Customary Law Journal, AICOPS Special Collection 2026, *Page*: 1-17

Strengthening the Smart Policing Legal System in Preventing Digital Radicalization through the Utilization of Big Data and Cyber Surveillance in Indonesia

Bambang Yulianto*, Albertus Wahyurudhanto, Kif Aminanto

Sekolah Tinggi Ilmu Kepolisian, South Jakarta, Indonesia ; bambangyuliyuni@gmail.com
Sekolah Tinggi Ilmu Kepolisian, South Jakarta, Indonesia ; wahyurudhanto@stik-ptik.ac.id
Sekolah Tinggi Ilmu Kepolisian, South Jakarta, Indonesia ; kif.92pw@gmail.com

DOI:
https://doi.org/10.47134/jcl.v3i3.2.6326
*Correspondence: Bambang Yulianto
Email: bambangyuliyuni@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/).

Abstract: *The development of digital transformation has led to the emergence of digital radicalization or cyber radicalization as a new form of threat to national security that develops through social media, encrypted communication, artificial intelligence, and various cyberspace-based digital platforms. This study aims to discuss the threat of digital radicalization from a national legal perspective, examine the weaknesses of conventional cyber surveillance and law enforcement systems in Indonesia, and formulate a legal reconstruction of smart policing based on big data and cyber intelligence in preventing digital radicalization. This study employs a normative juridical method under legislative and conceptual approaches by analyzing various regulations related to cybersecurity, terrorism, personal data protection, and digital law enforcement. The results show that the Indonesian legal system still faces regulatory disharmony, weak integration of authority between institutions, limitations in cyber intelligence, and the absence of a comprehensive legal basis for cyber surveillance, predictive policing, and the use of artificial intelligence in cyberspace surveillance. Therefore, legal reform is needed through the establishment of national smart policing regulations, integration of big data for cybersecurity, strengthening cyber intelligence, institutional harmonization, and the development of an accountable digital surveillance system based on human rights protection. The legal reconstruction is expected to create an effective smart policing system to prevent the spread of digital radicalism while still ensuring the principles of the rule of law, constitutional democracy, and the protection of citizens' privacy rights in Indonesian cyberspace.*

Keywords: *smart policing, digital radicalization, cyber intelligence.*

Introduction

The development of digital transformation in the last two decades has fundamentally changed the lifestyle of Indonesian society, especially through the increased use of the internet, social media, artificial intelligence, encrypted communication, and various digital platforms that have made cyberspace a central part of modern society's social activities. (Erwin, 2023) Based on Article 28F of the 1945 Constitution of the Republic of Indonesia, everyone has the right to communicate and obtain information to develop their personality and social environment, including seeking, obtaining, possessing, storing, processing, and conveying information through all available channels. This constitutional provision was further reinforced by Law Number 11 of 2008 on Information and Electronic Transactions, as amended by Law Number 1 of 2024, which recognizes the legality of electronic activities

in cyberspace (Wijaya, P., & Gusliana, 2024). However, the rapid development of information technology has also caused cyberspace to no longer function only as a communication medium, but has developed into a space for forming public opinion, an arena for political contestation, the spread of ideology, mass mobilization, and even a means of information warfare that transcends the boundaries of state jurisdiction. The dominance of algorithm-based social media platforms such as short videos, live streaming, podcasts, digital forums, and encrypted communication platforms has created new patterns of interaction that are borderless, real-time, massive, and anonymous (Makarawung, 2026). This situation has made state control over the flow of information increasingly complex, as the distribution of content is no longer limited by geographic space or conventional surveillance mechanisms. In this regard, the development of digital technology has created new challenges for the national legal system, as the state is required to continue to guarantee freedom of expression and citizens' digital rights, while simultaneously maintaining national security from the threat of misuse of cyberspace for radicalization and digital extremism.

This development in cyberspace has been accompanied by a shift in the spread of radical ideology from conventional methods to digital radicalization, or cyber radicalization, which utilizes information technology as the primary instrument for the spread of extremist ideology. While previously the spread of radicalism occurred through closed meetings, exclusive religious studies, or specific organizational networks, today the radicalization process occurs digitally through social media, online forums, video platforms, podcasts, gaming platforms, the dark web, and even encrypted messaging applications such as end-to-end encrypted communication. (Susanti, 2020) This transformation in methods has resulted in the spread of radical ideology becoming faster, more anonymous, difficult to trace, transnational, and capable of reaching a wider community without direct physical contact. From a national legal perspective, this threat is closely related to the provisions of Law Number 5 of 2018 concerning Amendments to Law Number 15 of 2003 concerning the Eradication of Criminal Acts of Terrorism, which broadens the approach to countering terrorism through aspects of prevention, national preparedness, counter-radicalization, and deradicalization. Articles 43A to 43D of the Terrorism Law emphasize that the government has an obligation to prevent the spread of radical ideology that leads to terrorism (Shabirin, 2025). However, in practice, these regulations are still more oriented towards physical threats and have not fully addressed the characteristics of cyber radicalization based on digital algorithms, anonymous networks, and artificial intelligence. As a result, the pattern of digital radicalization has developed into a new security threat that is not only difficult to detect but also capable of forming self-radicalization and lone wolf terrorism without the involvement of conventional terrorist organizations. (Betawi, 2025)

In practice, digital radicalization develops through increasingly complex and structured methods, ranging from the spread of digital propaganda, the production of hate narratives, online recruitment, digital fundraising, and the use of artificial intelligence to automatically and massively produce extremist content. Social media platforms, with their personalized content and micro-targeting algorithms, indirectly reinforce the formation of echo chambers, causing users to be continuously exposed to radical content tailored to their

digital preferences (Putra, 2026). This situation is exacerbated by the ability of digital platform algorithms to automatically recommend similar content based on user search history, interactions, and behavior.

From a national security perspective, this situation poses a serious threat to the state ideology, social stability, and national resilience, as mandated in the Preamble to the 1945 Constitution, which affirms the state's goal of protecting the entire Indonesian nation and its entire homeland. The spread of digital radicalism is also closely linked to acts of terrorism, cyberterrorism, hate speech, disinformation, and anti-state propaganda, which have the potential to trigger social conflict and national disintegration. (F. K. Kusuma, 2021) Provisions regarding the prohibition of the dissemination of information inciting hatred and hostility are actually regulated in Article 28, paragraph (2), in conjunction with Article 45A, paragraph (2) of the ITE Law. However, this norm still faces problems in implementation due to difficulties in identifying transnational perpetrators, the use of anonymous accounts, the use of VPNs, encrypted communication, and weak national cyber intelligence mechanisms (Sepima, 2020). Therefore, the threat of digital radicalization can no longer be viewed as an ordinary crime, but rather as an extraordinary, technology-based crime that requires a legal and security approach that adapts to developments in modern cyberspace.

On the other hand, the Indonesian legal framework for addressing digital radicalization still presents several normative and institutional challenges. Academic discussions have identified limitations relating to cyber-intelligence capacity, digital surveillance, inter-agency data integration, early detection, and the handling of electronic evidence (Usrinase, 2025). Because this study employs a normative juridical method, these conditions are not presented as independent empirical findings of the research, but as contextual issues identified in relevant literature and used to examine the adequacy of the existing legal framework.

From a normative perspective, the more fundamental issue is the fragmentation of authority and the absence of sufficiently clear legal standards governing cyber surveillance, big-data collection, digital profiling, and the use of artificial intelligence by state institutions. Regulatory interaction between the ITE Law, the Terrorism Law, Law Number 27 of 2022 concerning Personal Data Protection, and other cybersecurity regulations may create uncertainty regarding institutional authority and the permissible limits of digital surveillance (Widagdo, 2017). Therefore, the central problem examined in this study is not the quantitative measurement of institutional weakness, but whether the existing legal architecture provides an integrated, accountable, and constitutionally legitimate framework for preventing digital radicalization.

In facing the complexity of these threats, the concept of smart policing has become relevant as a modern policing model based on digital technology that utilizes big data, artificial intelligence, predictive policing, cyber intelligence, digital profiling, and real-time surveillance to support the prevention of digital radicalization. The concept of smart policing essentially represents a transformation of the modern police system from a reactive approach to a predictive approach based on data and information technology. (Jaladriyanta, 2020) Through the integration of big data analytics, law enforcement officers can map patterns of radical propaganda distribution, identify digital networks, analyze online

behavior, and even detect potential extremist threats before they develop into terrorist acts. In state administrative law, the implementation of smart policing is also in line with the principles of good governance, government effectiveness, and the use of information technology in implementing national security. However, the implementation of this system must have a clear legal basis so as not to conflict with the principles of due process of law, the principle of legality, and the protection of human rights as guaranteed in Article 28J of the 1945 Constitution which emphasizes that restrictions on rights can only be carried out based on law to guarantee recognition and respect for the rights and freedoms of others and in the interests of national security and public order (Santoso, 2025). Therefore, the implementation of smart policing must not be solely oriented towards security effectiveness, but must also pay attention to the proportionality principle, the necessity principle, accountability of supervision, and control mechanisms for the use of surveillance technology by the state.

Based on these various issues, Indonesia needs to reform and reconstruct its smart policing legal system, adapting to developments in digital technology and the threat of modern cyber radicalization. This legal reform must integrate cyber surveillance systems, cyber intelligence, big data utilization, and artificial intelligence while ensuring the protection of human rights and the principles of a democratic state based on the rule of law. Legal reform is also needed to clarify the division of authority between institutions, establish legitimate data exchange mechanisms, strengthen the legal basis for cyber surveillance, and create standards of accountability and oversight for the use of digital technology by state officials. The experiences of countries such as the United States, the United Kingdom, Singapore, Australia, and China demonstrate that strengthening cyber intelligence and predictive policing can increase the effectiveness of preventing digital radicalism, but at the same time, it also raises serious debates about privacy, mass surveillance, and the protection of civil liberties. Therefore, Indonesia must develop a smart policing model that aligns with the characteristics of a state based on the rule of law, namely a digital surveillance system that is effective in maintaining national security while still respecting constitutional democracy and human rights. Thus, updating smart policing laws is an urgent need to create a modern, legitimate, adaptive, and equitable digital radicalization prevention system in the face of cybersecurity challenges 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 theory, and the synchronization of various laws and regulations related to smart policing, cyber surveillance, and the prevention of digital radicalization in Indonesia. Normative juridical research was chosen because the problems studied are based on normative gaps, regulatory disharmony, and the need for legal reformulation to address the growing threat of information technology-based digital radicalization. The approaches used in this study are the statute approach and the 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 concerning Electronic Information and Transactions, Law Number 5 of 2018

concerning the Eradication of Criminal Acts of Terrorism, Law Number 27 of 2022 concerning Personal Data Protection, as well as various regulations related to cybersecurity, police authority, and digital surveillance. Meanwhile, a conceptual approach is used to analyze the concepts of smart policing, cyber surveillance, predictive policing, cyber intelligence, big data analytics, as well as the theory of the rule of law, human rights protection, national security, and due process of law as a basis for formulating an ideal legal construction for a digital radicalization prevention system in Indonesian cyberspace. The legal materials used consist of primary legal materials, secondary legal materials, and tertiary legal materials that are analyzed prescriptively through legal interpretation techniques, legal systematization, and legal argumentation to produce a formulation of smart policing legal updates that are adaptive to developments in digital technology while still guaranteeing the principles of constitutional democracy and human rights protection.

Result and Discussion

Legal Analysis of the Threat of Digital Radicalization and Weaknesses in the Cyber Surveillance System in Indonesia

Developments in information and communication technology have created a major transformation in the processes through which radical ideas are communicated, disseminated, and amplified. For the purpose of this study, several concepts must be distinguished clearly. Digital radicalization refers to the process through which digital communication, platforms, networks, or algorithmic systems are used to expose, influence, mobilize, or reinforce individuals or groups toward extremist beliefs that may develop into support for violence. Cyber radicalization may be understood as a narrower form of digital radicalization in which cyberspace constitutes the primary environment for ideological interaction, recruitment, networking, and mobilization.

Extremism should not automatically be equated with criminal conduct because political, religious, academic, or ideological positions remain protected expressions unless they cross the legal threshold of incitement, recruitment, preparation, facilitation, or advocacy of unlawful violence. Radical content therefore refers to digital material containing ideological narratives, symbols, or messages associated with radical or extremist ideas, but such content does not necessarily constitute a criminal offense. It becomes legally relevant when, based on its context, purpose, dissemination pattern, and foreseeable effect, it satisfies the statutory elements of prohibited incitement, terrorist propaganda, recruitment, threats, or other unlawful conduct.

Cyberterrorism, by contrast, should be reserved for conduct involving the use of information and communication technology as a means, target, or operational infrastructure for terrorist activity, including attacks against critical systems or the use of cyberspace to facilitate legally defined terrorist offenses. Consequently, the relationship among these concepts is sequential rather than synonymous: digital radicalization may create a process of ideological influence; extremism refers to the ideological orientation; radical content constitutes a possible medium of expression; and cyberterrorism refers to conduct that has crossed into legally defined terrorist activity. This distinction is essential to ensure that the

prevention of digital radicalization does not improperly criminalize lawful political, religious, academic, or ideological expression (Aminudin, 2023).

The transformation of radicalization patterns from conventional to digital methods has occurred due to the development of social media and communication technology, which allows the spread of extreme ideologies quickly, massively, anonymously, and across national jurisdictions. While previously the radicalization process occurred through closed religious study groups, specific organizational networks, or physical meetings, the process has now evolved through digital platforms such as social media, live streaming, podcasts, gaming platforms, online forums, the dark web, and encrypted communication applications that are difficult for law enforcement to monitor. This modus operandi allows perpetrators to conduct digital propaganda, recruit members, raise funds, and coordinate actions covertly without direct physical contact. From a national criminal law perspective, these activities are closely linked to acts of terrorism as stipulated in Law Number 5 of 2018 concerning Amendments to Law Number 15 of 2003 concerning the Eradication of Criminal Acts of Terrorism. Article 1, number 2 of the Terrorism Law defines terrorism as an act that uses violence or the threat of violence that creates an atmosphere of terror or widespread fear and causes mass casualties or damage to vital strategic objects, the environment, public facilities, or international facilities for ideological, political, or security disturbance motives. Furthermore, Articles 43A to 43D of the Terrorism Law regulate the state's obligation to carry out prevention through national preparedness, counter-radicalization, and deradicalization. However, these norms still focus more on physical threats and do not comprehensively regulate cyber surveillance mechanisms for the spread of radical ideology based on digital technology. As a result, the development of cyber radicalization is far faster than the legal system's ability to conduct early detection and cyberspace surveillance (Wibowo, 2023).

In practice, the spread of digital radicalism through various increasingly complex patterns by utilizing social media algorithms and artificial intelligence to expand exposure to extremist propaganda to certain groups. Personalized content and micro-targeting algorithm systems cause internet users to continuously receive content recommendations similar to their digital preferences, thus creating an echo chamber that gradually strengthens the radicalization process. In addition, radical groups also utilize anonymous accounts, virtual private networks, cryptocurrency, and encrypted communication to avoid tracking by law enforcement officials. The use of these technologies has caused cyberspace to develop into a new medium for cyber terrorism that integrates digital propaganda, fundraising, member recruitment, and coordination of violent acts based on electronic networks. In the context of Indonesian positive law, the prohibition on the dissemination of information that incites hatred and hostility has actually been regulated in Article 28 paragraph (2) in conjunction with Article 45A paragraph (2) of Law Number 1 of 2024 concerning Information and Electronic Transactions, which regulates the prohibition on the dissemination of electronic information that incites hatred or hostility based on ethnicity, religion, race, and intergroup relations. In addition, Article 27A and Article 28 paragraph (3) of the ITE Law also provide a legal basis for taking action against the dissemination of

information containing threats of violence or disturbances to public order in the digital space. However, the implementation of these provisions still faces serious obstacles due to the transnational, anonymous, and encrypted communication-based nature of cyberspace, making the identification of perpetrators and proof of criminal acts very complex (N. S. Kusuma, 2021). The concern shows that the national legal system is still not fully capable of responding to the challenges of the development of digital technology used as a means of modern radicalization.

In addition to facing the complexity of digital threats, Indonesia's cyber surveillance system also faces institutional problems and regulatory disharmony, which have prevented effective handling of digital radicalization. Regulations regarding cyberspace surveillance are scattered across various regulations, such as the ITE Law, the Terrorism Law, Law Number 27 of 2022 concerning Personal Data Protection, Law Number 2 of 2002 concerning the Indonesian National Police, and various regulations related to cybersecurity and state intelligence. However, these regulations have not yet established an integrated cyber surveillance legal system, resulting in overlapping authority between the Indonesian National Police, the National Counterterrorism Agency, the National Cyber and Crypto Agency, and the Ministry of Communication and Digital in conducting surveillance, blocking, investigations, and digital data collection. For example, Article 14 paragraph (1), letter g of the Police Law authorizes the National Police to conduct inquiries and investigations into all criminal acts, including cybercrimes, while the National Cyber and Crypto Agency (BSSN), based on Presidential Regulation Number 28 of 2021, has the function of implementing national cybersecurity. On the other hand, Komdigi has the authority to control electronic systems and terminate access to illegal content based on Article 40 of the ITE Law. This situation indicates a fragmentation of authority that has the potential to lead to overlapping authority, weak coordination, and legal uncertainty in the practice of monitoring cyber activity. As a result, the state's response to the threat of digital radicalization is often partial, sectoral, and not supported by adequate integration of national cyber intelligence (Christy, 2020).

Another fundamental problem is the lack of clear regulations regarding the legality of cyber surveillance, digital profiling, and the use of big data by state officials to prevent digital radicalization. Digital surveillance directly affects citizens' rights to privacy and personal data protection, as guaranteed under Article 28G paragraph (1) of the 1945 Constitution and reinforced by Law Number 27 of 2022 on Personal Data Protection. Article 20 of the Personal Data Protection Law emphasizes that the processing of personal data must be carried out based on the valid consent of the data subject, while Article 65 prohibits the unlawful acquisition or collection of personal data. However, in the context of national security and terrorism prevention, the state also requires surveillance mechanisms and digital data collection to detect threats pre-emptively. The problem is that, to date, there are no clear normative boundaries regarding the legal standards for big data collection, digital activity monitoring, the use of artificial intelligence, or control mechanisms for electronic surveillance by state officials. This lack of norms has the potential to lead to abuse of power, mass surveillance, excessive profiling, digital criminalization, and violations of due process

of law. In a democratic state governed by the rule of law, state surveillance measures must comply with the principles of legality, proportionality, necessity, and accountability to prevent violations of citizens' constitutional rights (Mandala, 2024). Therefore, strengthening the cyber surveillance system cannot be done solely on the basis of security effectiveness, but must be built within a legitimate legal framework oriented toward human rights protection.

Based on these various issues, it is understandable that the threat of digital radicalization has grown far beyond the capabilities of Indonesia's current conventional cyber surveillance system. The national law enforcement system still faces limited human resources in the field of cyber intelligence, weak digital surveillance, minimal integration of big data between institutions, and the complexity of electronic evidence in the law enforcement process. Furthermore, regulatory disharmony and unclear authority between institutions mean that oversight of digital radicalism activities has not been carried out effectively, integrally, and accountably. Regardless of Article 30 paragraph (4) of the 1945 Constitution stating that the Indonesian National Police, as an instrument of the state, is tasked with protecting, serving, and enforcing the law to maintain public security and order. This provision demonstrates that the state has a constitutional obligation to build a cyber surveillance system capable of addressing the development of modern digital threats.

The Concept of Smart Policing Based on Big Data and Cyber Intelligence in Preventing Digital Radicalization

The concept of smart policing is essentially a form of transformation of the modern law enforcement system that utilizes developments in digital technology, big data, artificial intelligence, and cyber intelligence to increase the effectiveness of maintaining public security and order, including in preventing digital radicalization in cyberspace. The conventional policing model, which was previously reactive and focused on taking action after a crime had occurred, is deemed inadequate in addressing rapidly evolving, anonymous, and transnational cyber threats. Therefore, smart policing has developed as a technology-based preventive approach that enables law enforcement officers to conduct early detection, analyze threat patterns, and map digital networks in real time. From a national legal perspective, the implementation of smart policing is relevant to the duties and functions of the Indonesian National Police, as stipulated in Article 13 of Law Number 2 of 2002 concerning the Indonesian National Police, which affirms that the Indonesian National Police is tasked with maintaining public security and order, enforcing the law, and providing protection and services to the public. In addition, Article 14 paragraph (1) letter c and letter g of the Police Law gives the Indonesian National Police the authority to prevent and address the growth of social ills and to conduct investigations and inquiries into all criminal acts in accordance with criminal procedure law and other laws and regulations. In the context of the threat of digital radicalization, this task demands a transformation of the police system towards an information technology-based model that is capable of conducting cyber surveillance effectively and adaptively to the development of modern cyber radicalization.

The application of smart policing in preventing digital radicalization is carried out through the use of big data analytics and artificial intelligence to read people's digital behavior patterns and detect the potential spread of radical ideology in cyberspace. Big data enables security forces to collect, integrate, and analyze large amounts of digital data originating from social media, communication platforms, electronic transactions, online forums, and other cyber activities. Through this analysis, officers can identify patterns in the spread of radical propaganda, relationships between digital accounts, hidden communication networks, and user behavior that may indicate potential extremism. Meanwhile, artificial intelligence and machine learning are used for automated keyword detection, sentiment analysis, facial recognition, and real-time identification of suspicious communication patterns. This technology has subsequently evolved into predictive policing, a prediction-based surveillance system that enables security forces to map potential threats before criminal acts occur. In the context of national security, this approach aligns with Article 43A of Law Number 5 of 2018 concerning the Eradication of Criminal Acts of Terrorism, which emphasizes that the government is obliged to prevent criminal acts of terrorism through national preparedness and counter-radicalization. Therefore, smart policing can be understood as a modern instrument that supports the implementation of the state's obligation to prevent the development of digital radicalism and cyberterrorism through a data-based and information technology-based approach.

In addition to big data and artificial intelligence, the concept of smart policing also relies heavily on cyber intelligence and real-time surveillance to monitor digital activities that have the potential to threaten national security. Cyber intelligence is the process of collecting, processing, and analyzing digital information to detect cyber threats, radical network communication patterns, and propaganda activities developing in the digital space. In practice, cyber intelligence is conducted through monitoring social media, online forums, encrypted communication, and the dark web to obtain strategic information related to the spread of extremist ideology and potential acts of terrorism. Meanwhile, real-time surveillance allows authorities to conduct direct digital monitoring of certain electronic activities through an information technology-based monitoring system. In the context of Indonesian law, the use of electronic systems and digital surveillance has a normative basis in Law Number 1 of 2024 concerning Electronic Information and Transactions, specifically Article 40, which authorizes the government to prevent the dissemination of electronic information containing illicit content and disrupting public order. Furthermore, Article 43 of the ITE Law also grants law enforcement officials the authority to investigate cybercrimes. However, this regulation does not specifically address operational standards for cybersurveillance, the use of artificial intelligence in law enforcement, or the legal limits of digital profiling of citizens. As a result, the implementation of smart policing in Indonesia still faces a regulatory vacuum, leaving digital oversight mechanisms lacking legal certainty and clear accountability standards.

Internationally, various countries have developed smart policing and cybersurveillance models as part of their national security strategies to address the threats of digital radicalization and cyberterrorism. The United States, for example, developed a

predictive policing system and an intelligence fusion center through data integration between federal security agencies to detect extremist threats early after the September 2001 incident. The United Kingdom implemented a counter-radicalization system through its Prevent Strategy program, which utilizes social media monitoring and digital analysis to identify the potential spread of extremist ideology. Singapore is developing a smart nation security model by integrating artificial intelligence, surveillance cameras, and cyber intelligence into its national security system. Australia is developing digital surveillance based on anti-terrorism legislation to detect radical activity through the internet and encrypted communications. Meanwhile, China is implementing a broad digital surveillance model through facial recognition, a social credit system, and artificial intelligence surveillance as instruments of social control and state security. The experiences of these countries demonstrate that smart policing has become a crucial instrument for maintaining national security in the digital age. However, the implementation of these systems has also drawn serious criticism regarding mass surveillance, privacy violations, abuse of power, and the potential for digital criminalization by the state. Therefore, the development of smart policing must remain within the principles of the rule of law and the protection of human rights to prevent it from becoming an instrument of digital authoritarianism.

From the perspective of a democratic state based on the rule of law, the implementation of smart policing must adhere to the principles of due process of law, legality, proportionality, necessity, and the protection of human rights as guaranteed in the 1945 Constitution of the Republic of Indonesia. Article 28G paragraph (1) of the 1945 Constitution affirms that everyone has the right to protection of themselves, their families, their honor, their dignity, and their property, and the right to feel secure from the threat of fear for doing or not doing something that constitutes a human right. In addition, Article 28H paragraph (4) of the 1945 Constitution also guarantees the right to personal property and the protection of citizens' data and private lives. This protection is then strengthened through Law Number 27 of 2022 concerning Personal Data Protection, which stipulates that the processing of personal data must be carried out legally, in a limited, specific manner, and based on clear objectives. In the context of smart policing, the use of big data, digital profiling, and cyber surveillance has the potential to create conflicts between national security interests and citizens' privacy rights. If not strictly regulated, digital surveillance systems can develop into mass surveillance that violates civil liberties and creates abuse of power by state officials. Therefore, the implementation of smart policing must be based on the principle of proportionality and a clear need for national security threats, along with clear oversight, audit, and legal accountability mechanisms to ensure it does not conflict with the principles of constitutional democracy.

Based on these developments, smart policing based on big data and cyber intelligence is fundamentally a strategic necessity in a modern national security system to address the complex and inter-jurisdictional threat of digital radicalization. However, the effectiveness of smart policing implementation is determined not only by technological sophistication but also by the strength of the legal basis, institutional integration, and constitutional legitimacy of the state's digital surveillance system. Indonesia requires a

smart policing model capable of integrating artificial intelligence, predictive policing, cyber intelligence, and big data analytics in a coordinated manner between the Indonesian National Police (Polri), the National Counterterrorism Agency (BNPT), the National Cyber and Cyber Security Agency (BSSN), and the Indonesian Digital Technology Commission (Komdigi) to build an effective digital radicalization prevention system. However, this integration must be fostered through clear legal reforms regarding the legality of cyber surveillance, personal data protection, the limits of digital profiling authority, and control mechanisms for the state's use of surveillance technology. Thus, the development of smart policing in Indonesia is not only oriented towards the effectiveness of national security alone, but must also reflect the character of a Pancasila-based state that upholds democracy, legal certainty, protection of human rights, and accountability of power in the era of digital transformation.

The use of artificial intelligence, machine learning, sentiment analysis, digital profiling, facial recognition, and predictive analytics must not be based solely on ideological keywords, religious terminology, political criticism, negative sentiment, or expressions of unpopular beliefs. Lawful political, religious, academic, journalistic, and ideological expression must remain outside the category of actionable digital threat unless there are additional objective indicators connecting the activity to legally relevant conduct. A risk classification should therefore rely on a contextual and multi-factor assessment, including evidence of explicit advocacy or incitement to violence, recruitment for terrorist activity, operational preparation, credible threats, coordination with known violent networks, financing or facilitation of unlawful activity, or other conduct meeting legally defined risk indicators. No individual should be classified as a security threat solely because of belief, identity, religion, political preference, or association with a controversial opinion. AI-generated results should function only as preliminary analytical indicators. Any escalation into monitoring, investigation, or intrusive surveillance must be reviewed by a competent human authority and supported by independently verifiable information.

To prevent algorithmic bias, false positives, discriminatory profiling, and inaccurate risk classification, the smart-policing system should be subject to mandatory algorithmic governance. This includes pre-deployment testing, periodic independent auditing, documentation of data sources and analytical limitations, accuracy assessment, bias testing, and continuous monitoring of error rates. Where an automated system produces a risk classification, the affected person must not automatically be subjected to coercive legal consequences. High-risk classifications should require human review, while intrusive measures should require the additional legal safeguards applicable to the particular surveillance activity. Automated profiling must therefore never operate as an autonomous basis for arrest, prosecution, or punitive action. The legal framework should further require mechanisms for correcting inaccurate data, reviewing erroneous classifications, and providing remedies where individuals suffer material or legal consequences as a result of unlawful or substantially inaccurate surveillance. These safeguards are particularly important because preventive monitoring may occur before a criminal offense has taken place.

Reconstruction and Update of Smart Policing Laws to Prevent Digital Radicalization in Indonesia

Reconstruction of smart policing laws to prevent digital radicalization in Indonesia must begin with a systematic assessment of whether the existing legal framework can adequately regulate emerging forms of cyber surveillance and technology-assisted prevention. Law Number 1 of 2024 concerning Electronic Information and Transactions primarily regulates electronic systems and unlawful electronic conduct; Law Number 5 of 2018 concerning the Eradication of Criminal Acts of Terrorism focuses on terrorism prevention and prosecution; Law Number 2 of 2002 concerning the Indonesian National Police regulates general police authority; and Law Number 27 of 2022 concerning Personal Data Protection establishes general safeguards for personal-data processing. These regulations address important aspects of digital governance but do not yet establish a single legal architecture governing AI-assisted surveillance, predictive policing, digital profiling, inter-agency intelligence integration, automated risk assessment, and independent oversight of intrusive surveillance.

Therefore, the proposed National Cybersecurity and Smart Policing Law should not merely duplicate existing legislation. Its necessity lies in establishing cross-sectoral procedural standards that cannot be adequately addressed through fragmented sectoral regulation, particularly regarding the threshold for digital surveillance, human control over AI-generated risk classifications, judicial authorization for intrusive measures, data-sharing governance, algorithmic accountability, independent oversight, and remedies for unlawful surveillance.

Nevertheless, the legislative model should remain open to harmonization. If the legislature determines that these matters can be comprehensively incorporated through coordinated amendments to the Terrorism Law, Police Law, ITE Law, Personal Data Protection Law, and cybersecurity regulations, a separate statute would not be legally indispensable. The essential objective is the creation of an integrated and harmonized legal framework rather than institutional or legislative expansion for its own sake.

The second concrete action is the development of a National Cyber Intelligence Fusion Center as an inter-agency coordination mechanism rather than as a new institution that replaces the statutory authority of existing agencies. The Center may integrate relevant analytical capacities of the Indonesian National Police, BNPT, BSSN, PPATK, the Attorney General's Office, and the Ministry of Communication and Digital Affairs, while each institution retains its original statutory mandate.

Data sharing within the Center should be governed by the principles of legal authorization, purpose limitation, necessity, proportionality, data minimization, access classification, retention limitation, and auditability. Access should not be automatically available to every participating institution. Instead, information should be divided into levels based on sensitivity and operational necessity, with each access request recorded and capable of subsequent audit.

Data may only be shared for specifically defined purposes relating to national security, terrorism prevention, legally authorized investigations, or the assessment of

verified systemic threats. The legal framework should also establish maximum retention periods differentiated according to the nature and evidentiary relevance of the data, followed by mandatory deletion or anonymization when the legal purpose has expired. Unauthorized access, secondary use, unlawful disclosure, or use of data beyond the approved purpose must give rise to administrative, disciplinary, and, where applicable, criminal accountability.

The third concrete action is to strengthen cyber intelligence and digital surveillance capacity through institutional modernization and improving human resources for law enforcement in the cybersecurity sector. The threat of digital radicalization is evolving far faster than the authorities' ability to monitor cyber activity due to limitations in personnel, technology, and the state's digital analysis systems. Therefore, the state needs to establish a Smart Policing and Cyber Radicalism Prevention Directorate within the Indonesian National Police, specifically responsible for cyberspace surveillance based on artificial intelligence and cyber intelligence. This agency must possess digital forensics, dark web monitoring, cryptocurrency tracking, encrypted communication analysis, and social media intelligence capabilities to preventatively detect extremist propaganda activities. Furthermore, the government needs to establish educational centers and a national cyber intelligence certification to improve the competence of law enforcement officers in data science, machine learning, digital forensics, and cyber investigation. This capacity building is a concrete implementation of Article 30 paragraph (4) of the 1945 Constitution, which affirms that the Indonesian National Police (Polri), as a state instrument, is tasked with maintaining public security and order. In the modern context, maintaining national security is no longer solely carried out through physical patrols, but also through information technology-based cyber patrols capable of effectively and adaptively addressing the threat of cyber radicalization.

The fourth concrete action is the harmonization of authority between law enforcement and cybersecurity agencies through the establishment of a binding national coordination mechanism. Currently, cyberspace surveillance authority is spread across the Indonesian National Police (Polri), the National Counterterrorism Agency (BNPT), the National Cyber and Information Agency (BSSN), the Indonesian National Intelligence Agency (Komdigi), and state intelligence, which often results in overlapping authority and weak coordination in handling the threat of digital radicalism. Therefore, institutional regulatory reform is needed through revisions to the Police Law, the Electronic Information and Transactions Law, and cybersecurity regulations to clarify the boundaries of each agency's authority. The Indonesian National Police (Polri) should focus on law enforcement and cyber investigation, the National Counterterrorism Agency (BNPT) on prevention and deradicalization, the National Cyber Security Agency (BSSN) on national cyber infrastructure security, and the Digital Commission (Komdigi) on controlling electronic systems and blocking access to digital content containing radicalism. Furthermore, an integrated coordination system based on data interoperability needs to be established, so that each institution can exchange information quickly and accurately. This institutional harmonization is crucial for creating integrated cybersecurity governance capable of

collectively addressing cyberspace threats and avoiding fragmented operations. From a state administrative law perspective, this integration of authority will also strengthen legal certainty, strengthen the effectiveness of the national security bureaucracy, and prevent conflicts of authority between state institutions in digital surveillance practices.

The fifth concrete action is the development of an accountable digital surveillance system based on human rights protection through the establishment of an independent oversight mechanism for the state's use of surveillance technology. While the use of artificial intelligence, facial recognition, digital profiling, and predictive policing can increase the effectiveness of early detection of digital radicalization threats, they also have the potential to lead to mass surveillance, privacy violations, misuse of personal data, and digital criminalization. Therefore, any use of surveillance technology must adhere to the principles of proportionality, necessity, and accountability, as are standard in a democratic state governed by the rule of law. Concrete action that needs to be taken is the establishment of a Cyber Surveillance Oversight Commission as an independent institution tasked with overseeing the use of cyber surveillance by state officials, conducting audits of law enforcement artificial intelligence systems, and receiving public complaints regarding alleged misuse of digital surveillance. Furthermore, the state needs to require transparency reports and periodic reviews of the use of predictive policing and cyber surveillance systems so that the public knows the limits of state surveillance technology use. These mechanisms are crucial to ensure that the implementation of smart policing remains in line with Article 28G of the 1945 Constitution and Law Number 27 of 2022 concerning Personal Data Protection, which guarantees citizens' right to privacy and digital data protection.

The reconstruction and renewal of smart policing laws to prevent digital radicalization must be directed at developing a modern, adaptive, and democratic national cybersecurity system. Smart policing should not be understood merely as an expansion of state power in digital surveillance, but rather as a legal and technological instrument used proportionally to maintain national security without compromising citizens' constitutional rights. Therefore, legal reform must be implemented through regulatory harmonization, strengthening cyber intelligence, integrating national big data, establishing independent oversight mechanisms, and modernizing cybersecurity institutions based on the Pancasila principle of the rule of law. With this legal reformulation, Indonesia is expected to be able to build a smart policing system that is not only effective in detecting and preventing the spread of digital radicalism but also constitutionally legitimate, democratically accountable, and just in protecting human rights in the era of digital transformation. This reform also serves as a strategic step to strengthen national resilience and maintain national security stability from the increasingly complex threat of cyber radicalization in the future.

The proposed reconstruction should be translated into a structured regulatory model containing several core statutory provisions. First, the law should define digital radicalization, cyber radicalization, radical content, violent extremism, cyberterrorism, digital profiling, predictive policing, and intrusive cyber surveillance. The definitions must distinguish lawful ideological expression from conduct involving incitement, recruitment, preparation, facilitation, or credible threats of unlawful violence.Second, AI-assisted

surveillance and predictive policing should be legally characterized as decision-support mechanisms rather than autonomous systems of coercive state action. Any algorithmic risk classification must be subject to human review, accuracy testing, bias assessment, periodic audit, documentation, and procedures for correcting erroneous classifications. Third, the law should establish the National Cyber Intelligence Fusion Center as an inter-agency coordination mechanism with clearly defined data-sharing authority. Data exchange must be governed by purpose limitation, necessity, proportionality, access classification, retention periods, cybersecurity safeguards, audit trails, and institutional accountability.

Fourth, intrusive surveillance measures, including interception and monitoring of encrypted communications, should require prior judicial authorization based on specific and evidence-based grounds. The authorization must define the target, purpose, scope, duration, data category, and applicable renewal procedure. Emergency measures may only be used in narrowly defined circumstances and must be subject to prompt subsequent judicial review. Fifth, all cyber-surveillance measures must be assessed through a proportionality framework consisting of legality, legitimate aim, suitability, necessity, proportionality in the strict sense, and the use of the least-restrictive means. Lawful political, religious, academic, journalistic, and ideological expression may not constitute an independent basis for intrusive surveillance. Sixth, the Cyber Surveillance Oversight Commission should be granted institutional independence and authority to audit surveillance practices, examine classified operational records under appropriate safeguards, investigate complaints, review algorithmic systems, require corrective measures, recommend sanctions, and publish periodic transparency reports.

Finally, the legal framework should provide remedies for unlawful surveillance, including termination of surveillance, deletion or correction of unlawfully obtained data, exclusion or restriction of unlawfully obtained evidence where applicable, administrative and disciplinary sanctions, and compensation mechanisms where unlawful surveillance causes demonstrable harm. Through this model, the reconstruction would move beyond general institutional proposals toward an operational legal framework capable of balancing national security, technological effectiveness, constitutional rights, privacy, due process of law, and democratic accountability.

Conclusion

Based on the discussion, the development of digital transformation has given rise to a new form of threat in the form of digital radicalization or cyber radicalization, which develops through social media, encrypted communication, artificial intelligence, online forums, and various other digital platforms that are difficult to control through conventional law enforcement mechanisms. Digital radicalization is not only a matter of the spread of extremist ideology, but has developed into a real threat to national security, cyber resilience, social stability, and state ideology due to its close relationship with criminal acts of terrorism, cyber terrorism, digital propaganda, and lone wolf terrorism. In this context, the Indonesian legal system still faces various fundamental weaknesses in the form of regulatory disharmony between the ITE Law, the Terrorism Law, the Personal Data Protection Law, and other cybersecurity regulations, as well as weak integration of

authority between institutions such as the National Police, the BNPT, the BSSN, and Komdigi in conducting cyberspace surveillance. In addition, limited cyber intelligence, weak digital surveillance, minimal national big data integration, and the absence of a clear legal basis for cyber surveillance, predictive policing, or the use of artificial intelligence in law enforcement have caused the digital radicalization prevention system in Indonesia to not run effectively and adapt to developments in modern digital technology. Therefore, it is necessary to reconstruct and update smart policing laws that integrate big data analytics, cyber intelligence, predictive policing, artificial intelligence, and real-time surveillance into a modern national cybersecurity system while remaining compliant with the principles of the rule of law, due process of law, the proportionality principle, personal data protection, and human rights as guaranteed in the 1945 Constitution of the Republic of Indonesia.

Based on these conclusions, recommendations include the need to establish a National Cybersecurity and Smart Policing Law as a specific legal basis governing cybersurveillance, digital profiling, the use of artificial intelligence in law enforcement, national big data integration, and the limits of state authority in conducting digital surveillance of public activity in cyberspace. Furthermore, the government needs to immediately establish a National Cyber Intelligence Fusion Center that integrates the National Police (Polri), the National Counterterrorism Agency (BNPT), the National Cyber and Information Agency (BSSN), the Financial Transaction Reports and Analysis Center (PPATK), the Attorney General's Office (Kejasaan), and the Digital Digital Commission (Komdigi) into a single national cyber intelligence system based on real-time data analytics to accelerate early detection of the spread of radical propaganda and cyberterrorism threats. Strengthening the capacity of law enforcement officers through the establishment of the Smart Policing and Cyber Radicalism Prevention Directorate, modernizing digital forensics, cyber intelligence training, and developing national security-based artificial intelligence are also strategic steps that must be implemented immediately. Furthermore, to prevent abuse of power in the implementation of smart policing, the state needs to establish an independent oversight mechanism through the Cyber Surveillance Oversight Commission, tasked with auditing, supervising, and controlling the use of digital surveillance technology by state officials to ensure it remains in line with the principles of constitutional democracy and the protection of human rights. Therefore, smart policing legal reform in Indonesia is expected to create an effective, legitimate, accountable, and equitable cyber oversight system in addressing the threat of digital radicalization in the era of information technology transformation.

References

Aminudin, C. P. (2023). Media Sosial Dan Radikalisme: Bagaimana Teknologi Informasi Mempengaruhi Pemikiran Ekstrem. *Humaniorum*, 110–115.

Betawi, U. (2025). Kesenjangan Hukum Dalam Penanggulangan Terorisme Di Indonesia (Analisis Terhadap Ancaman Siber Dan Radikalisasi Online). *Istishlah (Jurnal Hukum Islam)*, 46–57.

Christy, G. P. (2020). Penanggulangan Cyber-Terrorism Melalui Website Radikal Dalam Perspektif Demokrasi Pancasila. *Paulus Law Journal*, 59–71.

Erwin, A. W. (2023). *Transformasi Digital*. Jambi: Sonpedia Publishing Indonesia.

Jaladriyanta, S. (2020). Polri Menuju Smart Police. *Jurnal Ilmu Kepolisian*.

Kusuma, F. K. (2021). Radikalisasi Sebagai Pola Politik Hukum Indonesia Di Era Society 5.0. *Journal Of Syntax Literate*.

Kusuma, N. S. (2021). Legal Sanctions For The Spread Of Radical Content On The Internet From The Perspective Of The Terrorism Law In Indonesia. *Decisio: Law Journal*, 25–29.

Makarawung, R. J. (2026). Keterlibatan Algoritma Di Atas Ikatan Autentik: Peran Media Sosial Yang Terus Berevolusi. *Jati (Jurnal Mahasiswa Teknik Informatika)*, 1819–1824.

Mandala, I. D. (2024). Transformasi Moderasi Beragama Berbasis Digital 2024: Sebagai Bentuk Upaya Memfilter Konten Radikalisme Dan Ekstremisme Di Era Disrupsi: Digital-Based Religious Moderation Transformation 2024: An Effort To Filter Radicalism And Extremism Content In The Ag. *Jurnal Bimas Islam*, 127–160.

Putra, D. A. (2026). Digital Literacy And Radicalism Potential: An Analysis Of Youth Digital Behavior In South Sumatra: Literasi Digital Dan Potensi Radikalisme: Analisis Perilaku Digital Generasi Muda Di Sumatera Selatan. *Jurnal Pemerintahan Dan Politik*, 592–602.

Santoso, J. E. (2025). Optimization Of Smart Policing And Democratic Policing Concepts As Polri's Efforts In Building Synergy With The Community To Realize Inclusive And Just Security Governance. *Jurnal Greenation Sosial Dan Politik*, 634–643.

Sepima, A. G. (2020). Penegakan Hukum Ujaran Kebencian Di Republik Indonesia. *Jurnal Retentum*.

Shabirin, A. (2025). Asas Legalitas Dalam Penanggulangan Radikalisme Online: Perspektif Hukum Pidana Indonesia. *Jejak Digital: Jurnal Ilmiah Multidisiplin*, 333–344.

Susanti, E. (2020). Sosialisasi Membangun Literasi Karakter Berbasis Pancasila Di Era Digital 4.0 Dalam Upaya Pencegahan Radikalisme Dan Terorisme Pada Remaja. *Jurnal Sumbangsih*, 9–18.

Usrinase, Y. I. (2025). Implementasi Asas Legalitas Dalam Penegakan Hukum Terhadap Tindak Pidana Radikalisme Digital Yang Berimplikasi Pada Terorisme. *Perahu (Penerangan Hukum): Jurnal Ilmu Hukum*, 140–150.

Wibowo, K. T. (2023). Penanggulangan Penyebaran Radikalisme Melalui Media Sosial Dalam Hukum Pidana Indonesia. *Jurnal Hukum Lex Generalis*, 187–212.

Widagdo, H. H. (2017). Kekerasan Dalam Dunia Digital (Pembacaan Terhadap Perubahan Gaya Radikal Di Era Digital). *Fikri: Jurnal Kajian Agama, Sosial Dan Budaya*, 425–456.

Wijaya, P., & Gusliana, H. B. (2024). Relevansi Hak Privasi Dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Dengan Pasal 28 G Ayat 1 Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. *Jurnal Ilmiah Wahana Pendidikan*.