencies and government structures to respond to the new reality. Despite the

impossibility of making accurate predictions, certain clear tendencies may be noticed now.

Multimodal AI-based models that will work with texts, images, audio recordings, videos, and computer codes will increase criminals' opportunities significantly. Full autonomy of AI, meaning its capability to conduct criminal operations autonomously from the setting of a certain goal to attacks and money laundering, may be expected to develop within the next ten years.

Combination of AI with quantum computing, robotics, drones, and self-driving cars will produce new types of crimes which can unite virtual anonymity of cyberattacks with direct actions. Markets of AI products on the black market are growing rapidly, providing more opportunities for criminals.

AI will augment policing efforts through predictive analytics, automated forensics, and real-time detection. Nevertheless, such applications should be deployed cautiously to preserve civil rights and eliminate potential biases.

Essentially, the increased autonomy of AI calls into question existing notions of criminal responsibility. Tackling AI-facilitated crimes is inextricably linked to the issue of ensuring that AI is developed for the greater good of humanity.

10. CONCLUSION

In conclusion, the study has analyzed the development and growth of crime from its classical form of being a local affair committed by human offenders to being a phenomenon of a modern age, that is, cybercrime, as well as its future evolution into AI crimes, including potentially self-driving AI crimes. As a result, a number of key insights have been generated.

Firstly, AI-based crime is not merely more massive or faster; rather, it is completely different from anything we knew previously in terms of crime, changing the nature of crime altogether. The low barrier to entry, scaling potential, and new economic model of the illegal activity are complemented by the erosion of evidentiary basis, undermining trust, and raising ethical and legal issues related to the autonomy of AI. Current legislation appears to be totally unprepared.

Secondly, conventional approaches to fighting the crime are inadequate when dealing with an enemy based on artificial intelligence. Law-enforcing bodies are no longer equipped to handle this opponent due to its unparalleled speed, magnitude, anonymity, and global presence.

Concepts such as human intent and causality become irrelevant when dealing with the interaction of a human and AI offender.

Thirdly, there are no quick fixes here; a comprehensive, multi-dimensional approach is needed, including technological security, legal reform, stronger global cooperation, enhanced training of law enforcement officers and judges, and greater public knowledge to harden society. Technology, law, education, and leadership must align.

Fourthly, addressing AI-driven crime must be viewed as an integral part of broader AI governance. Today's decisions on technical capabilities, safety, and deployment will determine future crime risks for decades. Put safety, transparency, and individuals before profit and politics. It's our best defense against AI crime.

Fifthly, AI crime is a test case of whether humankind can keep pace with technology's breakneck development. We've recovered from telegrams, automobiles, and the internet – eventually – but only after causing a great deal of harm. The exponential speed of AI leaves us no time to waste.

AI transforming crime is not some science fiction scenario but a reality we're living now. Can our legal system, technologies, and institutions rise to the challenge? This paper is just the beginning; much interdisciplinary and international research lies ahead. But the warning bells are ringing.

REFERENCES

The following references represent the academic, legal, policy, and technical literature that informs this research paper.

Books

- Akers, R. L., DEVIANT BEHAVIOR: A SOCIAL LEARNING APPROACH (3d ed. 1985).
- Brundage, M. et al., THE MALICIOUS USE OF ARTIFICIAL INTELLIGENCE: FORECASTING, PREVENTION, AND MITIGATION (Future of Humanity Inst., Univ. of Oxford 2018).
- Castells, M., THE RISE OF THE NETWORK SOCIETY (2011).
- Goodfellow, I., Bengio, Y. & Courville, A., DEEP LEARNING (2016).
- Lessig, L., CODE: AND OTHER LAWS OF CYBERSPACE (Version 2.0, 2006).
- Rid, T., RISE OF THE MACHINES: A CYBERNETIC HISTORY (2016).
- Schneier, B., CLICK HERE TO KILL EVERYBODY (2018).
- Sternberg, R. J., ADAPTIVE INTELLIGENCE (2023).

- Sutherland, E. H., PRINCIPLES OF CRIMINOLOGY (4th ed. 1947).
- Wall, D. S., CYBERCRIME: THE TRANSFORMATION OF CRIME IN THE INFORMATION AGE (2007).
- Zuboff, S., THE AGE OF SURVEILLANCE CAPITALISM (2019).

Journal Articles

- Caldwell, M. et al., AI-Enabled Future Crime, 9 CRIME SCI. 14 (2020).
- Cohen, L. E. & Felson, M., Social Change and Crime Rate Trends: A Routine Activity Approach, 44 AM. SOC. REV. 588 (1979).
- Floridi, L. et al., AI4People—An Ethical Framework for a Good AI Society, 28 MINDS & MACHINES 689 (2018).
- Grabosky, P., Virtual Criminality: Old Wine in New Bottles?, 10 SOC. & LEGAL STUD. 243 (2001).
- Hadlington, L., Human Factors in Cybersecurity, 3 HELIYON (2017).
- Haynes, A. & Taylor, M., Deepfakes and the Law, 49 COMPUTER L. & SEC. REV. 105823 (2023).
- Jagsi, R., Artificial Intelligence and the Future of Medicine, 330 JAMA 1019 (2023).
- Jonason, P. K. et al., The Dark Triad and Cybercrime, 23 CYBERPSYCHOL. BEHAV. SOC. NETWORKING 572 (2020).
- Kshetri, N., Cybercrime and the AI Revolution, 56 COMPUTER 67 (2023).
- Leppink, E. W. et al., The Young and the Stressed, 204 J. NERVOUS & MENTAL DISEASE 931 (2016).
- Maras, M. H. & Alexandrou, A., Determining Authenticity of Video Evidence, 23 INT'L J. EVIDENCE & PROOF 255 (2019).
- McGuire, M., Why We Still Don't Understand Cybercrime, in THE PALGRAVE HANDBOOK OF INTERNATIONAL CYBERCRIME AND CYBERDEVIANCE (2020).
- Mirsky, Y. & Lee, W., The Creation and Detection of Deepfakes, 54 ACM COMPUTING SURVS. 1 (2021).
- Müller, V. C. & Bostrom, N., Future Progress in Artificial Intelligence, in FUNDAMENTAL ISSUES OF ARTIFICIAL INTELLIGENCE (2016).
- Newman, N., AI, Algorithms and Predictive Policing, 26 IPPR PROGRESSIVE REV. 48 (2019).
- Patel, R. K. & Bhatt, N., Ethical Implications of AI in Criminal Justice, 25 TRENDS ORGANIZED CRIME 459 (2022).
- Seker, S. E., AI-Enabled Cyberattacks, in CYBERSECURITY—ATTACK AND DEFENSE STRATEGIES (3d ed. 2021).

- Taddeo, M. & Floridi, L., Moral Responsibilities of Online Service Providers, 24 SCI. & ENG'G ETHICS 1575 (2018).
- Wall, D. S., The New Cybercrime Ecosystem, 22 CRIMINOLOGY & CRIM. JUST. 350 (2022).
- Walsh, P., AI and the Architecture of Crime, 5 INT'L J. CYBERSECURITY INTELLIGENCE & CYBERCRIME 1 (2022).
- Winick, B. J., Criminal Law and Artificial Intelligence, 70 UCLA L. REV. 188 (2023).

Reports / Institutional Publications

- Council of Europe, CONVENTION ON CYBERCRIME (ETS No. 185, 2001).
- Europol, CHATGPT: THE IMPACT OF LARGE LANGUAGE MODELS ON LAW ENFORCEMENT (2023).
- Interpol, GLOBAL CRIME TREND REPORT 2023 (2023).
- National Crime Agency (UK), NCTA ANNUAL CYBER THREAT ASSESSMENT 2023 (2023).
- OECD, RECOMMENDATION OF THE COUNCIL ON ARTIFICIAL INTELLIGENCE (2019).
- United Nations Office on Drugs and Crime, CYBERCRIME MODULE 14 (2023).
- White House, EXECUTIVE ORDER ON THE SAFE, SECURE, AND TRUSTWORTHY DEVELOPMENT AND USE OF ARTIFICIAL INTELLIGENCE, Exec. Order No. 14,110 (2023).