ARTIFICIAL INTELLIGENCE-ENABLED CYBERCRIME: CURRENT THREATS, LEGAL IMPLICATIONS, AND FUTURE REGULATORY PRIORITIES

DR. MAYANK MATHUR
Associate Professor, RV University, Karnataka, Email id: mayankm@rvu.edu.in

Abstract

Artificial intelligence has created new opportunities for cybercriminals by increasing the speed, scale, personalization, and adaptability of malicious activity. This review examines the major forms of artificial intelligence-enabled cybercrime and evaluates their legal, evidentiary, jurisdictional, regulatory, and human rights implications. Evidence from legal, criminological, cybersecurity, and technological literature was synthesised to identify current threats and governance gaps. The review covers AI-assisted phishing, automated social engineering, deepfakes, synthetic impersonation, adaptive malware, ransomware, biometric misuse, privacy violations, dark web markets, cryptocurrency laundering, and AI-supported criminal services. It also analyses challenges involving criminal attribution, civil and corporate liability, digital evidence authentication, forensic reliability, cross-border investigations, and international cooperation. Current legal frameworks remain fragmented and often struggle to address distributed responsibility, autonomous system behaviour, rapidly changing attack methods, and inconsistent enforcement capacity. Effective governance requires coordinated application of criminal law, cybersecurity regulation, data protection, platform accountability, and procedural safeguards. Developers, deployers, users, and service providers should be subject to proportionate obligations based on control, foreseeability, and risk. Future priorities include secure-by-design development, synthetic media provenance, validated forensic tools, specialist law-enforcement training, rapid evidence-preservation mechanisms, victim remedies, and harmonized international standards. A preventive, adaptive, and rights-respecting regulatory approach is essential to reduce AI-enabled cybercrime while preserving innovation, privacy, equality, freedom of expression, and due process.

Keywords: *Artificial intelligence, Cybercrime, Cybersecurity, Digital evidence, Legal regulation*

Introduction

Artificial Intelligence (AI) has emerged as a key element of digital transformation in the government, commercial, healthcare, financial, educational and legal sectors. It has been able to process huge amounts of data, look for patterns, make decisions automatically and produce realistic content, which has led to significant opportunities for efficiency and innovation. The same features have also helped the cybercriminals to increase their attack techniques.The same features have also made cybercriminals' attack techniques more powerful. AI helps with reconnaissance, automates phishing, creates content that is highly believable, uncovers system flaws, impersonates trusted individuals, and speeds up malicious operations.AI can aid in reconnaissance, automate phishing attacks, produce deceptive material, uncover system vulnerabilities, mimic trusted individuals and quickly facilitate malicious activities, all of which conventional cybercrime methods may not easily match. The dual-use nature of AI means that it touches various aspects of technological progress, cybersecurity governance, data protection, and criminal law, with the objectives of these regulating areas often being similar, but not necessarily compatible and, more significantly, institutionally distinct (Andraško et al., 2021).

Organizations are now more reliant than ever on interconnected systems, cloud services, automated platforms and data-driven processes, as a result of digital transformation. This reliance has exposed a larger attack surface and made the damage of a security breach more severe, especially when a company's risk-management processes are not well-developed, staff is untrained and their incident-response procedures are weak. Cybersecurity has thus emerged as a key part of institutional resilience in recent years, rather than just a technical function (Saeed et al., 2023). The legal profession is also experiencing a digital transformation as legal files are digitized, online dispute resolution, automated legal research, algorithmic legal advice and digitally managed evidence are transforming the law industry. These advancements make it easier and more efficient to access and operate the system, but they also present new challenges related to unauthorized access, data manipulation, data security, and accountability for automated processes (Fekolli et al., 2025).

AI-powered cybercrime is unique from traditional cybercrime in that it enables it to be faster, more adaptive, more personal and more pervasive. Generative systems can fool users into believing they are receiving a legitimate phishing message, a genuine document, malware, a fake identity and even a fabricated audio-visual content. Machine-learning tools can help attackers to profile their victims, so they can beat their systems, and use feedback to make their attacks more precise. These functions can help reduce technical difficulties to make it easier for offenders to operate, and enable more advanced operations by skilled actors. It is therefore important to note that new tactics on digital crime put new challenges for the defensive systems relying on static rules, delayed reporting and traditional offender profiles (Cassidy et al., 2024).

There's also a recognition of vulnerabilities in the current criminal justice system.There is also an awareness of the gaps in the current criminal justice system as a result of its development. Cybercrime legislation has been fashioned to fit the concept of human directed crime, a known perpetrator, and relatively fixed types of cyber evidence. The assessment of intention, causation, attribution and responsibility is made more difficult in the case of AI-powered offences, especially if harmful outputs are by developers, service providers, deployers, users and/or autonomous technical processes. The overlap of jurisdiction and the varied definitions also hinder investigation or prosecution when the offenders, victim and platforms, servers and financial transactions are in different countries (Amoo et al, 2024). Enforcement officials might also be hampered by their lack of forensic skills, technical expertise, and expertise in e-discovery, as well as by delayed access to evidence that might be out of their country's borders and by uncertainty about admissibility and authenticity of AI-generated content (Ali, 2024).

More is needed than criminalisation and individual acts for effective responses. The technical, organizational, regulatory, threat monitoring and coordinated enforcement aspects of cybersecurity governance must be integrated. AI can be used to reinforce compliance by continually assessing risk, detecting anomalies, auditing automatically, and identifying suspicious activity swiftly—these applications must be transparent, proportionate and be legally monitored (Oluoha et al., 2022). Criminological theories can also contribute to information security management frameworks to understand the motives of cybercrime perpetrators, the opportunity structures, the vulnerability of the victim, and the environment in which cybercrime occurs (Mushtaq & Shah, 2025). In order to tackle technologically enhanced crime within the national cyber policy, the policy should include all of the following measures: prevention regulation, institutional coordination, public awareness, reporting system and investigative capacity (Ezeji, 2024).

Special emphasis is attached to the relationship between security and the fundamental rights, as this could be a matter of privacy, equality, freedom of expression and due process if fundamental rights are infringed by having a surveillance system that is too large, monitoring too automatically and too much content is removed. The justification for regulation, however, requires that it be necessary, proportional, transparent, reviewable and remedial to those affected by it.

Automated fraud, deepfakes, malware, breach of privacy, dark-web activities, and AI-based criminal services are the main types of artificial intelligence-driven cybercrime that are explored in this review. It assesses important legal issues, liability, digital evidence, law-enforcement capacity, jurisdiction, human rights issues and legal responses. The review will seek to spot current gaps in the governance and to set priorities for future adaptive, rights-respecting and internationally coordinated governance.

