

Lex Certa and Criminalization Expansion in Article 12B of Law No. 5 of 2018

Mukhlissuddin¹, Ayub Torry Satriyo Kusumo²

*Master of Law, Faculty of Law, Universitas Sebelas Maret
Kentingan Jl. Ir. Sutami No.36, Jebres, Kec. Jebres, Kota Surakarta, Jawa Tengah 57126
Email : mukhlisprobono@gmail.com*

*Master of Law, Faculty of Law, Universitas Sebelas Maret
Kentingan Jl. Ir. Sutami No.36, Jebres, Kec. Jebres, Kota Surakarta, Jawa Tengah 57126
Email : ayub.kusumo@staff.uns.ac.id*

Submitted : 28/10/2025 Reviewed: 20/02/2026 Accepted: 05/03/2026

Abstract: *This study analyzes the expansion of criminalization in Article 12B of Law Number 5 of 2018, particularly the inclusion of information and communication technology-based training as a criminal offense. The central legal problem addressed in this research concerns the ambiguity of normative boundaries in defining “training” within the digital context, which potentially undermines legal certainty and opens room for arbitrary law enforcement. The process of digitalization complicates the enforcement of Article 12B, as online activities related to knowledge sharing, expression, and association increasingly overlap with constitutionally protected civil liberties. Employing a normative juridical research method, this study examines statutory provisions, constitutional principles, and relevant human rights doctrines to assess the compatibility of Article 12B with the 1945 Constitution of the Republic of Indonesia. The analysis focuses on the principle of lex certa as an essential element of criminal law and its function in safeguarding freedom of expression and freedom of association in the digital era. The findings indicate that the expanded formulation of Article 12B lacks sufficient normative clarity, thereby creating tension between state security objectives and constitutional guarantees of human rights. This study concludes that, without strict interpretative limitations, Article 12B risks constitutional inconsistency, particularly with Articles 28E and 28G of the 1945 Constitution. Therefore, normative refinement and constitutional-oriented interpretation are necessary to ensure that counter-terrorism policies remain proportionate, legally certain, and aligned with human rights standards in the digital era.*

Keywords: *Criminalization; Terroism Law; Information Technology; Human Rights*

DOI: [10.32801/lamlaj.v11i1.271](https://doi.org/10.32801/lamlaj.v11i1.271)

INTRODUCTION

The threat of terrorism today is increasingly complex and multifaceted. It encompasses not only visible physical violence but also more subtle but potentially impactful digital and technological avenues. Advances in information and communication technology have opened up new avenues for the spread of radical ideologies, recruitment processes, funding, and even online training. This situation requires the state to strengthen its legal framework to address the challenges of the digital era while still respecting the principles of human rights and civil liberties, the foundation of the rule of law.

In the Indonesian context, the state's response to these dynamics is reflected in amendments to Law Number 5 of 2018 concerning the Eradication of Criminal Acts of Terrorism ("Law 5/2018"). One significant change is Article 12B, which broadens the definition of prohibited "training activities" beyond physical or militaristic training to include aspects of information and communication technology and other forms of non-conventional training. Thus, the norm for criminalizing terrorism has broadened the scope of punishable activities. Normatively, this amendment signifies an expansion of criminalization that substantially alters the scope and function of criminal law in counter-terrorism policy.

The Constitutional Court of the Republic of Indonesia also considered the legal standing in Decision Number 73/PUU-XVI/2018 regarding the definition of terrorism, which is relevant to the debate on the interpretation of norms in Article 12B of Law 5/2018.¹ This ruling is a constitutional review of Law No. 5 of 2018 (an amendment

to the Law on the Eradication of Criminal Acts of Terrorism). The Court rejected the applicant's petition challenging the definition of terrorism in Article 1 number 2 of Law No. 5/2018 against the provisions of the 1945 Constitution due to legal standing. However, this ruling reflects the Constitutional Court's interaction with terrorism norms and constitutional rights, including the aspect of legal certainty.

On the one hand, this broadening of meaning demonstrates the state's commitment to adapting regulations to current developments and new forms of threats, including digital ones. However, on the other hand, it also raises a number of pressing legal issues that require further examination. Such expansion raises concerns of over-criminalization, particularly when criminal norms lack precise boundaries, thereby undermining the principle of legal certainty (*lex certa*). For example, overly broad or ambiguous regulations can lead to the phenomenon of over-criminalization, a situation where criminal norms are excessively applied to activities not originally designed for terrorism. The unclear boundaries between illegal training activities and legitimate activities such as research, technology discussions, or civic capacity building open up wide scope for interpretation for law enforcement officials and potentially lead to violations of the rights to freedom of expression, freedom of association, and fair legal protection.

From the perspective of criminal law theory, this development reflects a fundamental shift from repressive justice toward pre-emptive justice. In conventional criminal law doctrine, punishment is generally

¹ Mahkamah Konstitusi Republik Indonesia, *Putusan Nomor 73/PUU-XVI/2018 tentang Pengujian Undang-Undang Nomor 5 Tahun 2018 terhadap Undang-*

Undang Dasar Negara Republik Indonesia Tahun 1945 (Jakarta, 2018).

imposed after the occurrence of a completed offense or a materially harmful act. Preparatory acts (*voorbereidingshandeling*) are, as a rule, not subject to criminal liability unless explicitly determined by law, as they are considered insufficiently dangerous to justify penal intervention. However, Law No. 5 of 2018 represents a deliberate departure from this principle by criminalizing preparatory conduct at an early stage, even when the potential harm remains abstract or has not yet materialized.

Literature reviews show that in the digital era, radicalization and acts of terrorism often utilize cyberspace. For example, according to Astuti (2024) in her study "Literacy on the Benefits of Technology for Cyber Terrorism in the Era of Disruption with AI (Artificial Intelligence)," digital advancements enable terrorists to recruit, train, and coordinate without direct face-to-face interaction, across national borders and even sovereignty, with significant psychological and structural impacts.² Similarly, Syamsurrijal et al. (2024) emphasized that social media and online platforms have become the main tools in the process of radicalization and deradicalization of society.³ However, these studies largely approach terrorism from sociological and policy perspectives, rather than addressing the normative uncertainty of criminal provisions governing digital-based preparatory acts.

Despite the growing body of literature on digital terrorism and cyber radicalization, most existing studies focus on patterns of online extremism, law enforcement strategies, or technological risks. Relatively few legal

studies examine the doctrinal implications of expanding preparatory criminalization in the digital sphere, particularly concerning the clarity and limits of criminal norms. As a result, the problem of normative uncertainty in defining technology-based "training activities" under Article 12B remains underexplored. This article differs from previous studies by critically analyzing Article 12B from a normative and constitutional perspective, focusing on the principle of *lex certa* and its function in safeguarding civil liberties. By examining the expansion of criminalization within the framework of pre-emptive justice, this study addresses the legal tension between state security objectives and constitutional guarantees of freedom of expression and freedom of association in the digital era.

These studies reinforce the argument that the challenges of terrorism regulation in the digital era are no longer limited to "military training" or "bombs," but also include training activities and the use of technology that can be exploited for terrorist purposes. Within a normative legal framework, the amendment to Article 12B of Law 5/2018 carries serious implications: first, from the perspective of legal norm analysis, which changes the scope of criminal law; second, from the perspective of implementation or application in the field (legal practice), which requires law enforcement officials and institutions to interpret the scope of the new "training." If it is not formulated clearly and implemented proportionally, it will not only impact national security but also fundamental citizen rights

² Astuti, Sri Ayu. "Literasi Kemanfaatan Teknologi terhadap Cyber Terrorism di Era Disrupsi dengan AI (Artificial Intelligence)." *Indonesian Journal of Criminal Law & Criminology* 5, no. 3 (2024): 1–12. <https://doi.org/10.18196/ijclc.v5i3.24225>.

³ Syamsurrijal, M., A. Nurmandi, H. Jubba, M. Hidayati, & B. Hariyanto. "De-radicalization through Social Media: Social Media Literacy in Countering Terrorism in Indonesia." *Wawasan: Jurnal Ilmiah Agama dan Sosial Budaya* 9, no. 1 (2024): 1–12. <https://doi.org/10.15575/jw.v9i1.16788>.

such as freedom of expression and association.

In the context of an ideal state based on the rule of law, enforcement of criminal law against terrorism must continue to be carried out with due regard to principles such as legality, legal certainty, proportionality, and fairness. However, the digital phenomenon and information and communication technology-based training demand new interpretations of norms. As a critical note, "criminal law politics" plays a strategic role in shaping the criminalization of terrorism policy in Indonesia, namely how criminal norms are not only a response to threats but also a regulatory instrument that must align with fundamental human rights values.⁴

Based on this framework, this research is important because, despite changes and expanded regulatory scope, few studies have systematically examined the legal and normative implications of "technology and communication training" in the context of the criminalization of terrorism in Indonesia, particularly regarding the balance between national security and human rights protection. This research seeks to fill this gap.

This study is highly relevant considering that the digital and cybersecurity regulatory framework in Indonesia is not yet fully aligned with international human rights protection standards. As noted by Situmeang et al., Indonesia's legal framework leaves significant room for potential human rights abuse due to normative loopholes. In the context of Article 12B, such loopholes are

evident in the absence of a clear distinction between lawful digital activities and punishable technology-based training. This normative uncertainty amplifies the risk of arbitrary enforcement, particularly when criminal provisions function as formal offenses without clearly defined elements."⁵

Furthermore, according to Rovida and Sasmini (2023), In the context of Article 12B of Law No. 5 of 2018, the protection of human rights, particularly freedom of expression and freedom of association, cannot be separated from the clarity of criminal norms governing technology-based activities. The expansion of criminalization toward information and communication technology, based training tends to operate as a formal offense (*delik formil*), where criminal liability arises from the act itself without requiring proof of concrete harm. When such offenses are formulated without clear normative boundaries, they risk violating the principle of legality, especially the requirement of *lex certa*, as individuals are unable to reasonably foresee which digital activities may constitute a criminal offense.⁶ Rovida and Sasmini emphasize that advancements in information and communication technology pose serious challenges to freedom of expression and digital privacy. From a criminal law perspective, these challenges become more acute when the expansion of criminalization is not accompanied by precise normative limits. Without a clear classification of whether Article 12B constitutes a material offense (*delik materiil*) requiring demonstrable harm,

⁴ Patria, Widya Nusa, Md. Shodiq, & Supot Rattanapun. "The Political Role of Criminal Law in Shaping Counter-Terrorism Policy in Indonesia." *PENA LAW: International Journal of Law* 3, no. 1 (2025): 1–23. <https://doi.org/10.56107/penalaw.v3i1.222>.

⁵ Situmeang, Ampuan; Ninne Zahara Silviani; Satria Unggul Wicaksana Prakasa; David Tan; Emiliya Febriyani. 2024. "Balancing Human Rights and

Cybersecurity: Analyzing Indonesia's Legal Framework." *Jurnal Hukum Novelty* 15, no. 2: 200–214. <https://doi.org/10.26555/jhn.v15i2.28738>.

⁶ Rovida, Khofidhotur, and Sasmini. 2023. "Digital Human Rights Protection: Legal Transplantation Strategies to Realize Sustainable Development in Indonesia's Digitalization Era." *Domus Legalis Cogitatio* 1, no. 2: 35–50. <https://doi.org/10.24002/dlc.v1i2.9926>.

or a formal offense, the enforcement of anti-terrorism law risks disproportionately restricting constitutionally protected digital activities. In this context, policymakers are required to not only broaden the definition of criminalization but also ensure effective oversight and protection mechanisms for human rights. Therefore, the protection of human rights in the digital era is inseparable from the fulfillment of the *lex certa* requirement, particularly in criminal provisions that target preparatory conduct through technology based activities.

Therefore, this study aims to analyze the expansion of criminalization under Article 12B of Law No. 5 of 2018, particularly concerning the regulation of technology-based training in the context of counter-terrorism policy. This research focuses on examining the normative implications of such expansion on legal certainty and its impact on the protection of freedom of expression and freedom of association in the digital era. The results of this study are expected to provide policy input that is responsive to technological dynamics and human rights values, so that the implementation of anti-terrorism norms remains effective without neglecting citizen protection.

This condition reveals a fundamental digital paradox, while the state seeks to strengthen national security through the expansion of preventive criminalization, Article 12B simultaneously generates legal uncertainty that may discourage academics and information technology professionals from conducting legitimate cybersecurity research. Based on the foregoing discussion, this research addresses the following legal issues. What are the legal implications of the expansion of criminalization under Article

12B of Law No. 5 of 2018 in regulating technology-based training for the prevention of terrorism in Indonesia? How does the expansion of criminalization affect the protection of freedom of expression and freedom of association in the digital era from the perspective of legal certainty and constitutional principles?

METHOD

Juridical research method as the primary approach in analyzing the expansion of the meaning of criminalization in the amendment to Article 12B of Law Number 5 of 2018 concerning Terrorism. This method aims to examine applicable legal norms through a literature review and relevant legislation. The data used consists of primary legal materials such as laws and government regulations, as well as secondary legal materials such as legal literature, journals, and related legal doctrines. In this way, the research focuses on a normative and systematic analysis of concepts, rules, and legal applications. According to Soerjono Soekanto (2006), the normative juridical method is highly appropriate for studying law in a normative sense, namely as a system of norms that is autonomous and independent of its sociological aspects..⁷

A normative legal approach allows research to assess the synchronization of formal law while exploring its legal implications in the context of human rights protection and the development of information technology. This study strengthens the legal theoretical framework and emphasizes critical analysis of existing legal regulations to provide more responsive and equitable policy recommendations.

⁷ Soekanto, S. 2006. *Pengantar Penelitian Hukum*. Jakarta: UI Press, 51.

ANYLISIS AND DISCUSSION

Legal Implications of the Expansion of the Criminalization of Article 12B of Law No. 5/2018 Regarding Restrictions on the Use of Information Technology

The amendment to Article 12B of Law No. 5 of 2018 marks a paradigm shift in Indonesian criminal law policy regarding terrorism. This norm expands the scope of terrorism training beyond physical or militaristic training to include training using or related to information and communication technology (ICT). This expansion is normatively intended to address the new phenomenon of digital terrorism developing through social media, the dark web, and online forums. However, from a legal perspective, this raises serious implications for the clear legal boundaries between criminal and legitimate activities in the digital realm.

From the perspective of criminal law theory, the formulation of Article 12B raises serious concerns regarding the principle of legality (*nullum crimen sine lege*), particularly the requirement of *lex certa*. Criminal norms must be formulated with sufficient precision so that individuals are able to foresee the legal consequences of their actions. Douglas Husak argues that vague criminal prohibitions tend to expand the scope of punishment beyond socially harmful conduct and often result in overcriminalization.⁸ In a similar vein, Barda Nawawi Arief emphasizes that criminal law should function as a last resort (*ultimum remedium*) and must be limited to conduct that is clearly blameworthy and socially dangerous.⁹ The use of open ended phrases such as “other training” and “that can be used”

in Article 12B lacks clear technical and intentional boundaries, thereby failing to meet the requirement of legal certainty and opening space for excessive interpretation by law enforcement authorities.

National data from the National Counterterrorism Agency (BNPT) shows that between 2018 and October 2024, 1,703 terrorism suspects were arrested and 43,204 pieces of documented cyber extremist content were discovered, indicating that the digital realm is becoming a crucial arena in anti-terrorism strategies. Furthermore, law enforcement officials at the regional level are increasingly active in handling cases of the spread of violent ideology through online platforms. One example is the arrest of a suspect in Purworejo on May 26, 2025, for spreading propaganda via social media..¹⁰

In practice, the formulation of Article 12B paragraphs (1) and (2) of Law 5/2018 can open up wide interpretation for law enforcement officials. Terms such as providing training or receiving training that can be used to commit terrorist acts can potentially be interpreted subjectively, especially when associated with online activities that are difficult to distinguish between technology training, academic research, or general education.

Similarly, Ramadhan (2024) explains that terrorism-related cybercrimes now often take the form of cyber-proselytizing or digital preaching, which does not always have a criminal purpose, but is vulnerable to being categorized as “terrorist training” if legal norms lack clear boundaries. He writes, “the growing overlap between digital

⁸ Douglas Husak, *Overcriminalization: The Limits of the Criminal Law* (Oxford: Oxford University Press, 2008), 55–58.

⁹ Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana* (Jakarta: Kencana, 2010), 43–45.

¹⁰ Norbertus Arya Dwiangga Martiar. “Sebarkan Paham Kekerasan Melalui Internet, Terduga Teroris di Purworejo Ditangkap”. <https://www.kompas.id/artikel/sebar-paham-kekerasan-melalui-internet-terduga-teroris-di-purworejo-ditangkap> . diakses 30 Oktober 2025.

proselytizing, ideological coordination, and cyberterrorism demands precise legal criteria to avoid over-criminalization." This statement suggests that without clear boundaries, Article 12B could become a tool for excessive restrictions on freedom of opinion and expression in the digital space.

A legal study by Situmeang et al. (2024) highlights similar weaknesses in national laws governing the digital world: "the existing legal framework in Indonesia still leaves room for potential human rights abuses due to normative loopholes and underestimation of digital threats." The ambiguity of legal norms can increase the possibility of over-criminalization, especially in the context of increasingly complex technology use.

Within the framework of the rule of law, the existence of broad norms without explicit limitations contradicts the principle of *lex certa* (legal certainty). Criminal norms, according to Marzuki, should be "formulated clearly and without openness to multiple interpretations, so that citizens understand precisely what actions are prohibited by criminal law."¹¹ When the definition of training is expanded to include digital activities without clear parameters, the potential for violations of citizens' rights in using technology becomes inevitable.

This concern regarding legal certainty has also been expressly addressed by the Constitutional Court of the Republic of Indonesia. In its Decision Number 103/PUU-XXI/2023, the Court emphasized that criminal provisions related to terrorism must be formulated with clear and measurable parameters to avoid arbitrary interpretation by law enforcement authorities. The Court warned that vague formulations concerning

preparatory or preventive acts, if not accompanied by strict limitations, risk violating the principle of legality and undermining constitutional guarantees of legal certainty.¹² According to the Court, the state's authority to combat terrorism cannot justify the use of elastic criminal norms that blur the boundary between lawful conduct and criminal behavior, particularly in the context of ideological expression and activities conducted in digital spaces.

A closer examination of Article 12B reveals that the phrases "pelatihan lain" (other forms of training) and "yang dapat digunakan" (that can be used) constitute the core source of normative uncertainty. From a grammatical and systematic interpretation, these phrases lack technical or functional limitations that define what specific forms of digital expertise qualify as terrorist training. The term "pelatihan lain" operates as an open-ended category, while the phrase "yang dapat digunakan" introduces a speculative standard based on potential usability rather than actual intent or concrete harm. As a result, the provision allows criminal liability to be constructed on hypothetical assumptions rather than objectively verifiable conduct.

In the context of digital activities, this formulation raises a critical question: whether learning coding, encryption techniques, cybersecurity skills, or data protection methods may fall within the scope of "training that can be used" for terrorism. Normatively, such activities are value-neutral and widely utilized for legitimate purposes, including education, research, and national cybersecurity development. However, due to the absence of clear technical criteria or limiting elements in Article 12B, these forms

¹¹ Marzuki, Peter Mahmud. *Penelitian Hukum*. Edisi Revisi. Jakarta: Kencana, 2022, 89–90.

¹² Constitutional Court of the Republic of Indonesia. Decision Number 103/PUU-XXI/2023 concerning the

Judicial Review of Law Number 5 of 2018 against the 1945 Constitution of the Republic of Indonesia. Jakarta, 2024.

of digital training may be subject to expansive interpretation by law enforcement authorities. This condition confirms the elastic nature of the provision, rendering it a *pasal karet* that enables discretionary and potentially arbitrary criminalization.

From the standpoint of criminal law doctrine, such elasticity violates the principle of *nullum delictum sine lege stricta*, which requires criminal norms to be formulated with strict clarity and precision. Criminal liability must be based on clearly defined acts, not on abstract possibilities or speculative future misuse. By criminalizing training activities merely because they “can be used” for terrorism, Article 12B departs from strict legality and shifts the burden of interpretation to law enforcement discretion. This condition undermines legal certainty and contradicts the fundamental function of criminal law as *ultima ratio*, particularly in regulating preparatory conduct in the digital sphere.

Furthermore, the formulation of Article 12B suggests a tendency toward a formal offense (*delik formil*), where the act of training itself is punishable regardless of whether it results in concrete harm or directly facilitates a terrorist act. Without a clear requirement of causality or operational linkage, the provision lacks the characteristics of a material offense (*delik materiil*). This doctrinal ambiguity further exacerbates the risk of over-criminalization, especially when applied to digital activities that inherently involve abstract knowledge and transferable skills.

Several studies have shown a sharp increase in cyber threats related to

technology-based training and radical digital activities. For example, research by "Reconstruction of Criminal Law to Address Cyber Terrorism in Indonesia" (Marsudianto & Bakir 2024) found that attacks or activities classified as "cyber terrorism" in Indonesia increased by 300% in the last year analyzed..¹³ This study confirms that while regulations such as the Electronic Information and Transactions Law and the Terrorism Law exist, significant normative gaps remain that do not yet address online training, technology training, or cross-border digital activities. This reinforces the need for expanded legal norms, such as those in Article 12B, to encompass forms of training that utilize ICT and online spaces as a means of terrorism.

Furthermore, research in Indonesia's Digital Security Strategy: Countering the Threats of Cybercrime and Cyberterrorism (Khoirunnisa & Jubaidi 2024) shows that the Indonesian government has noted that “threats of cybercrime and cyberterrorism ... in both physical and digital forms ... have increased alarmingly.”.¹⁴ While not explicitly identifying "online training" figures, these findings demonstrate a growing trend of digital activities potentially linked to terrorism training and coordination. Therefore, legal norms that only regulate physical training may be too late to address this phenomenon.

In terms of legal norms controlling digital activities, it is important to emphasize that technology-based training can take place without face-to-face interaction, for example through webinars, online modules, closed forums, or encrypted group chats. If norms

¹³ Marsudianto, Dwi Nugroho, dan Herman Bakir. 2024. "Reconstruction of Criminal Law to Address Cyber Terrorism in Indonesia." *Journal of Social Science (JoSS)* 3, no. 11: 765–771. <https://doi.org/10.57185/joss.v3i11.382>.

¹⁴ Khoirunnisa, K., & Didi Jubaidi. 2024. "Indonesia's Digital Security Strategy: Countering the Threats of Cybercrime and Cyberterrorism." *Politeia : Journal of Public Administration and Political Science and International Relations* 2, no. 2: 62-82. <https://doi.org/10.61978/politeia.v2i2.211>.

such as Article 12B of Law 5/2018 criminalize "training that uses or is related to ICT... that can be used to commit acts of terrorism," then the interpretation of what "can be used" by law enforcement officials and prosecutors becomes crucial. Without clear parameters, such as the duration of the training, its purpose, or its correlation with acts of terrorism, there is the potential for excessive control of legitimate digital activities.

In practice, when authorities use broad norms without limited interpretation, it is highly likely that technological research, online courses, or technology training for civilians could be implicated, even if their intentions are not terrorist. In other words, controlling digital activity through criminal norms must be balanced with legal certainty mechanisms (*lex certa*) and clear boundaries. Legally, norms such as Article 12B must be interpreted restrictively, emphasizing that only training proven to have a purpose, *modus operandi*, or direct operational correlation with terrorist acts can be categorized as terrorism training. Control of digital activities through this norm should not be used as a means of generically restricting legitimate and productive digital technology or communication training.

Article 12B of the Terrorism Law emphasizes that the expansion of the criminalization of digital activities must be accompanied by a thorough understanding of ethics and technological literacy. While this article is designed to counter the potential for online activities to lead to acts of terrorism, its broad scope risks overinterpreting legitimate activities such as research, technology training, and community discussions. By fostering healthy legal awareness and widespread digital literacy, the public can

better understand the legitimate boundaries of online interactions, so that not every technological innovation or experiment is perceived as a threat. This strategy also serves as a reminder that criminal law should not be the sole instrument of control; rather, the law should serve to reinforce ethical values and social norms that have been instilled through education and literacy.¹⁵ This approach allows law enforcement to focus on interventions that truly pose a risk, while citizens remain safe to innovate and create in the digital space.

In other words, the integration of digital literacy and ethics in the implementation of Article 12B not only strengthens the effectiveness of counter-terrorism but also safeguards the principles of democracy and human rights. Productive online activities, such as application development, cybersecurity research, and technology community discussions, remain protected as long as there is no concrete evidence of a link to terrorism. This approach emphasizes that national security and citizen freedom are not incompatible; they can be harmonious if the law is enforced with proportionality and accountability, while prioritizing digital education as the foundation of a society resilient to online radicalization.

Therefore, a restrictive (narrow) interpretation of Article 12B is legally necessary, ensuring that its application is limited to activities proven to be directly related to the planning or implementation of terrorist acts. This clear boundary is crucial to prevent any overlap with citizens' rights to education, research, and digital expression.

Impact of the Expansion of Criminalization on Human Rights Protection in the Digital Era

¹⁵ Floridi, Luciano. *The Ethics of Information*. Oxford: Oxford University Press, 2013.

<https://doi.org/10.1093/acprof:oso/9780199641321.001.0001>.

This study addresses a fundamental legal problem arising from the expansion of criminalization under Article 12B of Law No. 5 of 2018, particularly through the use of the phrases “*pelatihan lain*” (other forms of training) and “*yang dapat digunakan*” (that can be used) in relation to terrorism. The inclusion of technology-based or information and communication technology (ICT)-related training within the scope of terrorism offenses represents a significant shift in Indonesian criminal law policy. While this expansion is normatively intended to respond to the evolving phenomenon of digital terrorism, it simultaneously raises serious concerns regarding compliance with the principle of legality (*nullum delictum sine lege stricta*), especially the requirement of *lex certa* and legal foreseeability.

At the national level, the Constitutional Court of Indonesia has consistently emphasized the importance of legal certainty in preventive criminal legislation. In Decision No. 103/PUU-XXI/2023, the Court held that criminal norms addressing radicalism and terrorism must be formulated clearly and narrowly to prevent arbitrary enforcement and violations of constitutional rights.¹⁶ The Court stressed that vague and elastic formulations undermine the principle of foreseeability and risk transforming preventive measures into repressive instruments. This constitutional reasoning is directly applicable to Article 12B of Law No. 5 of 2018, which similarly employs broad terminology without sufficient safeguards to distinguish between terrorist intent and legitimate digital activities.

This situation illustrates a digital paradox inherent in contemporary counterterrorism law. On the one hand, the state asserts a legitimate interest in

safeguarding national security against technologically mediated terrorist threats. On the other hand, the vague formulation of Article 12B produces a chilling effect that disproportionately affects academics, cybersecurity researchers, and information technology practitioners engaged in lawful security research. In the absence of clear intent-based and technical criteria, activities aimed at strengthening digital resilience may be perceived as legally risky, thereby discouraging innovation, research, and open academic inquiry in the field of cybersecurity.

From the perspective of criminal law doctrine, Article 12B lacks precise technical and normative boundaries regarding what forms of digital expertise or technological knowledge may qualify as “terrorism training.” The formulation does not distinguish clearly between prohibited conduct and legitimate activities such as coding education, cybersecurity research, encryption studies, academic webinars, or ideological discussions conducted online. The phrase “*yang dapat digunakan*” is particularly problematic, as it criminalizes conduct based on potential utility rather than demonstrable intent or direct operational linkage to terrorist acts. Such a construction allows for excessively broad interpretation by law enforcement authorities and risks transforming Article 12B into a *pasal karet*, contrary to the strict legality requirement that criminal norms must be formulated narrowly and predictably.

This normative ambiguity becomes increasingly problematic in the digital context, where freedom of expression and freedom of association are predominantly exercised through online platforms. In constitutional terms, this situation raises

¹⁶ Constitutional Court of the Republic of Indonesia, Decision No. 103/PUU-XXI/2023, 112–114.

serious concerns regarding the protection of fundamental rights guaranteed under Articles 28E and 28F of the 1945 Constitution, which safeguard freedom of expression, association, and access to information.¹⁷ When criminal liability may arise from participation in online training or digital knowledge exchange without clear intent-based criteria, individuals are placed in a position of legal uncertainty, unable to foresee whether their lawful activities might later be classified as terrorism-related conduct.

Having established that Article 12B fails to satisfy the requirements of *lex certa* and foreseeability, it is necessary to assess this provision through the framework of digital rights theory. Digital rights scholarship emphasizes that state restrictions in cyberspace must meet the standards of legality, proportionality, and necessity. Rachovitsa (2016) and Yüksel (2022) underline that online expression and digital autonomy occupy a central position in contemporary human rights discourse and cannot be restricted solely on the basis of abstract security risks.¹⁸ Applied to Article 12B, this perspective highlights the danger that broad criminalization of technology-based training may lead to disproportionate interference with lawful online activities that are educational, political, or ideological in nature.

The absence of clear intent-based and operational criteria in Article 12B also generates a tangible *chilling effect* in the

digital sphere. When individuals are unable to distinguish between lawful technological learning and potentially criminalized conduct, they may refrain from participating in online discussions, training programs, or collaborative research out of fear of criminal liability. This self-censorship undermines not only freedom of expression and association but also the broader development of digital innovation and civic participation. In this sense, Article 12B risks shifting from a preventive counterterrorism instrument into a repressive mechanism that discourages legitimate engagement in digital spaces.

From a human rights perspective, vague criminal norms in the digital domain generate what is commonly referred to as a chilling effect, where individuals refrain from lawful expression or association due to fear of criminal liability. Brunner argues that digital surveillance and preventive criminalization must comply with the principles of necessity and proportionality to avoid suppressing legitimate online activities.¹⁹ Yüksel further emphasizes that the internet places personal autonomy and freedom of expression at the core of contemporary human rights discourse, requiring states to exercise heightened caution when regulating digital conduct.²⁰ In the absence of foreseeable legal standards, Article 12B risks discouraging academics, IT professionals, and researchers from engaging in cybersecurity research, thereby undermining both digital innovation and

¹⁷ *The 1945 Constitution of the Republic of Indonesia*, arts. 28E, 28F.

¹⁸ Rachovitsa, Adamantia. 2016. "Engineering and lawyering privacy by design: understanding online privacy both as a technical and an international human rights issue." *International Journal of Law & Information Technology* 24, no. 4: 374-399. <https://doi.org/10.1093/ijlit/eaw012>. , Yüksel, Saadet. 2022. "New Technologies through a Human Rights Lens: Reflecting on Personal Autonomy and

Non-Discrimination." *Journal of Penal Law and Criminology* 10, no. 2: 281-305. <https://doi.org/10.26650/JPLC2022-1213410>.

¹⁹ Franziska Brunner, "Human Rights and Cybersecurity Due Diligence," *Human Rights Law Review* 18, no. 4 (2018): 791-793.

²⁰ Sezgin Yüksel, "Digital Rights and Freedom of Expression in the Internet Age," *Computer Law & Security Review* 45 (2022): 6-7.

democratic participation in the online public sphere.

Therefore, a restrictive and narrow interpretation of Article 12B is legally imperative. The provision should be applied only to technology-based training that is proven to possess a clear terrorist intent and a direct operational connection to the planning or execution of terrorist acts. Without such limitations, Article 12B fails to comply with the principle of *nullum delictum sine lege stricta* and undermines constitutional guarantees of freedom in the digital era. Human rights protection thus serves as a critical benchmark for evaluating the legitimacy of expanded criminalization under Article 12B, ensuring that efforts to combat terrorism do not erode the foundational principles of legal certainty, democracy, and constitutionalism.

In the context of digital technology, the distinction between legitimate cybersecurity research and prohibited terrorism training is often technically blurred. Dorothy E. Denning explains that many cybersecurity practices such as penetration testing, encryption analysis, and malware reverse engineering are inherently dual-use in nature, meaning that they can serve both defensive and malicious purposes depending on intent.²¹ Without clear intent-based and operational criteria, criminalizing technology-based training risks encompassing lawful academic research and professional cybersecurity education. Conway similarly warns that counterterrorism regulations in the digital sphere frequently suffer from conceptual ambiguity, which may lead to the misclassification of preventive or defensive cyber activities as terrorist conduct.²² Therefore, the absence of precise

normative limits in Article 12B increases the risk that legitimate digital skills development is mistakenly subsumed under the scope of terrorism related offenses.

Thus, the protection of human rights in the application of Article 12B serves as a test of the state's commitment to democratic values and constitutionalism. The state must ensure that efforts to eradicate terrorism are not used as a justification for restricting constitutionally guaranteed civil rights. This study still has limitations in terms of empirical analysis; further research could utilize a qualitative approach to law enforcement officials' understanding of digital norms.

CONCLUSION

The expansion of criminalization embodied in Article 12B of Law Number 5 of 2018 reflects Indonesia's effort to respond to the evolving nature of terrorism in the digital era, particularly the shift from physical training to technology-based and online forms of radicalization. This study demonstrates that the expansion of Article 12B embodies a digital paradox, where preventive security measures intended to protect the state may simultaneously undermine the development of cybersecurity research and technological expertise essential for national resilience. Normatively, this expansion is intended to close regulatory gaps in addressing digital terrorism training. However, this study demonstrates that the formulation of Article 12B, especially the use of vague phrases such as "other forms of training" and "that can be used", creates significant legal uncertainty and fails to fully comply with the principle of legality, particularly the requirements of *lex certa* and foreseeability in criminal law.

²¹ Dorothy E. Denning, "Cyberterrorism," *Testimony before the Special Oversight Panel on Terrorism*, US House of Representatives. (2000), 6–8.

²² Maura Conway, "Determining the Role of the Internet in Violent Extremism and Terrorism," *Studies in Conflict & Terrorism* 40, no. 1 (2017): 79–80.

The findings of this research confirm that the absence of clear legal parameters regarding intent, technical scope, and direct operational linkage to terrorist acts risks transforming preventive counterterrorism norms into overly broad instruments of control. In the digital context, such ambiguity may result in the criminalization of legitimate activities, including academic research, technology-based education, and lawful online discourse. Consequently, the application of Article 12B without restrictive interpretation has the potential to generate a chilling effect on freedom of expression and freedom of association, which are constitutionally protected rights and increasingly exercised through digital platforms.

From a human rights perspective, this study affirms that counterterrorism policies in the digital era must be grounded in proportionality and accountability. National security objectives cannot justify the erosion of fundamental freedoms, particularly when restrictions are imposed through norms that lack precise legal boundaries. Criminal law must therefore function as an *ultimum remedium*, applied only when there is clear evidence of intent and a demonstrable connection between technology-based training and the commission of terrorist acts.

Based on these findings, this study proposes several concrete recommendations. First, the government should adopt an implementing regulation, such as a Government Regulation (Peraturan Pemerintah), that explicitly delineates the types of information and communication technology skills, training modalities, and digital competencies that may legitimately fall within the scope of terrorism-related training. Such regulation should distinguish clearly between prohibited conduct and lawful

activities, including education, research, and technological innovation. This step is essential to ensure legal certainty and prevent arbitrary enforcement.

Second, the strengthening of judicial oversight mechanisms is imperative. Every preventive measure taken under Article 12B, particularly those involving surveillance, interception of digital communications, or restrictions on online activities, should be subject to prior authorization and continuous supervision by an independent judicial authority. Enhanced judicial oversight would serve as a safeguard against abuse of power while reinforcing due process guarantees and public trust in counterterrorism law enforcement.

Ultimately, the effectiveness of counterterrorism efforts in the digital era depends not only on the breadth of criminalization but on the precision, accountability, and human rights orientation of legal norms. By refining the normative framework of Article 12B and reinforcing judicial control, Indonesia can ensure that its counterterrorism strategy remains both effective and constitutionally legitimate. In this way, national security and the protection of civil liberties are not mutually exclusive but can coexist within a legal system that upholds democracy, the rule of law, and human dignity.

BIBLIOGRAPHY

Books

- Arief, Barda Nawawi. *Bunga Rampai Kebijakan Hukum Pidana*. Jakarta: Kencana, 2010.
- Husak, Douglas. *Overcriminalization: The Limits of the Criminal Law*. Oxford: Oxford University Press, 2008.
- Marzuki, Peter Mahmud. *Penelitian Hukum*. Edisi Revisi. