

The Indonesian National Police's Strategy in Combating Artificial Intelligence-Based Digital Content Manipulation as a Means of Political Crime and Cyber Fraud in Indonesia

Adrian Batubara *, Vita Mayastinasari, Kif Aminanto

Sekolah Tinggi Ilmu Kepolisian, South Jakarta, Indonesia ; adrian.batubara.ab@gmail.com

Sekolah Tinggi Ilmu Kepolisian, South Jakarta, Indonesia ; mamayovi@gmail.com

Sekolah Tinggi Ilmu Kepolisian, South Jakarta, Indonesia ; kif.92pw@gmail.com

DOI:

<https://doi.org/10.47134/jcl.v3i3.2.6329>

*Correspondence: Adrian Batubara

Email: adrian.batubara.ab@gmail.com

Received: 08/08/2026

Accepted: 27/08/2026

Published: 31/08/2026



Copyright: © 2026 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution-ShareAlike (CC BY-SA) license (<http://creativecommons.org/licenses/by-sa/4.0/>).

cybersecurity system, and developing smart policing and cyber resilience to create an adaptive, responsive, and sustainable cyber law enforcement system in the era of digital transformation.

Abstract: *The development of Artificial Intelligence has given rise to new forms of cybercrime through deepfake-based digital content manipulation, voice cloning, synthetic media, and AI-generated content, which are used as a means of political crime and cyber fraud in Indonesia. This study aims to analyze problems in law enforcement, weaknesses in the Indonesian National Police's strategy, and legal reforms in addressing artificial intelligence (AI)-based digital content manipulation through strengthening smart policing and cyber resilience. This study employs a normative juridical method with a legislative and conceptual approach, through the analysis of various regulations, legal theories, and doctrines related to cybercrime, artificial intelligence, and national cybersecurity. The results reveal that law enforcement against AI-based digital content manipulation still faces several weaknesses, including the absence of specific legal norms related to AI crimes and political deepfakes, limited capacity in cyber policing and digital forensics, weak coordination between institutions, and low public digital literacy. The Indonesian National Police's strategy is still reactive and has not been optimal in implementing artificial intelligence-based predictive policing. Therefore, legal reform is needed through the establishment of specific regulations for Artificial Intelligence Crime, strengthening AI forensic and cyber intelligence units, developing an integrated*

Keywords: *Artificial Intelligence, Digital Content Manipulation, Deepfake, Smart Policing.*

Introduction

The development of Artificial Intelligence technology has brought about a major transformation in the digital social life of modern society, especially through the emergence of generative AI capable of automatically creating text, sound, images, and video with a level of precision that resembles real reality. Technologies such as deepfakes, voice cloning, synthetic media, and AI-generated images and videos have changed digital communication patterns while creating new forms of cyber threats that are increasingly complex and difficult to detect (Ramadhina, 2023). From the perspective of Ulrich Beck's risk society theory, technological modernization gives rise to new risks that are global, abstract, and difficult to control with conventional legal instruments. (Beck, 1992) The development of AI

not only provides economic benefits and social efficiency, but also opens up space for the misuse of technology for criminal interests, political propaganda, and the manipulation of public information. This phenomenon shows the transformation of conventional crime into cyber-enabled crime that utilizes the sophistication of digital technology as the main tool for conducting crimes. (Apriliana, 2024) From the perspective of Technological Determinism theory, technological developments directly influence social structures and human behavior, so that changes in AI technology also contribute to changes in crime patterns in digital society. This situation is further exacerbated by the digitalization of the political and economic sectors, which has made the digital public sphere highly vulnerable to the spread of disinformation, opinion manipulation, and artificial intelligence-based fraud. Normatively, Indonesia already has a legal basis for electronic information through Law Number 1 of 2024, which amends Law Number 11 of 2008. However, this regulation does not specifically address the misuse of artificial intelligence and the manipulation of digital content based on synthetic media, creating a legal vacuum in addressing the escalation of AI crimes in the digital era. (Kurniarullah, 2024)

Artificial intelligence-based digital content manipulation is essentially a form of modern cybercrime committed through audio, visual, and audiovisual manipulation to create false information that appears authentic in order to influence public perception or obtain certain unlawful benefits. Deepfake and AI manipulation technology are characterized by the ability to realistically replicate a person's face, voice, expressions, and even communication patterns, making them difficult to distinguish from the original content (Erdiyanti, 2026). In practice, digital content manipulation has been used in various criminal *modus operandi* such as investment fraud, impersonation of state officials, engineering political speeches, spreading election hoaxes, digital blackmail, and social engineering to obtain victims' personal data. Unlike conventional digital manipulation, which can still be detected through manual editing, AI-generated manipulation is able to produce fake content automatically, quickly, massively, and very convincingly, thereby increasing the level of public victimization. (Adella, 2026) Internationally, the misuse of deepfakes has occurred in elections in several countries through fake videos of political figures, while in Indonesia, the phenomenon of the spread of manipulative videos, political hoaxes, and voice cloning-based fraud has begun to show a significant increase, along with the development of digital platforms. It not only impacts economic losses for the community but also political disinformation, a crisis of public trust in state institutions, and disruptions to national security. (Librianti, 2025) In national criminal law, the provisions of Article 28 paragraphs (1) and (2) of Law Number 1 of 2024 actually regulate the prohibition of the dissemination of fake news and information that incites hatred. However, this norm is still general and does not specifically regulate the use of artificial intelligence as an instrument of digital manipulation, thus creating weaknesses in the construction of criminal liability for perpetrators of deepfake and synthetic media crime.