Objectives of the review:

1.To identify the major forms and emerging patterns of AI-enabled cybercrime.
2.To examine associated legal, evidentiary, jurisdictional, and human rights challenges.
3.To evaluate regulatory responses and propose future governance priorities.
2. Conceptual Foundations of Artificial Intelligence-Enabled Cybercrime

Artificial intelligence cyber crime is defined as cybercrime in which AI systems take part of it, either in assisting, automating, scaling or changing it in a way that is harmful or illegal. The concept goes beyond the transgression of the machine itself, to encompass acts of theft where AI technology, and its various components such as machine learning, generative models, computer vision, natural language processing or autonomous agents, are used as tools in the criminal enterprise. These various technologies can be used to improve reconnaissance, victim profiling, deception, intrusion, evasion, and decision making which can help offenders to attack faster, more accurately, and more adaptively (Blauth et al., 2022).

There is a good difference between AI-assisted, AI-automated and AI-generated crime. In AI-assisted crime, humans guide the crime, while the AI tools help them make intelligent decisions and execute the crime; in AI-automated crime, a large portion of the crime is automated and driven by algorithms. AI-generated crime uses AI-generated text, images, audio, code or identities to facilitate or escalate criminal activity. This classification helps to provide greater clarity about the level of human control, and helps to facilitate more accurate judgements of intent, causation and responsibility. Additionally, there are existing taxonomies that differentiate attacks on AI models from attacks that are facilitated by AI, which include vulnerabilities such as data poisoning, model manipulation, adversarial inputs and system exploitation (Jeong, 2020).

Accessibility and scalability, together with a lower level of technical barriers, contribute to the dynamics of crime. AI technologies can also be adapted for phishing, fraud, malware creation, surveillance and misinformation, and there are specific technologies that can enable adaptive attacks and concealment (Saba'F et al., 2025). In a criminological lens, AI changes the ways in which offenders' capacity, opportunity, victim, and the interplay of human agents and technological autonomy are configured. Such changes demand cybercrime analysis to include in the process the combination of technical taxonomy, criminological theory, legal principles, and governance (Hayward & Maas, 2021). Table 1 indicates the main areas of AI-related cybercrime.

Table 1. Classification of Artificial Intelligence-Enabled Cybercrime

Category	Description	Common Applications	Principal Risks	Reference
AI-assisted crime	Human-directed offences supported by AI tools	Victim profiling, phishing preparation, vulnerability identification	Greater precision, reduced effort, increased attack success	(Blauth et al., 2022)
AI-automated crime	Offences in which algorithms perform substantial operational tasks	Automated reconnaissance, credential attacks, bot-driven fraud	High scalability, rapid execution, limited human intervention	(Jeong, 2020)
AI-generated crime	Criminal activity enabled through synthetic AI outputs	Fake identities, deceptive messages, synthetic images, malicious code	Impersonation, fraud, misinformation, evidentiary uncertainty	(Hayward & Maas, 2021)
AI-targeted attacks	Attacks directed against AI models or supporting infrastructure	Data poisoning, adversarial inputs, model manipulation	Corrupted outputs, compromised decision-making, system failure	(Saba'F et al., 2025)

3. Generative AI, Social Engineering, and Automated Fraud

GPT has significantly changed the landscape of social engineering, allowing criminals to generate humanly convincing, personalised and contextually appropriate deceptive messages at little cost. Large language models can create phishing emails, fraudulent messages, impersonation scripts that mimic professional communication styles and tailor to specific victims, and impersonate customer-service interactions. This feature helps prevent the common language errors that are often linked to phishing attacks and enable attackers to launch multilingual attacks at an unprecedented speed and scale (Schmitt & Flechais, 2024).

AI-driven social-engineering also helps to enhance the victim profiling and manipulation of behaviour. Analyse publicly available information on social media, work and professional websites, and from data breaches to discover personal interests, workplace roles, relationships, and vulnerabilities. These insights can be used by an offender to develop a very sophisticated investment fraud, a romance scam, a business email compromise, an executive impersonation scam, and employment fraud. The attacks are harder to identify as the technical sophistication and trust, urgency and emotional appeal of well-known principles of communication are unnecessarily exploited.

On all these attacks, human factors continue to be an important factor for success. Low levels of cybersecurity awareness, cognitive overload, common digital practices, and overemphasis on the visual and/or linguistic authenticity can make them susceptible. These are exacerbated through the use of generative AI, which generates content that meets the recipient's expectations, professional context, and communication style (Raja et al., 2025).

The rise of new platforms like FraudGPT and WormGPT and similar tools, where malicious actors can exploit

generative systems to enable their own phishing, fraud, malware communication, and other criminal activities, underscores the potential of generative systems to be tailored for these kinds of attacks without traditional safety filters. These resources reduce these technical constraints and deepen the reach of organised methods of cybercrime (Falade, 2023). Technical detection systems, user education, identity-verification processes, platform accountability and swift reporting systems are essential to good prevention. As seen in Figure 1, social engineering has evolved over time, progressing from basic to more sophisticated methods.

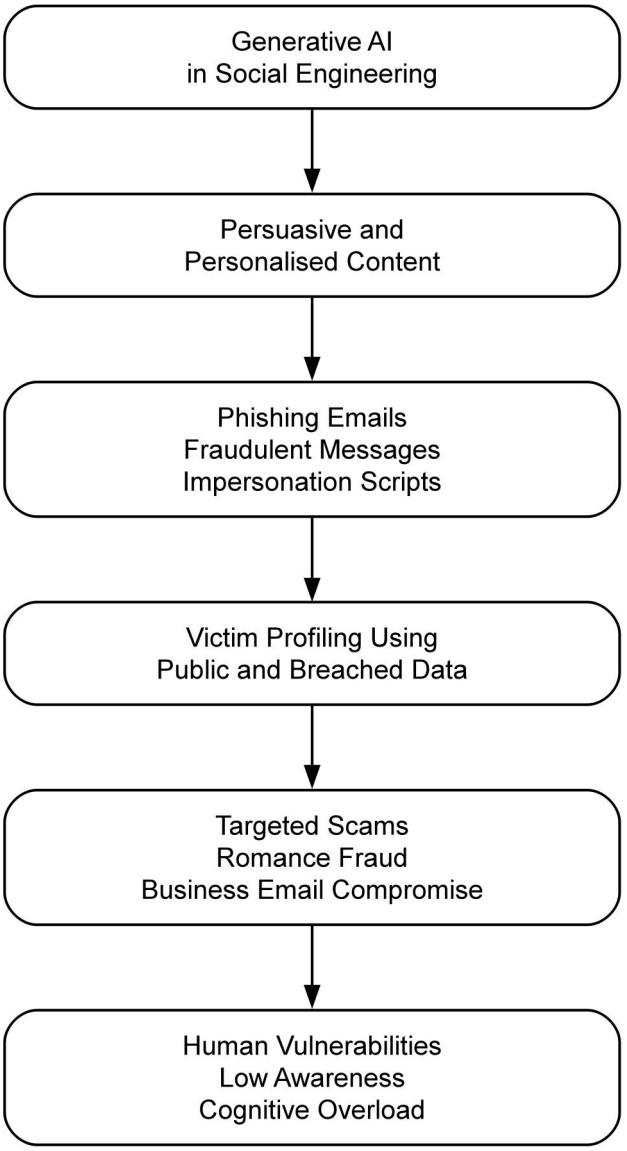

Figure 1. Generative Artificial Intelligence in Social Engineering and Automated Fraud

4. Deepfakes, Synthetic Media, and Digital Impersonation

Deep fake technology involves using artificial intelligence to create or alter audio, images and videos in which someone speaks or does something that they actually did not. The use of generative adversarial networks and other synthesis methods has led to higher fidelity, ease of access and faster production of synthetic media. All these have grown legitimate creative applications and posed serious concerns with respect to deception, reputational damage, privacy invasion and manipulation of public trust (Folorunsho & Boamah, 2025).

Deepfakes can be used for various purposes, including entertainment, education, fraud, harassment, politics, and extortion. People might pretend to be an executive, family member, public official or a financial representative, to solicit funds, confidential information, or access. Synthetic media can also be used for the purpose of creating false evidence, misinformation, the destruction of professional reputation or the manufacture of unwanted sexual material. There is greater potential for both victimization and social disruption as it is more difficult to identify authentic from manipulated material (Busacca & Monaca, 2023).

The hyper-realistic manipulation also engenders a broader evidence issue as true media can be belittled or rejected. This liar's dividend can make people question digital records, news, judicial evidence, as well as institutional communication. Deep fake manipulation of content is amplified by its fast spread across social media platforms, making it possible for discredited material to spread to large audiences well before it can be verified or removed (George & George, 2023).

Current laws mostly tackle the misuse of deepfakes in more general terms, such as in data protection laws, laws on defamation, privacy laws, laws on identity theft, laws on harassment or laws on intellectual property. These piecemeal solutions might not sufficiently resolve the issues of synthetic impersonation, platform liability, cross-border distribution and victim restitution. For effective regulation, the law needs to be clear and have a fast takedown process, set standards for content provenance, set accountability standards for platforms, and provide proportionate penalties for malicious use (Darma et al., 2025). Table 2 indicates the key types of generative AI-powered deception.

Table 2. Major Forms of Generative AI-Enabled Deception

Threat Type	AI-Enabled Mechanism	Typical Targets	Potential Consequences	Reference
Phishing	Generation of convincing and personalized emails or messages	Employees, consumers, financial institutions	Credential theft, financial loss, unauthorized access	(Schmitt & Flechais, 2024)
Business email compromise	Executive or organizational impersonation	Finance departments and corporate employees	Fraudulent transfers and disclosure of confidential data	(Yu et al., 2024)
Deepfake impersonation	Synthetic audio, video, or images replicating real individuals	Executives, public officials, family members	Fraud, extortion, reputational damage, misinformation	(Folorunsho & Boamah, 2025)
Romance and investment fraud	Automated emotional engagement and targeted persuasion	Social media and online-platform users	Financial exploitation and psychological harm	(Raja et al., 2025)
Malicious generative platforms	Unrestricted generation of deceptive content or attack materials	Inexperienced and organized cybercriminals	Lower technical barriers and wider access to cybercrime tools	(Falade, 2023)
Non-consensual synthetic content	Fabrication of intimate or defamatory media	Women, children, public figures, private individuals	Privacy violations, harassment, and social stigma	(Darma et al., 2025)

5. AI-Enhanced Malware, Ransomware, and Network Intrusions

AI is now impacting the creation, delivery and evolution of malware. Malicious software with artificial intelligence capabilities can study the target environment, change the way they operate, choose an attack path, and avoid traditional signature-based detection. These capabilities can enable malware to run more autonomously and persistently than normal programs. Machine-learning methods can also be used to enable faster and more advanced cyber attacks, such as automated reconnaissance, identification of vulnerabilities, targeting of credentials or lateral movements in compromised networks (Thanh & Zelinka, 2019).

Similar capabilities might be of value for ransomware campaigns. AI can help offenders to determine which systems are valuable, which systems are vulnerable, which are suitable for extortion messages, and what is the best means of encryption or data-exfiltration. Malware may adapt, postpone execution to evade sandbox analysis, and/or mimic legitimate processes. These methods make it more difficult to attribute and reduce the effectiveness of static defence measures.

AI is also vital in today's malware detection. Machine-learning models can identify suspicious files, analyse network traffic, detect anomalous behaviour, and identify previously unknown threats. They rely on representative training data, the robustness of the model, interpretability and resistance to the adversarial manipulation. There can be false positives and poorly designed systems fail when attackers change the characteristics of malware (Gaber et al., 2024).

By automating the process of feature extraction and pattern recognition, AI-driven malware analysis can enhance reverse engineering, behavioural classification, and threat intelligence. These applications enhance defensive ability, but can also be leveraged by an attacker to test and evolve malicious code (Tyagi & Addula, 2024). A multi-layered approach to security, ongoing surveillance, adversarial testing, quick patching, and human oversight in cyber operations (Schram, 2021) are necessary for effective remediation. The figure 2 indicates that the main phases of the occurrence of AI-related malwares and ransomwares.

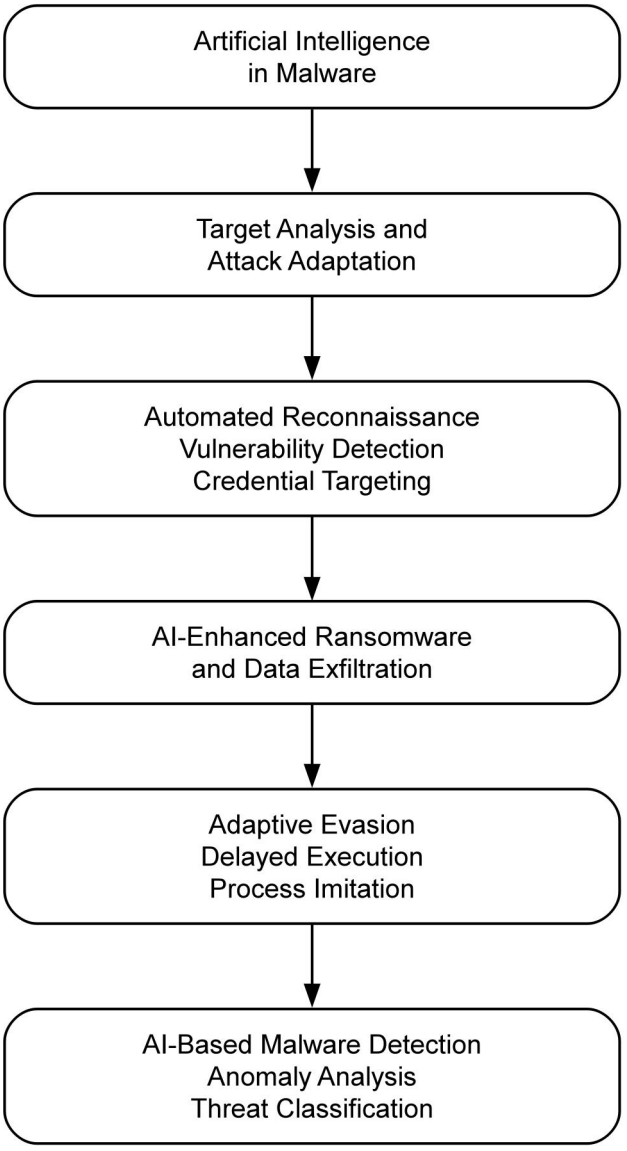

Figure 2. Artificial Intelligence-Enhanced Malware, Ransomware, and Network Intrusions

6. AI-Driven Privacy Violations and Data Exploitation

AI has created vast opportunities for scale and sophistication in privacy violations as it allows for the rapid collection, analysis, linkage, and inference from personal data. Biometric surveillance systems based on 'snapshots' of the face, fingerprints, iris patterns, voice and behaviour can assist in the identification of a crime and in the protection of the public. While they can help law enforcement find suspects and investigate violent crime, they can also lead to wrongful suspicion or intervention of innocent people if the matches are inaccurate, the number of people being monitored is disproportionate, or law enforcement is poorly supervised (Haley, 2025).

Another danger of AI-powered biometric systems is that biometric data is permanent and hard to replace when stolen. During data collection, storage, transmission, matching, and third-party processing, vulnerabilities can occur. Identity theft, surveillance, and discriminatory profiling may be made easier through spoofing, template theft, adversarial attacks, and unauthorized access to the database. To achieve effective safeguards, it is necessary to encrypt, securely store, implement access controls, detect liveness, minimize data, and regularly assess security (Choudhry et al., 2024).

Biometric information is not uniformly protected under laws. There are still concerns about informed consent, the lawful purpose for the collection, retention period, secondary use, cross-border transfer, and commercial exchange of biometric data. The traditional approaches to privacy may be insufficient in situations where identifiers are constantly collected and analyzed by automated systems in public or semi-public spaces (Roberg-Perez, 2016).

Another way of using personal data is by way of re-identification, behavioural prediction, price discrimination, manipulation, exclusion or automated decision-making. Information that's gathered for a good reason can be used in ways that are harmful to individuals and/or groups. These risks show how privacy protection needs to go beyond data breaches to include inferences that are harmful and downstream use (Kröger et al. 2021). There should be strong regulation that is transparent, necessary, proportional, independent, and provides for remedies that are easily accessible. The key routes along which privacy and biometric data can be exploited with the help of AI are shown in Figure 3.

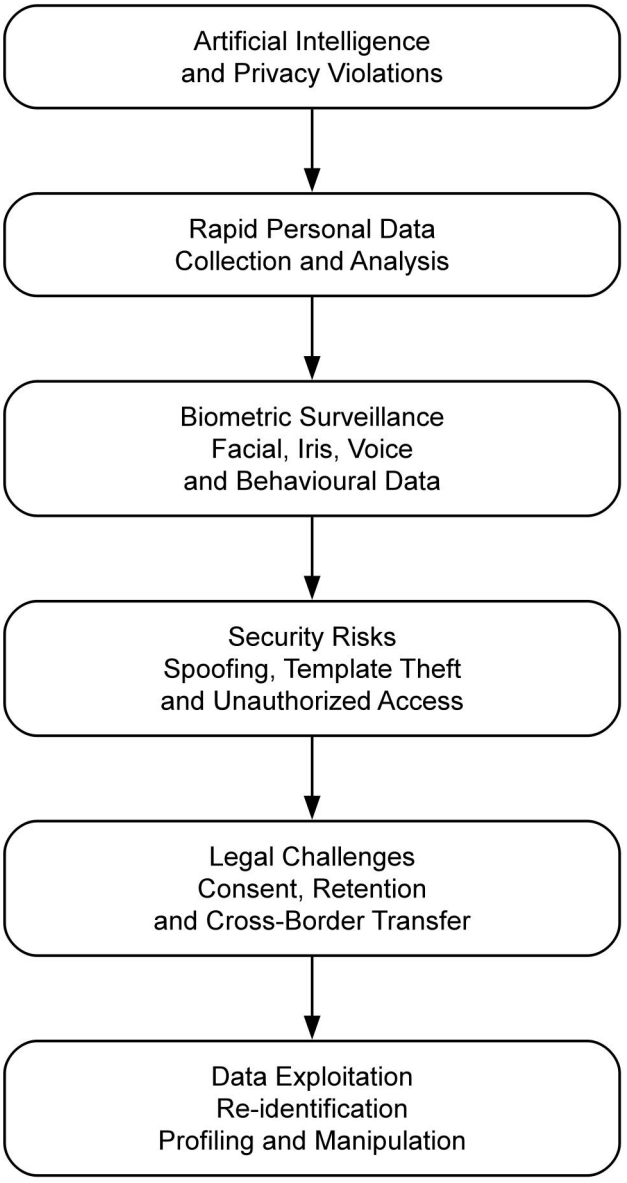

Figure 3. Artificial Intelligence-Driven Privacy Violations and Biometric Data Exploitation

7. Dark Web Markets and AI-Supported Criminal Ecosystems

The dark web is a hidden place where bad guys are able to conduct illegal business, sell stolen information, distribute viruses and other malware, and offer illegal services. AI can enhance such ecosystems with automation, pinpointing vulnerable targets, facilitating fraudulent communication, and boosting operational privacy. Cryptocurrency plays a crucial role in many transactions, such as cross-border transfers and pseudonymous payments, which can be done swiftly, and criminal proceeds can be moved via complex laundering techniques (Navani & Cirella, 2024).

The weaponization of darknets has enabled the proliferation of cybercrime-as-a-service, enabling individuals with less technical expertise to buy phishing kits, ransomware, stolen credentials, botnets, and data-exfiltration tools. AI technologies can help these services become more efficient by creating content for attacks, analyzing victim behavior, and modifying malicious tools to evade detection. The decentralized and encrypted nature of darknet activity makes surveillance, attribution, and prosecution (Adel & Norouzifard, 2024) difficult.

AI and cloud solutions can also help investigators in darknet investigations, such as sifting through vast amounts of data, uncovering concealed connections, tracking marketplace activity, and finding patterns in usernames, transactions, and communication systems. While these capabilities could enhance threat intelligence, there are concerns about their accuracy, privacy, and evidentiary reliability (Goud & Sharma, 2025).

The use of machine learning in cryptocurrency forensics has become a pivotal component in the detection of clusters of suspicious transactions, paths of laundering, and connections between wallet addresses and various types of illegal markets. These tools can aid in enforcement and asset tracing, albeit privacy-enhancing technology, mixers, chain-hopping, and decentralized exchanges pose significant threats (El-Kady, 2025). Good control needs to be coordinated, exchange oversight needs to be improved, there should be specific forensic capacity, international cooperation, and proportional monitoring safeguards for lawful and accountable investigative practice. Figure 4 indicates the structure of dark web criminal ecosystems with the support of AI.

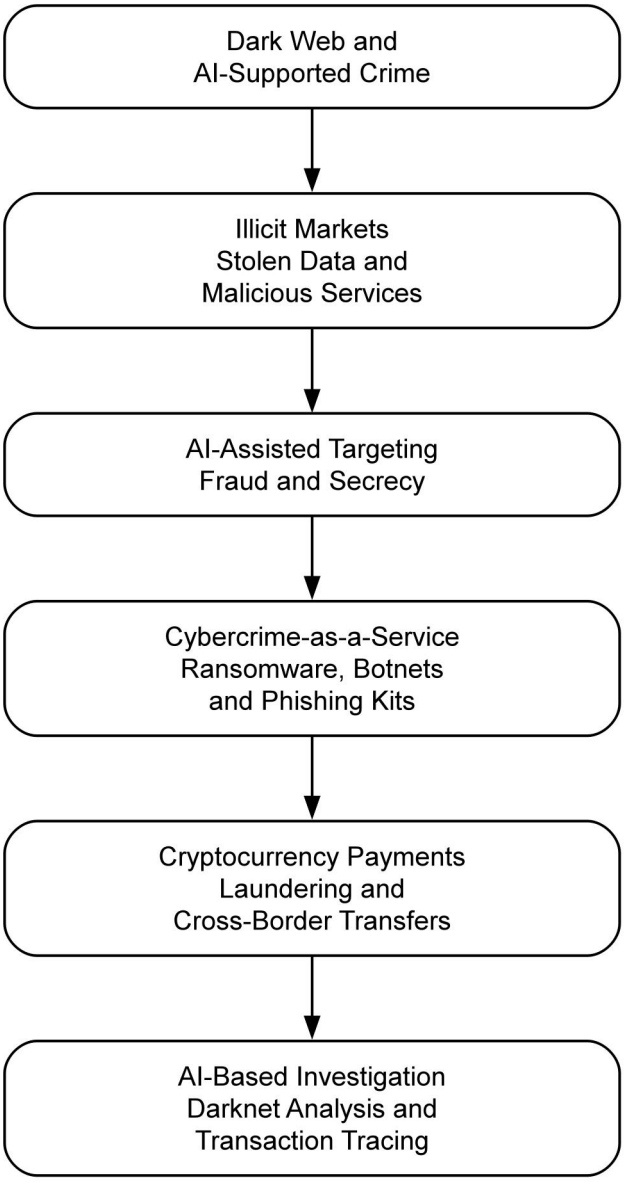

Figure 4. Dark Web Markets and Artificial Intelligence-Supported Criminal Ecosystems

8. Legal Classification, Liability, and Attribution

Criminal liability is problematic as it is more difficult to prove that a criminal act was committed by artificial intelligence, as most legal systems require a human being with intention, knowledge, recklessness, or negligence in order to prove criminal liability. If the AI system causes harm, who is responsible will be subject to court determination—either the developer, deployer, operator, owner, platform, or some other entity. It is hard to establish mens rea with AI systems as their consciousness and moral agency are absent (Dremliuga & Prisekina, 2020).

The liability is based on human control, foreseeability, design, training information, supervision, and opportunity for misuse. Developers could be held responsible when their architecture, inadequate testing, or disregarded risks lead to harm, and users could be held accountable when they intentionally use AI to perpetrate fraud, harassment, intrusion, or other violations. The failure of good governance or inadequate compliance can also lead to corporate liability for foreseeable misconduct (Lagioia & Sartor, 2020).

The issue of civil liability involves questions of negligence, product defect, vicarious liability, cause in action, and damages. The complex supply chains can make it challenging for victims to determine who is accountable if harmful outputs are caused by interactions between models, datasets, platforms, and user prompts. To avoid spreading responsibility among multiple actors, there is a need for clear statutory duties and evidential rules (Dharm et al., 2024).

The idea of giving advanced AI systems legal personhood is still a subject of debate. This recognition may provide avenues for rights and obligations, but may also help to protect both human and corporate actors from accountability. The focus of regulation should be on the human actors who are responsible for the actions of AI, the need for oversight, the risks attached to the duty, and the remedies, not on AI as a legal entity (Lovell, 2023).

9. Digital Evidence and Law-Enforcement Challenges

AI has become a valuable tool for the digital forensics community to analyze, categorize, and decipher massive amounts of electronic evidence. These AI-driven tools can aid in log analysis, malware analysis, image identification, network

reconstruction, and uncovering covert relationships between devices and communication logs. Such abilities can speed up a country's security and cybercrime investigations, especially in complex data environments where in-depth manual analysis is time-consuming. These are capabilities that can help speed up national security and cybercrime investigations, especially in the case of complicated data where conventional manual analysis is too time-consuming.

Large language models (LLMs) also have important reliability issues with regard to their use in forensic analysis. Interpretations produced by AI can be incorrect or include speculations or fabrications, so it is important to always independently verify them. The investigators should keep the original data, record the analytical procedures, confirm the results using available forensic tools, and make sure that the results can be reproduced. AI-generated evidence should not be believed if the AI system gives it a high level of confidence, without any investigation (Khatiwala et al., 2025).

The authentication of electronic evidence can be enhanced by cryptographic verification, timestamping, smart contracts, and automated audit trails. Such mechanisms can provide evidence of integrity and provenance and the chain of custody but require clear processes, standards, and recognition by the judiciary to be credible. AI-powered authentication should be reviewed by humans and have appropriate procedures for protection (Han, 2025).

However, there is a global cyber enforcement deficit due to the fact that there are different levels of technical capacity across the globe, different laws, fewer cyber experts, and more delays in obtaining evidence across different nations. These weaknesses may make it difficult to investigate even if pertinent information is available. Requiring their resolution will be a matter of harmonized procedures, interoperable forensic standards, consistent institutional investment, fast cooperation mechanisms and capacity building of jurisdictions with fewer forensic resources (Peters & Jordan, 2019). Table 3 provides some of the issues which are likely to influence the legal and investigatory aspects.

Table 3. Legal and Investigative Challenges Associated With AI-Enabled Cybercrime

Challenge	Core Legal Issue	Practical Implication	Required Response	Reference
Criminal attribution	Difficulty identifying the responsible human actor	Uncertainty regarding developer, deployer, operator, or user liability	Traceability requirements and documented human oversight	(Dremliuga & Prisekina, 2020)
Distributed liability	Harm may result from multiple actors and technical systems	Victims may struggle to identify an accountable party	Clear statutory duties across the AI lifecycle	(Dharm et al., 2024)
Mens rea assessment	AI systems lack consciousness and conventional criminal intent	Traditional culpability standards may be difficult to apply	Focus on human intention, foreseeability, and negligence	(Lagioia & Sartor, 2020)
Evidence authenticity	AI-generated or manipulated material may appear genuine	Courts may question reliability and admissibility	Provenance verification and forensic authentication	(Han, 2025)
AI-assisted forensic error	Large language models may produce unsupported conclusions	Risk of inaccurate investigative or judicial findings	Independent validation and reproducible forensic procedures	(Khatiwala et al., 2025)
Cross-border evidence access	Data may be stored in foreign jurisdictions	Delays in preservation, disclosure, and prosecution	Mutual legal assistance and rapid data-preservation mechanisms	(Perloff-Giles, 2018)
Extraterritorial jurisdiction	Multiple states may claim authority over the same offence	Sovereignty conflicts and duplicate proceedings	Clear jurisdictional connections and proportionality	(Arnell & Faturoti, 2023)

10. Jurisdiction, Cross-Border Enforcement, and International Cooperation

Cybercrime that is enabled by AI is often transnational, as the perpetrators, victims, servers, platforms, digital assets, and evidence can be in other jurisdictions. This geographic dispersion makes it difficult to identify the law applicable, investigative jurisdiction and/or prosecuting capabilities. Conflicting legal standards and procedures can also prevent the timely availability of data or allow bad actors to take advantage of jurisdictions which may have weaker capabilities in cybercrime (Perloff-Giles, 2018).

Issues of jurisdiction, privacy, and digital evidence are related. Foreign service providers may hold information that

investigators would like to access, but domestic warrants may not have any effect beyond the country. Variability in the rules for evidence collection, retention of evidence, admissibility, and disclosure can hinder timely collection of evidence. These barriers are particularly acute when digital documents can easily be distorted, removed, or moved quickly (Atrey, 2023).

Responses to questions regarding transnational or extraterritorial jurisdiction can seem like a force for increased enforcement, but can also lead to conflicts of jurisdiction, multiple prosecutions, and diminished procedural fairness. An overly broad jurisdiction can also make the defendants vulnerable to the possibility of being subject to different laws and more than one liability for the same acts. This should therefore inform decisions on prosecution, whereby the connecting factors, proportionality, and respect for territorial authority should be taken into consideration (Arnell & Faturoti, 2023).

International organizations have enhanced the legal definitions, investigative cooperation, capacity building, and procedural standards in the cybercrime and AI realm. There are instruments in place to assist each other in legal matters, as well as in extradition, evidence sharing, and coordinated enforcement, but the implementation of these is inconsistent (Velasco, 2022). To achieve effective cooperation, the data-preservation mechanism should be faster, the legislation for data-preservation should be compatible, contact persons should be identified, judicial protection should be provided, and technical assistance should be made available on an ongoing basis from one jurisdiction to another. Avoid infringing human rights; transparency, accountability, and due process should be maintained.

11. Regulatory Responses and Future Governance Priorities

There is a need for artificial intelligence regulation to reflect the changing dynamics between technological innovation, combating cybercrime, accountability and fundamental rights. Traditional legal systems are not designed to react quickly to systems that learn, adapt and produce outputs in several jurisdictions. Flexible and technology-independent rules are essential to effective governance that can deal with harmful uses without hampering legitimate research, commercial development and applications in the public interest. What regulatory design should look at is the risk, transparency, traceability, human oversight, and who is responsible and how through the lifecycle of AI (Hoffmann-Riem, 2019).

The installation of malicious apps, their modification and distribution, and deployment at scale present further difficulties with AI-powered cybercrime. Abolishing inappropriate conduct should be made clear in future legal measures; duties should be reinforced for high-risk developers and service providers, incident reporting, auditability, and cooperation should be mandated with lawful investigations. Cybercrime legislation should also be harmonized with the law on data protection, consumer protection, platform governance and cyber security, and minimize the number of regulatory rules. The cross-border aspect of offences relates to infrastructure, digital assets and cloud-based services, which requires international harmonization (Volodymyr et al., 2025).

Development of regulations must always have a human rights focus. Automated systems, biometric surveillance, predictive policing, and/or the use of algorithms for content control can be used to improve security but can also cause problems with privacy, equality, expression, and due process. To ensure that rights-respecting governance, it is necessary and proportionate to have independent oversight, must have remedies that are accessible, and must have measures to prevent discriminatory outcomes (Ahmad et al., 2025).

The priorities for the future are to implement a mandatory framework of risk assessment, a development framework of secure-by-design, a provenance standard for synthetic media, to strengthen platform accountability, to provide specialist training for law enforcement, to provide victim support and to establish international evidence sharing procedures. The policy on adaptive regulation should be monitored to ensure that it is effective and remains in line with the ongoing development of AI capabilities and criminal techniques. Table 4 indicates some of the key regulatory and governance concerns.

Table 4. Regulatory Priorities for Addressing AI-Enabled Cybercrime

Regulatory Priority	Proposed Measure	Intended Outcome	Key Implementation Concern	Reference
Risk-based AI governance	Classify systems according to their potential for misuse and societal harm.	Proportionate regulatory obligations	Avoiding excessive restrictions on legitimate innovation	(Hoffmann-Riem, 2019)
Secure-by-design development	Require testing, access controls, misuse monitoring, and vulnerability management.	Reduced criminal exploitation of AI systems	Compliance costs and technical standardization	(Volodymyr et al., 2025)
Synthetic media provenance	Introduce watermarking, content credentials, and traceable origin records	Improved detection and authentication of manipulated media	Interoperability and resistance to removal or alteration	(Darma et al., 2025)
Platform accountability	Require reporting, moderation, rapid takedown, and cooperation with	Faster restriction of harmful AI-generated	Balancing platform duties with freedom of	(Ahmad et al., 2025)

	investigations.	content	expression	
Digital evidence standards	Establish validated procedures for AI-assisted collection and analysis	Greater evidentiary reliability and judicial acceptance	Need for specialist expertise and independent auditing	(Njuguna, 2024)
International legal harmonization	Align cybercrime definitions, evidence procedures, and cooperation mechanisms.	Improved cross-border enforcement	Differences in sovereignty, privacy law, and institutional capacity	(Velasco, 2022)
Human rights safeguards	Require necessity, proportionality, transparency, oversight, and remedies	Protection of privacy, equality, expression, and due process	Preventing discriminatory or excessive surveillance	(Ahmad et al., 2025)

2. Limitations and Future Directions

The fast-paced advances of artificial intelligence and cybercrime pose a limitation to this review, as technical and legal points outlined might become obsolete in the future with the advent of new models, attack techniques, and regulations. The literature that is available is also diverse in terms of terminology, methodology, area of jurisdiction, and quality of evidence. Some sources are conceptual, conference, or non-empirical, which makes the comparison and generalizability of the source limited. The prevalence and the impact of cybercrime and the effectiveness of law enforcement are also hampered by underreporting of cybercrime, limited access to law-enforcement data and varying legal definitions of cybercrime.

The focus of future studies should be on empirical, cross-jurisdictional research on offender behaviour and its impact on victims, the performance of the investigation and the efficacy of legal interventions. The need for standardized reporting and definition of terms for better comparability between studies and jurisdictions. Risk-based governance and platform accountability, digital evidence standards and international cooperation mechanisms should be included in regulatory research. It is also important to put more focus on vulnerable groups, human rights protection measures, forensic validation using AI, and the ongoing review of the law based on technological capacities.

13. Conclusion

Cybercrime has evolved into a faster, larger, more personalized, and adaptive activity with the help of artificial intelligence. AI-powered phishing attacks, deepfakes, automated fraud, adaptive malware, biometric misuse, services on the dark web, and cryptocurrency-based laundering pose threats to cybersecurity that go beyond standard cybersecurity controls. The current legal frameworks can be weaker due to overlapping definitions, unclear obligations, unclear liability, lack of digital evidence, a lack of capacity to enforce, and jurisdiction issues. Good governance needs coordination of the use of criminal legislation, legislation on data protection, regulation of cybersecurity, platforms' accountability, and human rights safeguards. Everyone, from developers to deployers, users, service providers and organizations, should have proportionate duties according to the level of control, foreseeability and risk. Law-enforcement agencies need to be trained, to have validated forensic tools, to have quick procedures for evidence preservation and to have enhanced cooperation with international law enforcement. Regulatory actions should be technology-agnostic and flexible to new advancements in AI, and uphold privacy, equality, freedom of expression, and due process. Future frameworks should focus on secure-by-design development, transparency and traceability, synthetic-media provenance, independent oversight, and regular legal checks and balances. A prevention, adaptive and internationally coordinated response is needed to minimise the effects of cybercrime by AI while not stifling legitimate innovation or fundamental rights.

References

1. Adel, A., & Norouzifard, M. (2024). Weaponization of the growing cybercrimes inside the dark net: The question of detection and application. Big Data and Cognitive Computing, 8(8), 91.
2. Ahmad, R., Saleem, S., & Hussain, S. (2025). Ethical and Legal Challenges of Artificial Intelligence: Implications for Human Right. Journal of Law, Society and Policy Review, 2(01), 10-25.
3. Ali, M. J. (2024). Cybercrime and cybersecurity: A critical analysis of legal frameworks and enforcement mechanisms. BHARATI INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH AND DEVELOPMENT Учредители: Gungun Publishing House, 2(8), 137-154.
4. Amoo, O. O., Atadoga, A., Abrahams, T. O., Farayola, O. A., Osasona, F., & Ayinla, B. S. (2024). The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. World Journal of Advanced Research and Reviews, 21(2), 205-217.
5. Andraško, J., Mesarčík, M., & Hamuľák, O. (2021). The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework. AI & society, 36(2), 623-636.
6. Arnell, P., & Faturoti, B. (2023). The prosecution of cybercrime–why transnational and extraterritorial jurisdiction should be resisted. International Review of Law, Computers & Technology, 37(1), 29-51.
7. Atrey, I. (2023). Cybercrime and its Legal Implications: Analysing the challenges and Legal frameworks

surrounding Cybercrime, including issues related to Jurisdiction, Privacy, and Digital Evidence. International Journal of Research and Analytical Reviews, 10(3).
8. Blauth, T. F., Gstrein, O. J., & Zwitter, A. (2022). Artificial intelligence crime: An overview of malicious use and abuse of AI. Ieee Access, 10, 77110-77122.
9. Busacca, A., & Monaca, M. A. (2023). Deepfake: Creation, purpose, risks. In Innovations and economic and social changes due to artificial intelligence: the state of the art (pp. 55-68). Cham: Springer Nature Switzerland.
10. Cassidy, A. A. T. J., Fuad, A., & Shofy, M. U. A. A. (2024). Emerging trends and challenges in digital crime: A study of cyber criminal tactics and countermeasures. TechComp Innovations: Journal of Computer Science and Technology, 1(1), 38-45.
11. Çela, E. Analysis of the Impact of Digital Transformation of the Legal Field on Data Cybersecurity.
12. Choudhry, M. D., Sundarrajan, M., Jeevanandham, S., & Saravanan, V. (2024). Security and privacy issues in AI-based biometric systems. In AI Based Advancements in Biometrics and its Applications (pp. 85-100). CRC Press.
13. Darma, M., Gisymar, N. A., Purwadi, A., Zubaedah, P. A., & Judijanto, L. (2025). Legal Implications of Deepfake Technology Misuse in Digital Content on Social Media. Science of Law, 3, 98-103.
14. Dharm, J., Girme, A., & Gharde, U. (2024). Artificial intelligence: Challenges in criminal and civil liability. International Journal of Law, 10(2), 52-57.
15. Dremliuga, R., & Prisekina, N. (2020). The concept of culpability in criminal law and AI systems. J. Pol. & L., 13, 256.
16. El-Kady, R. (2025). Unveiling the Illegal Uses of Cryptocurrencies in Dark Web and Advanced AI and Machine Learning Techniques in Cryptocurrency Forensics. In Concept, Theories, and Management of Cryptocurrencies (pp. 363-394). IGI Global Scientific Publishing.
17. Ezeji, C. L. (2024). Cyber policy for monitoring and regulating cyberspace and cyber security measures for combating technologically enhanced crime in South Africa. International Journal of Business Ecosystem & Strategy (2687-2293), 6(5), 96-109.
18. Falade, P. V. (2023). Decoding the threat landscape: ChatGPT, FraudGPT, and WormGPT in social engineering attacks. arXiv preprint arXiv:2310.05595.
19. Fekolli, S., Çela, E., Erdolatov, C., Biyashev, B., & Ismailova, G. (2025). Analysis of the Impact of Digital Transformation of the Legal Field on Data Cybersecurity. Law, State & Telecommunications Review/Revista de Direito, Estado e Telecomunicações, 17(2).
20. Folorunsho, F., & Boamah, B. F. (2025). Deepfake technology and its impact: ethical considerations, societal disruptions, and security threats in ai-generated media. International journal of information technology and management information systems, 16(1), 1060-1080.
21. Gaber, M. G., Ahmed, M., & Janicke, H. (2024). Malware detection with artificial intelligence: A systematic literature review. ACM Computing Surveys, 56(6), 1-33.
22. George, A. S., & George, A. H. (2023). Deepfakes: the evolution of hyper realistic media manipulation. Partners Universal Innovative Research Publication, 1(2), 58-74.
23. Goud, V. C., & Sharma, A. K. (2025). Analyzing DarkWeb Using AI and Cloud. In Establishing AI-Specific Cloud Computing Infrastructure (pp. 259-268). IGI Global Scientific Publishing.
24. Haley, P. (2025). The impact of biometric surveillance on reducing violent crime: Strategies for apprehending criminals while protecting the innocent. Sensors, 25(10), 3160.
25. Han, P. (2025). AI-powered digital arbitration framework leveraging smart contracts and electronic evidence authentication. Scientific Reports, 15(1), 37327.
26. Hayward, K. J., & Maas, M. M. (2021). Artificial intelligence and crime: A primer for criminologists. Crime, Media, Culture, 17(2), 209-233.
27. Hoffmann-Riem, W. (2019). Artificial intelligence as a challenge for law and regulation. In Regulating artificial intelligence (pp. 1-29). Cham: Springer International Publishing.
28. Jeong, D. (2020). Artificial intelligence security threat, crime, and forensics: Taxonomy and open issues. IEEE Access, 8, 184560-184574.
29. Khatiwala, J. P., Addai, D. K. N., & Xu, W. (2025, July). Evaluating the Reliability of Digital Forensic Evidence Discovered by Large Language Model: A Case Study. In 2025 IEEE 49th Annual Computers, Software, and Applications Conference (COMPSAC) (pp. 1067-1076). IEEE.
30. Kröger, J. L., Miceli, M., & Müller, F. (2021). How data can be used against people: A classification of personal data misuses. Available at SSRN 3887097.
31. Lagioia, F., & Sartor, G. (2020). Ai systems under criminal law: a legal analysis and a regulatory perspective. Philosophy & Technology, 33(3), 433-465.
32. Lovell, J. J. (2023). Legal Aspects of Artificial Intelligence Personhood: Exploring the Possibility of Granting Legal Personhood to Advanced Ai Systems and the Implications for Liability, Rights and Responsibilities. Rights and Responsibilities.(May 10, 2023).
33. Mushtaq, S., & Shah, M. (2025). Threats to the digital ecosystem: Can information security management frameworks, guided by criminological literature, effectively prevent cybercrime and protect public data?. Computers, 14(6), 219.
34. Navani, S., & Cirella, G. T. (2024). Cybercrimes in the cryptocurrency domain: Identifying types, understanding motives and techniques, and exploring future directions for technology and regulation. Journal of Geography, Politics and Society, 14(2), 1-22.
35. Njuguna, L. W. (2024). AI-Assisted Digital Forensics for National Security Investigations. International Journal

of Technology, Management and Humanities, 10(01), 125-146.
36. Oluoha, O. M., Odeshina, A., Reis, O., Okpeke, F., Attipoe, V., & Orieno, O. H. (2022). Artificial intelligence integration in regulatory compliance: A strategic model for cybersecurity enhancement. Journal of Frontiers in Multidisciplinary Research, 3(1), 35-46.
37. Perloff-Giles, A. (2018). Transnational cyber offenses: Overcoming jurisdictional challenges. Yale J. Int'l L., 43, 191.
38. Peters, A., & Jordan, A. (2019). Countering the cyber enforcement gap: Strengthening global capacity on cybercrime. J. Nat'l Sec. L. & Pol'y, 10, 487.
39. Raja, J., Le, J., & Nguyen, C. (2025). Phishing attacks in the age of generative artificial intelligence: A systematic review of human factors. AI, 6(8), 174.
40. Roberg-Perez, S. (2016). The future is now: Biometric information and data privacy. Antitrust, 31, 60.
41. Saba'F, T., Alnawafleh, N. M., Alodainat, N. S., & Al-Dmour, N. A. (2025, May). AI in Cybersecurity: a Taxonomy of Security Threats, Crime Dynamics. In 2025 3rd International Conference on Business Analytics for Technology and Security (ICBATS) (pp. 1-6). IEEE.
42. Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. Sensors, 23(15), 6666.
43. Schmitt, M., & Flechais, I. (2024). Digital deception: Generative artificial intelligence in social engineering and phishing. Artificial Intelligence Review, 57(12), 324.
44. Schram, G. (2021). The Role of Artificial Intelligence in Cyber Operations: An Analysis of AI and Its Application to Malware-Based Cyberattacks and Proactive Cybersecurity (Master's thesis, Utica College).
45. Thanh, C. T., & Zelinka, I. (2019). A survey on artificial intelligence in malware as next-generation threats. In Mendel (Vol. 25, No. 2, pp. 27-34).
46. Tyagi, A. K., & Addula, S. R. (2024). Artificial intelligence for malware analysis: A systematic study. Artificial Intelligence-Enabled Digital Twin for Smart Manufacturing, 359-390.
47. Velasco, C. (2022, May). Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments. In ERA Forum (Vol. 23, No. 1, pp. 109-126). Berlin/Heidelberg: Springer Berlin Heidelberg.
48. Volodymyr, Z., Valery, B., Borys, K., Volodymyr, S., Oleksiy, O., & Yehor, P. T. (2025). Artificial intelligence and cybercrime: New challenges and prospects for legal regulation. Contemporary Issues in Artificial Intelligence, 1.
49. Yu, J., Yu, Y., Wang, X., Lin, Y., Yang, M., Qiao, Y., & Wang, F. Y. (2024). The shadow of fraud: The emerging danger of ai-powered social engineering and its possible cure. arXiv preprint arXiv:2407.15912.