The misuse of artificial intelligence-based digital content manipulation has also developed into a means of political crime that threatens the integrity of democracy in Indonesia. The era of electronic democracy has made digital media a primary arena for shaping public opinion and political contestation, so deepfake technology has the potential to be used as a tool for propaganda, black campaigns, character assassination, and

manipulation of public perception of certain political figures. (Ahda, 2026) From the perspective of digital democracy theory, cyberspace has a significant influence on the legitimacy of power and public political participation. Therefore, the misuse of AI in political contestation can undermine the quality of substantive democracy. Furthermore, power and media theory explain that control over digital information can be used as an instrument of political domination and the formation of hegemonic public opinion. The phenomenon of the spread of AI-based manipulative content has the potential to delegitimize election results, social polarization, horizontal conflict, and even threats to national stability due to systematic and massive disinformation. Even from the perspective of national security theory, digital information manipulation can be categorized as a non-military threat that may undermine national sovereignty through foreign cyber interference and transnational digital influence operations. (Nurwahid, 2026) The fundamental problem in Indonesia is the lack of specific regulations regarding political deepfakes or synthetic political propaganda, making it difficult for law enforcement officials to determine normative boundaries and legal accountability for perpetrators of AI-based political content manipulation. This regulatory vacuum demonstrates that the national legal system has not been able to optimally adapt to the rapid development of digital technology, even though Article 28F of the 1945 Constitution of the Republic of Indonesia guarantees the public's right to obtain true and accurate information as part of citizens' constitutional rights.

In addition to its use for political gain, AI-based digital content manipulation has also become a key instrument of increasingly complex and organized modern cyberfraud. The development of AI-based digital fraud has seen the emergence of various new crime methods, such as voice cloning scams, romance scams, AI-based phishing, fake identities, and fake customer service, which utilize sophisticated technology to psychologically deceive victims. Criminals can imitate the voices of family members, officials, and banks to gain financial access to victims through engineered digital communications that appear authentic. (Anthony, 2023) From a cybercriminology perspective, the development of digital technology creates new space for criminals to carry out social and economic exploitation through virtual mechanisms that are difficult to trace conventionally. The accumulation of public victimization is influenced by low digital literacy and the public's limited ability to distinguish between original and AI-generated content. This condition has serious impacts on the stability of the digital economy, public trust in electronic transactions, and the security of people's personal data. Normatively, personal data protection is regulated in Law Number 27 of 2022, while aspects of electronic fraud are regulated in Article 378 of the Criminal Code and Article 28 paragraph (1) of the ITE Law. However, these regulations do not comprehensively address the construction of AI-based crimes that use synthetic media and voice cloning as the primary means of criminal activity. (Tarigan, 2025) As a result, law enforcement officials still face difficulties in gathering digital evidence, identifying transnational perpetrators, and determining criminal liability in AI-generated fraud crimes.

The problems of law enforcement against Artificial Intelligence-based digital content manipulation in Indonesia essentially reflect the weaknesses of the national legal system in addressing the development of modern cybercrime. From the perspective of Lawrence M. Friedman's legal system theory, the effectiveness of law enforcement is influenced by the interconnected substance of the law, legal structure, and legal culture. From a legal

substance perspective, Indonesia does not yet have specific regulations governing AI crime, synthetic media crime, or political deepfakes, resulting in a normative vacuum regarding the definition, classification of criminal acts, and legal accountability mechanisms for perpetrators of AI-based digital content manipulation. The provisions in the ITE Law, the Criminal Code, and the Privacy and Security Law are still partial and unable to address the complexities of rapidly evolving artificial intelligence crimes. From a legal structure perspective, cyber police capacity still faces various limitations, such as a lack of AI digital forensics, limited human resources, the complexity of electronic evidence, and cross-border jurisdictional constraints in handling global cybercrime. This situation indicates that the national law enforcement structure is not fully prepared to face the transnational and multidimensional threat of AI-based crimes. From a legal culture perspective, low digital literacy among the public has led to a high rate of spread of hoaxes and information manipulation due to the growing culture of sharing without verification in the digital space. (Novera, 2024) As a result, the public is highly vulnerable to AI-based disinformation and fraud. Constitutionally, the state has an obligation to protect the public from digital threats, as mandated by the Preamble to the 1945 Constitution and Article 30 of the 1945 Constitution concerning the state defense and security system. However, the implementation of this protection remains suboptimal in the context of artificial intelligence-based cybersecurity.

The weaknesses of the Indonesian National Police's strategy in addressing artificial intelligence-based digital content manipulation are also a significant factor contributing to the suboptimal response to modern digital crime in Indonesia. The National Police's law enforcement strategy still tends to be reactive and repressive after a crime occurs, while the development of AI requires a preventative, predictive, and adaptive approach based on digital technology. To date, there is no AI-based cyber predictive policing system, a dedicated AI forensic unit, internal regulations regarding handling deepfakes, or a nationally integrated digital crisis communication mechanism. Furthermore, coordination between institutions such as the Ministry of Communication and Digital of the Republic of Indonesia, the National Cyber and Crypto Agency, the Attorney General's Office, and global digital platforms remains suboptimal in addressing the threat of AI-based content manipulation. In fact, several countries, such as the United States, Singapore, China, and European Union countries, have begun developing artificial intelligence regulations, deepfake detection systems, and cyber-resilience-based smart policing models to address the threat of modern digital crime. Therefore, legal reforms are needed for police strategies through regulatory reconstruction, strengthening cyber police institutions, developing AI governance, increasing digital forensic capacity, and integrating cybersecurity, criminal policy, digital rights, and democratic protection within the national law enforcement system. These legal reforms are crucial for realizing a police system that is adaptive to technological developments, capable of protecting the integrity of digital democracy, and ensuring public safety from the threat of artificial intelligence-based digital content manipulation in the era of digital transformation.

Methodology

This study employs a normative juridical research method that focuses on the study of legal norms, legal principles, legal theories, and regulations related to the Indonesian National Police's strategy in combating Artificial Intelligence-based digital content manipulation as a means of political crime and cyber fraud in Indonesia. The approaches used in this study include a statutory approach and a conceptual approach. The statutory approach is carried out by examining various relevant regulations, including the 1945 Constitution of the Republic of Indonesia, Law Number 1 of 2024, Law Number 27 of 2022, the Criminal Code, as well as various regulations related to cybersecurity, digital law enforcement, and police authority in combating cybercrime. Meanwhile, the conceptual approach is used to analyze various legal doctrines, theories, and concepts related to cybercriminology, artificial intelligence, deepfakes, smart policing, cyber resilience, and legal reforms in the cyber law enforcement system. The legal materials used consist of primary, secondary, and tertiary legal materials obtained through library research. Furthermore, all legal materials are analyzed prescriptively using qualitative analysis methods to find legal arguments, identify gaps in norms, and formulate legal reform concepts for police strategies in addressing the development of Artificial Intelligence-based digital content manipulation crimes in the era of digital transformation.

Result and Discussion

Law Enforcement Issues Regarding Artificial Intelligence-Based Digital Content Manipulation as a Means of Political Crime and Cyber Fraud in Indonesia

The development of artificial intelligence-based digital content manipulation has generated increasingly complex legal and law-enforcement issues due to the emergence of technologies such as deepfakes, voice cloning, synthetic media, and AI-generated content. In this study, the development of these technologies is not presented as an independent empirical finding regarding the statistical prevalence of AI-based crime in Indonesia. Rather, it constitutes the technological and normative context identified in relevant legal and academic discussions concerning the transformation of cybercrime and electronic information manipulation. Digital content manipulation may involve the use of artificial intelligence to generate, alter, synthesize, or simulate images, sounds, videos, or narratives in a manner capable of creating the appearance of authenticity. Such technological capabilities may be misused for political disinformation, impersonation, cyber fraud, extortion, social engineering, and other unlawful purposes. The normative issue examined in this study is therefore whether the existing Indonesian legal framework, particularly the ITE Law, the Criminal Code, personal data protection law, and police regulations, provides sufficiently specific legal categories and procedural mechanisms to address the distinctive characteristics of AI-generated manipulation. In this context, Article 28 paragraphs (1) and (2) and Article 35 of Law Number 1 of 2024 provide a general legal basis concerning false information, harmful electronic information, and electronic manipulation, although these provisions do not expressly regulate artificial intelligence as a specific technological instrument of manipulation (Cantika, 2025).

The main problem in law enforcement against AI-based digital content manipulation lies in the absence of sufficiently precise legal categories capable of distinguishing harmful

AI-enabled conduct from legitimate technological and expressive activity. For the purpose of legal reconstruction, AI-generated content should be understood as content wholly or partially generated, transformed, or substantially modified through artificial intelligence systems. This definition should remain technologically neutral and should not itself imply illegality.

Synthetic-media manipulation should refer to the intentional use of artificial intelligence or comparable computational technology to generate, alter, simulate, or materially modify audio, visual, audiovisual, or textual content in a manner capable of creating a materially false representation of a person, event, statement, or circumstance. Deepfake crimes should not be defined merely by the use of deepfake technology, but by the intentional creation, dissemination, or use of materially deceptive synthetic content for an unlawful purpose, to cause legally relevant harm, to obtain unlawful benefit, to impersonate another person without lawful authorization, or to interfere with legally protected interests.

A political deepfake should constitute a criminal offense only when the AI-generated or materially manipulated content: (a) falsely represents a candidate, public official, political actor, electoral institution, or political event as authentic; (b) is disseminated with knowledge of its deceptive character or with reckless disregard for authenticity; (c) is intended to deceive the public, manipulate electoral decision-making, damage legally protected interests, or unlawfully influence a political process; and (d) creates or is reasonably capable of creating a concrete risk of legally relevant harm. These elements distinguish criminal political deepfakes from protected political criticism, parody, satire, artistic expression, journalism, research, or educational content, particularly where the synthetic or fictional nature of the material is reasonably disclosed or apparent.

Accordingly, the proposed legal framework must regulate harmful conduct rather than criminalize artificial intelligence or AI-generated expression as such. The existing provisions of the ITE Law, the Criminal Code, and Law Number 27 of 2022 concerning Personal Data Protection may remain applicable to particular forms of fraud, impersonation, manipulation, or unlawful personal-data processing, but they do not yet provide a unified legal framework for AI-specific synthetic impersonation and technologically mediated deception (Sabela, 2026).

In addition to legal substance issues, law enforcement challenges also arise from the legal structure, which relates to the capacity of law enforcement officials to address the development of Artificial Intelligence-based digital crimes. Handling deepfakes, voice cloning, and AI-generated manipulation requires highly sophisticated digital forensic skills because the authenticity of electronic evidence is often difficult to verify. In the context of criminal procedural law, electronic evidence is recognized through Article 5 paragraphs (1) and (2) of Law Number 1 of 2024, which states that electronic information and electronic documents, along with their printouts, constitute valid legal evidence. However, in practice, proving AI-based content manipulation requires specialized detection technology and human resources competent in digital forensic artificial intelligence. (Pramesti, 2025) This situation presents a significant challenge for the police due to limited cyberforensic

infrastructure, a shortage of AI forensic experts, and the complexity of tracking perpetrators, who often use foreign servers and anonymous identities. Furthermore, AI-based digital manipulation crimes are generally transnational in nature, requiring international cooperation in the investigation and law enforcement process. Indonesia itself does not yet have a cyber law enforcement system fully integrated with global mechanisms for handling AI-based cybercrime. As a result, the law enforcement process is often slow and ineffective in providing legal protection to the public as victims of modern digital crime.

Artificial Intelligence-based digital content manipulation also poses serious problems in the context of political crimes and threatens digital democracy in Indonesia. The use of deepfakes in political propaganda, black campaigns, and character assassination has the potential to undermine election integrity and democratic legitimacy. In the era of electronic democracy, the digital space has become the primary arena for shaping public opinion, allowing the spread of AI-based false information to massively influence people's political behavior. This phenomenon contradicts the principles of a democratic rule of law as stipulated in Article 1 paragraph (3) of the 1945 Constitution of the Republic of Indonesia, which affirms that Indonesia is a state based on the rule of law, and Article 28F of the 1945 Constitution, which guarantees the public's right to obtain true and accurate information. The spread of political deepfakes not only undermines the public's constitutional right to obtain valid information but also has the potential to create social conflict, political polarization, and national instability. The fundamental problem facing Indonesia is the lack of specific regulations regarding political deepfakes or synthetic political propaganda, making it difficult for law enforcement officials to determine the legal boundaries between freedom of expression and destructive information manipulation. This lack of norms demonstrates that the national legal system has not been able to anticipate the rapid development of threats to digital democracy based on artificial intelligence in the era of information technology transformation (Pratama, 2026).

On the other hand, artificial intelligence-based digital content manipulation has also become a primary tool for cyberfraud, threatening the security of the national digital economy. AI-based fraud methods such as voice cloning scams, fake customer service scams, AI phishing scams, and romance scams have led to increased public victimization through highly convincing digital communications. Criminals can imitate the voices of family members, officials, and even banks to gain financial access to victims through artificial intelligence-based psychological manipulation. In this context, the provisions of Article 30 of Law Number 1 of 2024 concerning illegal access to electronic systems and Article 32 of the Electronic Information and Transactions Law concerning the alteration or transfer of electronic information can actually be used to ensnare perpetrators of digital crime. However, these norms do not specifically regulate the use of AI-generated identities and synthetic impersonations in cyberfraud crimes. This situation is exacerbated by low public digital literacy, which has led to the high spread of AI-based information manipulation and fraud. In many cases, victims are unaware that the digital communications they receive are artificially engineered due to their high similarity to their original identities. This situation demonstrates that the development of AI technology has

created a new form of cyberfraud that is far more dangerous than conventional digital fraud, requiring a more adaptive and progressive legal approach (Juditha, 2025).

The challenges of law enforcement against Artificial Intelligence-based digital content manipulation ultimately demonstrate the urgency of national legal reform in addressing the development of modern cybercrime. From the perspective of Lawrence M. Friedman's legal system theory, the weakness of law enforcement against AI-based cybercrime arises from the lack of synchronization of legal substance, legal structure, and legal culture within the national legal system. Therefore, legal reconstruction is needed, including the establishment of specific regulations regarding artificial intelligence crime, political deepfakes, and synthetic media manipulation as part of the national cyber legal system. Furthermore, the capacity of cyber policing needs to be strengthened through the establishment of an AI forensic unit, the development of cyber predictive policing, the enhancement of digital forensic competencies, and the reinforcement of international cooperation in handling transnational cybercrime. The state is also required to develop a public protection system based on cyber resilience and digital literacy to prevent the spread of AI-based content manipulation in the digital public sphere. This legal reform reflects the state's obligation to protect the public, as mandated by the Preamble of the 1945 Constitution of the Republic of Indonesia, which affirms the objective of protecting the entire Indonesian nation and all its territory.

Weaknesses of the Indonesian National Police's Strategy in Countering Artificial Intelligence-Based Digital Content Manipulation from a Cyber Policing and National Security Perspective

The Indonesian National Police's strategy in countering artificial intelligence-based digital content manipulation still faces various fundamental weaknesses in terms of regulation, institutions, technology, and human resource capacity. Developments in artificial intelligence technologies such as deepfakes, voice cloning, synthetic media, and AI-generated content have created new, fast-moving crime patterns that are difficult to detect through conventional law enforcement approaches. However, the police's strategy in addressing these threats still tends to be reactive, focusing primarily on taking action after a crime has occurred, rather than on technology-based prevention and early detection systems. This situation demonstrates that the cyber policing system in Indonesia has not yet fully adapted to the transformation of modern digital threats. Normatively, the duties and authorities of the Indonesian National Police are regulated in Law Number 2 of 2002, specifically Article 13, which states that the main duties of the Indonesian National Police include maintaining public security and order, enforcing the law, and providing protection, guidance, and services to the community. Furthermore, Article 14 paragraph (1) letter g affirms the authority of the Indonesian National Police (Polri) to conduct inquiries and inquests into all criminal acts in accordance with criminal procedure law and other laws and regulations. However, this regulation does not specifically accommodate an artificial intelligence-based cyber policing strategy, resulting in the police's approach to digital content manipulation remaining fragmented and not yet systematically integrated within the national cybersecurity framework.

The main weakness of the Indonesian National Police's strategy is seen in the limited technological and digital forensic capacity in detecting artificial intelligence-based digital content manipulation. Modern deepfakes and voice cloning have a very high level of authenticity, making them difficult to distinguish from genuine content, even by law enforcement officers. In empirical practice, various cases of the spread of manipulated videos, AI-based hoaxes, and digital fraud involving the impersonation of officials and family members demonstrate that digital forensic detection capabilities in Indonesia remain very limited. Many cases of manipulated content have spread widely on social media before police officers are able to clarify or take legal action. This demonstrates the weakness of the police's early warning and cyber surveillance systems. In fact, Article 15, paragraph (1), letter c of Law Number 2 of 2002 gives the National Police the authority to prevent and address the growth of social ills, including cybercrimes that disrupt public security. However, empirically, the National Police does not yet have an AI forensic unit that specifically handles deepfake and synthetic media crimes. The limitations of technological devices for detecting AI-generated content and the lack of artificial intelligence-based digital forensic laboratories cause the investigation process to run slowly, and often make it difficult to determine the authenticity of electronic evidence. This situation shows a gap between the development of digital crime technology and the institutional capacity of the police in carrying out modern cyber policing.

In addition to technological limitations, the weakness of the National Police's strategy is also evident in the lack of strengthening of internal regulations and operational standards for handling Artificial Intelligence-based digital content manipulation. To date, there are no internal National Police regulations specifically governing the handling of deepfakes, voice cloning, or AI-generated disinformation as threats to national digital security. Consequently, case handling still uses a general approach based on the provisions of Law Number 1 of 2024 and the Criminal Code, which are fundamentally not designed to address the characteristics of artificial intelligence crimes. In practice, law enforcement officers often struggle to determine the appropriate article construction for perpetrators of AI-based content manipulation due to the lack of legal definitions of deepfakes or synthetic media manipulation in the national legal system. In some cases of the spread of political hoaxes and manipulative videos, the law enforcement process focuses more on the consequences of the dissemination of false information than on the use of artificial intelligence as the primary instrument of crime. This situation indicates that the National Police's law enforcement strategy remains oriented towards a conventional repressive approach and has not yet developed an artificial intelligence-based predictive policing approach. Yet, from a modern cybersecurity perspective, cyber policing functions not only as a criminal enforcement measure but also as a digital intelligence system to detect, mitigate, and prevent cyber threats before they cause wider harm to society and the state.

The deficiency of the police strategy is also evident in the poor coordination between institutions in addressing the threat of Artificial Intelligence-based digital content manipulation. Combating deepfakes and AI-based cybercrime requires synergy between the Indonesian National Police (Polri), the National Cyber and Crypto Agency (BKSDA),

the Ministry of Communication and Digital Affairs of the Republic of Indonesia, the Attorney General's Office (AGO), state intelligence agencies, and global digital platforms. However, empirically, this coordination has not been optimal, resulting in delayed and unintegrated responses to the spread of manipulative content. In some cases of hoaxes and political disinformation, the process of taking down digital content takes considerable time due to weak coordination between law enforcement officials and social media platforms. Furthermore, the lack of a real-time data exchange system between institutions makes identifying perpetrators and tracking digital footprints less effective. In fact, Article 30, paragraph (4) of the 1945 Constitution of the Republic of Indonesia emphasizes that the Indonesian National Police, as a state instrument that maintains public security and order, is tasked with protecting, serving, and enforcing the law. In the digital national security, protecting the public is no longer sufficient through physical patrols and conventional law enforcement, but requires an integrated cybersecurity system that is capable of responding to digital threats quickly, in a coordinated manner, and based on intelligent technology. The absence of a strong national cyber coordination system means that handling AI-based content manipulation is still sectoral and ineffective in dealing with the increasingly complex escalation of digital threats.

Another empirical problem is the low capacity of human resources within the police force in the fields of artificial intelligence and cybersecurity. The development of AI technology is progressing much faster than the development of the competence of law enforcement officers, resulting in many investigators lacking the technical skills to understand the workings of deepfakes, machine learning, and synthetic media algorithms. This situation causes the investigation process into AI-based cybercrime to become highly dependent on external experts and specific digital laboratories. From a cybercriminology perspective, the development of cybercrime requires law enforcement officers with multidisciplinary skills encompassing law, information technology, digital forensics, and cyberintelligence. However, empirically, training and competency development for AI policing within the Indonesian police force remain relatively limited. Furthermore, limited budget and technological infrastructure also pose serious obstacles to the development of artificial intelligence-based smart policing. Article 13(a) of Law Number 2 of 2002 stipulates that the National Police (Polri) is tasked with maintaining public order and security, which in the current digital context includes cyberspace security and protecting the public from the threat of AI-based information manipulation. The unpreparedness of human resources and police institutions to face this technological transformation has the potential to render the state incapable of ensuring the digital security of the public in the era of artificial intelligence.

The weaknesses in the Indonesian National Police's strategy in dealing with Artificial Intelligence-based digital content manipulation ultimately demonstrate the need for an updated cyber policing system within a modern national security framework. The threats of deepfakes, digital disinformation, and AI-based fraud can no longer be seen as ordinary crimes, but rather as multidimensional threats that can disrupt political stability, economic security, and the integrity of national democracy. Therefore, the police strategy needs to be

restructured through the development of artificial intelligence (AI)-based predictive policing, the establishment of a dedicated AI forensic unit, the strengthening of cyber intelligence capabilities, and the integration of national cybersecurity systems across relevant agencies. In addition, internal regulations within the Indonesian National Police (Polri) are required to govern the handling of AI-based cybercrime, along with the strengthening of international cooperation to effectively combat transnational digital crime. From a national security perspective, the reform of cyber policing strategy must be directed at building a cyber-resilience society by increasing public digital literacy and strengthening early detection systems for digital information manipulation. This step implements the mandate of the Preamble to the 1945 Constitution of the Republic of Indonesia, which affirms the state's goal to protect the entire Indonesian nation and its entire territory. Therefore, strengthening the police strategy based on smart policing and artificial intelligence is an urgent need to realize a national security system that is adaptive to the development of cyber threats in the era of digital transformation.

Legal Updates to the Indonesian National Police's Strategy for Combating Artificial Intelligence-Based Digital Content Manipulation through Strengthening Smart Policing and Cyber Resilience

Legal updates to the Indonesian National Police's strategy for combating artificial intelligence-based digital content manipulation are urgently needed to address the increasingly complex and organized developments in modern cybercrime, which have a wide-ranging impact on national stability. The development of deepfake technology, voice cloning, synthetic media, and AI-generated content has created new threats to digital security, democratic integrity, and the economic security of society, rendering conventional law enforcement approaches inadequate. Therefore, legal updates must be directed at developing an artificial intelligence-based smart policing system capable of working preventively, predictively, and responsively to detect and combat digital content manipulation. Normatively, these updates align with the mandate of Law Number 2 of 2002, specifically Article 13, concerning the National Police's duties in maintaining public order and security and enforcing the law in all social spaces, including the digital space. Furthermore, Article 30, paragraph (4) of the 1945 Constitution of the Republic of Indonesia affirms that the Indonesian National Police (Polri) is a state instrument tasked with maintaining public security and order and providing protection to the public. In this context, concrete action that must be taken is the establishment of specific national regulations regarding Artificial Intelligence Crime and Deepfake Regulations, which regulate legal definitions, classifications of criminal acts, criminal liability, digital evidence mechanisms, and the obligations of digital platforms to detect and remove AI-based manipulative content. These regulations must also establish specific criminal sanctions for the use of AI for political propaganda, digital impersonation, and cyber fraud to create legal certainty within the national law enforcement system.

Legal reform must also be realized through strengthening cyber policing institutions based on smart policing within the Indonesian National Police. The proposed Artificial Intelligence and Cyber Manipulation Crime Directorate may operate within the existing

cybercrime structure and exercise specialized authority in handling deepfakes, synthetic-media manipulation, digital impersonation, and AI-enabled cyber fraud. Its investigative functions should be supported by the establishment of a National AI Digital Forensic Center responsible for the scientific examination and authentication of suspected AI-generated or manipulated digital material.

The conclusions of the National AI Digital Forensic Center should not be treated as automatically conclusive. Forensic assessment must be based on documented and reproducible methods, validated detection tools, known or measurable error limitations, independent verification where technically feasible, and human expert review. A forensic conclusion should express the degree of confidence and methodological limitations of the examination rather than simply declaring content to be “real” or “fake.”

The legal framework should further establish a specific chain of custody for AI-related digital evidence. This chain should record the origin of the material, the method and time of acquisition, cryptographic integrity verification, metadata preservation, every transfer or duplication, forensic processing, analytical tools used, and the identity of each authorized person handling the evidence. Where available, provenance information, content credentials, cryptographic signatures, model identifiers, or generation records may be examined, but the absence of such information must not automatically invalidate evidence because AI-generated material may originate from open-source, anonymous, or untraceable systems.

AI-assisted forensic findings should therefore be admissible only as electronic or expert-supported evidence subject to adversarial examination. The parties must be able, where relevant, to challenge the reliability of the forensic methodology, integrity of the chain of custody, analytical limitations, and conclusions of the examining experts. This framework complements the recognition of electronic information and electronic documents as legal evidence under Article 5 paragraphs (1) and (2) of Law Number 1 of 2024 while providing more specific procedural safeguards for AI-related evidence (Pramesti, 2025).

Predictive cyber policing should not operate as an autonomous mechanism for determining criminality. AI-assisted monitoring may be used to identify patterns, anomalies, coordinated dissemination, repeated impersonation techniques, or other indicators requiring further assessment, but an automated risk score or algorithmic classification must never constitute the sole basis for criminal investigation, content removal, arrest, or other coercive measures.

The operation of predictive systems should therefore be governed by the principles of legality, necessity, proportionality, purpose limitation, and human oversight. High-impact decisions must be subject to meaningful human review, and systems should undergo periodic testing for accuracy, false-positive rates, discriminatory or systematic bias, and unintended interference with legitimate expression. Monitoring should prioritize publicly available or lawfully accessible content and must not justify indiscriminate surveillance of private communications or individuals who have not met an objectively defined legal threshold for further investigation.

Legitimate political criticism, satire, journalism, artistic expression, academic discussion, and other forms of protected communication must not be classified as criminal merely because they contain controversial narratives, manipulated imagery, or AI-generated elements. The relevant legal question should remain the combination of deceptive representation, intent, unlawful purpose, concrete or reasonably foreseeable harm, and the applicable substantive offense, rather than the mere use of artificial intelligence.

In addition to institutional strengthening, legal reform must also be directed toward the establishment of an Integrated National Cyber Security Command as a coordination mechanism for responding to cross-sectoral threats involving AI-generated manipulation, deepfakes, synthetic impersonation, and coordinated digital deception. To prevent the creation of a new institution with overlapping operational authority, the Command should function primarily as a legally defined coordination, information-sharing, and national crisis-management mechanism rather than as an independent substitute for the statutory powers of participating agencies.

BSSN should exercise primary national coordinating authority in relation to cybersecurity and national cyber-risk coordination, while Polri retains authority over criminal investigation and law enforcement, Komdigi retains authority concerning electronic system governance and platform compliance, the Attorney General's Office retains prosecutorial authority, and intelligence institutions operate according to their respective statutory mandates. Where an incident develops into a criminal investigation, operational command over investigative measures remains with the competent law-enforcement authority.

The regulatory framework should establish a clear command hierarchy based on the nature of the incident, a written division of institutional functions, standardized data-sharing procedures, mandatory incident reporting, and an auditable record of significant decisions. No institution should acquire unlimited authority over the functions of another agency merely by participating in the Integrated National Cyber Security Command. Accountability should be ensured through periodic reporting, independent audit, and legally defined responsibility for unauthorized data access, unlawful surveillance, or failure to comply with established coordination procedures.

Legal reforms to the police strategy must also be realized through strengthening human resources and developing AI-based cyber policing competencies. The rapid development of AI demands that law enforcement officers possess multidisciplinary capabilities that encompass not only criminal law but also digital technology, machine learning, cyber forensics, and cyber intelligence. Therefore, a concrete action that needs to be taken is the establishment of an AI Cyber Policing Academy as a specialized education and training center for police officers in the fields of artificial intelligence investigation, deepfake detection, cyber intelligence analysis, and modern digital forensics. Furthermore, the Indonesian National Police (Polri) needs to establish strategic partnerships with universities, technology research institutions, and global technology companies to strengthen the technical capacity of law enforcement officers in addressing AI-based

cybercrime. This human resource development must also be accompanied by the modernization of the police's technological infrastructure through the procurement of AI-powered cyber patrol systems, automated digital evidence analysis, and predictive threat intelligence platforms to detect patterns in the spread of manipulated digital content on social media. From a smart policing perspective, the police no longer act solely as conventional law enforcers but also as cyber guardians capable of proactively and sustainably maintaining the stability of the national digital space.

In addition, legal reforms must also be directed at developing a digital literacy-based public protection system and public participation in combating artificial intelligence-based digital content manipulation. The threat of deepfakes and AI-generated disinformation is not only caused by weaknesses in state security technology, but also by the public's low ability to recognize digital information manipulation. Therefore, concrete action that must be taken is the establishment of a National Digital Literacy and Anti-Deepfake Movement involving the government, police, academics, media, and civil society in raising public awareness of the dangers of AI-based digital content manipulation. This program can be realized through national education on deepfake awareness, digital information verification training, and the development of public AI detection tools that can be used by the public to verify the authenticity of digital audio and video. Furthermore, the Indonesian National Police (Polri) needs to develop an artificial intelligence-based Cyber Public Complaint System that allows the public to report manipulative content and is integrated with the police investigation system. This stage is crucial for creating collaborative cyber policing between state officials and the public in maintaining the security of the national digital space.

Legal updates to the Indonesian National Police's strategy for combating Artificial Intelligence-based digital content manipulation must be directed at developing a modern, adaptive, and sustainable digital national security system. The threat of deepfakes, digital propaganda, and AI-based cyber fraud is no longer just a matter of ordinary crime but rather a threat to information sovereignty, political stability, and national resilience in the era of digital transformation. Therefore, the state must undertake comprehensive reform of the cyber policing system by establishing national AI crime regulations, strengthening smart policing, building cyber resilience, developing modern digital forensics, and integrating artificial intelligence-based national cybersecurity. All of these steps implement the mandate of the Preamble to the 1945 Constitution of the Republic of Indonesia, which affirms the state's goal to protect the entire Indonesian nation and its entire nation. Therefore, legal updates to the police strategy based on smart policing and cyber resilience are an important foundation for realizing a responsive, progressive cyber law enforcement system capable of facing the threat of Artificial Intelligence-based digital content manipulation in the future.

The proposed legal reconstruction should be translated into a structured regulatory model governing artificial intelligence-based digital content manipulation. First, the regulatory framework should define AI-generated content, synthetic-media manipulation, deepfake crime, synthetic impersonation, and political deepfakes in a technologically

neutral manner. The mere generation or use of AI content should not constitute a criminal offense. Criminal liability should arise only where legally defined elements of deception, intent, unlawful purpose, and concrete or reasonably foreseeable harm are satisfied. Political expression, parody, satire, journalism, education, research, and artistic expression should remain protected unless the relevant conduct independently fulfills the statutory elements of an offense. Second, digital platforms and AI service providers should be subject to proportionate due-diligence obligations. These obligations may include reasonable AI-content labeling or provenance mechanisms, preservation of available content credentials, risk-based detection of synthetic impersonation, accessible reporting channels, preservation of relevant evidence following a lawful request, and proportionate response procedures for verified unlawful content. Watermarking should not be treated as an absolute condition of legality because content may originate from open-source models, foreign providers, user modification, or systems without reliable attribution. The deliberate removal or alteration of provenance information for the purpose of deception may, however, constitute an aggravating factor where connected with an independently unlawful act.

Third, emergency takedown or restriction mechanisms should be based on clearly defined thresholds. A platform or competent authority should act rapidly where there is a verified and imminent risk of serious fraud, public disorder, electoral manipulation, impersonation causing substantial harm, or other legally protected interests. Temporary emergency measures should be subject to prompt human review, documented reasons, time limitations, and an accessible correction or appeal mechanism where content is wrongly restricted. Fourth, AI-related digital evidence should comply with specific standards concerning provenance, metadata integrity, cryptographic verification, chain of custody, reproducibility of forensic methods, disclosure of relevant methodological limitations, expert qualification, and the possibility of independent verification. Automated detection tools should assist rather than replace forensic judgment, and the degree of certainty or error limitation of the examination should be disclosed in legal proceedings. Fifth, AI-assisted predictive cyber policing should be limited to lawful, necessary, and proportionate purposes. Automated systems may generate risk indicators but may not independently establish criminal liability, justify coercive action, or permanently restrict expression. Significant decisions must remain subject to meaningful human oversight, periodic accuracy and bias audits, and accountability mechanisms for wrongful classification or unlawful surveillance.

Finally, the proposed Integrated National Cyber Security Command should operate through a clear division of authority among BSSN as national cybersecurity coordinator, Polri as criminal law-enforcement authority, Komdigi as the authority responsible for electronic-system and platform governance, and other institutions according to their statutory mandates. Inter-agency data sharing should follow purpose limitation, role-based access, cybersecurity standards, logging, retention limits, and accountability for unauthorized access or misuse. Through this structure, the legal reconstruction would strengthen cyber resilience while maintaining freedom of expression, privacy, evidentiary integrity, and due process of law.

Conclusion

This study concludes that the development of artificial intelligence (AI)-driven digital content manipulation, including deepfakes, voice cloning, synthetic media, and AI-generated content, has generated new forms of cybercrime that pose significant threats to national security, democratic integrity, the stability of the digital economy, and the protection of public rights in cyberspace. The misuse of artificial intelligence technology as a means of political crime and cyber fraud demonstrates that the national legal system and existing law enforcement strategies are not yet fully capable of anticipating the transformation of modern digital threats. Law enforcement problems are evident in the weak legal substance due to the lack of specific regulations regarding AI crime, political deepfakes, and synthetic media manipulation, the limitations of the legal structure in the form of minimal capacity for cyber policing and digital forensic artificial intelligence, and the weak legal culture of the community due to low digital literacy and the high spread of disinformation. Furthermore, the Indonesian National Police's strategy still tends to be reactive and repressive, thus hampering the optimal development of predictive policing and AI-based cyber intelligence approaches. This situation demonstrates the urgent need for legal reforms to the police's strategy in combating Artificial Intelligence-based digital content manipulation by strengthening smart policing and cyber resilience as part of a digital national security system in the era of information technology transformation.

From these conclusions, this study highlights the urgency of establishing specific national regulations on Artificial Intelligence crime that comprehensively define, classify, and determine criminal liability, as well as set out clear law enforcement mechanisms for AI-based digital content manipulation, particularly in relation to political crimes and cyber fraud. Furthermore, the Indonesian National Police (Polri) needs to undertake institutional reform by establishing a special AI forensic and cyber predictive policing unit supported by deepfake detection system technology, cyber intelligence analytics, and an integrated digital forensic laboratory to improve the effectiveness of cyber law enforcement. The state also needs to build an integrated national cybersecurity system between the Indonesian National Police (Polri), the National Cyber and Crypto Agency (BKSDA), the Ministry of Communication and Digital of the Republic of Indonesia, the Attorney General's Office (KPK), and global digital platforms within a collaborative cybersecurity and cyber resilience framework. Furthermore, strengthening public digital literacy must be a national strategic policy to improve the public's ability to recognize artificial intelligence-based information manipulation and prevent the spread of disinformation in the digital space. Thus, legal updates to police strategies based on smart policing and cyber resilience are expected to create a cyber law enforcement system that is adaptive, progressive, and responsive to the development of Artificial Intelligence-based digital crimes in Indonesia.

References

- Adella, S. J. (2026). Perlindungan Hukum terhadap Korban Penyalahgunaan Kecerdasan Buatan (Artificial Intelligence) sebagai Alat Pencipta Konten Viral. *Judge: Jurnal Hukum*, 1471–1478.
- Ahda, H. a. (2026). Dampak Pemanfaatan Artificial Intelligence Generatif terhadap Praktik Komunikasi Digital dan Etika Media di Indonesia. *DIGIMUN-Digital Communication*

Journal, 33–37.

- Anthony, C. A. (2023). Peranan Audit Internal dalam Pengendalian Fraud di Era Digital. *Accounting Student Research Journal*, 31–45.
- Apriliana, H. K. (2024). Perkembangan Penerapan Teknologi Artificial Intelligence Di Indonesia. *Jurnal Syntax Admiration*, 3864–3874.
- Beck, U. (1992). *Risk Society: Towards a New Modernity*. London: Sage Publications.
- Cantika, N. F. (2025). Pertanggungjawaban Pidana Atas Penyalahgunaan Artificial Intelligence (Ai) Dalam Produksi Konten Hoaks Dan Deepfake Di Media Sosial. *Jurnal Kepemimpinan Dan Pengurusan Sekolah*, 2590–2599.
- Erdiyanti, N. L. (2026). Perlindungan hukum terhadap korban sexual harassment akibat manipulasi konten digital berbasis artificial intelligence. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 3915–3924.
- Juditha, C. (2025). Artificial Intelligent Dan Hoaks: Tantangan Disrupsi Bagi Literasi Digital Masyarakat Di Komunitas Online Dan Upaya Antisipasi Pemerintah. *Jurnal Ilmiah Manajemen Informasi Dan Komunikasi*, 534–547.
- Kurniarullah, M. R. (2024). Tinjauan Kriminologi terhadap Penyalahgunaan Artificial Intelligence: Deepfake Pornografi dan Pencurian Data Pribadi. *Jurnal Ilmiah Wahana Pendidikan*, 10(10).
- Librianti, E. O. (2025). Deepfake Dalam Komunikasi Politik: Tantangan Etika dan Aspek Hukum Dalam Era Artificial Intelligence. *Siyasah*, 221–283.
- Novera, O. (2024). Analisis Pengaturan Hukum Pidana terhadap Penyalahgunaan Teknologi Manipulasi Gambar (Deepfake) dalam Penyebaran Konten Pornografi Melalui Akun Media Sosial. *El-Faqih: Jurnal Pemikiran Dan Hukum Islam*, 10(2), 460–474.
- Nurwahid, T. S. (2026). Deepfake sebagai Kejahatan: Manipulasi AI Audio, Video, dan Gambar dalam Hukum Pidana Indonesia. *LEGAL DIALOGICA*.
- Pramesti, I. A. (2025). Regulasi Di Indonesia Terkait Tindak Pidana Kekerasan Seksual Berbasis Digital Melalui Deepfake. *Jurnal Media Akademik (JMA)*.
- Pratama, L. R. (2026). Pengaturan Pidanaan Penyalahgunaan Artificial Intelligence dalam Penyebaran Hoax Politik Melalui Media Sosial. *Jurnal Ilmu Sosial Dan Humaniora*, 780–791.
- Ramadhina, N. F. (2023). Dinamika perubahan dalam komunikasi manusia di era teknologi artificial intelligence. *Communicator Sphere*, 114–123.
- Sabela, I. N. (2026). Hoaks Berbasis Kecerdasan Buatan Ai Sebagai Tantangan Literasi Media Sosial. *RELASI: Jurnal Penelitian Komunikasi*, 44–54.
- Tarigan, I. F. (2025). No Title. *Analisis Pola Tren Transaksi Mencurigakan Pada Aplikasi Dana Sebagai Indikator Fraud Digital Tahun 2020-2024*, 259–266.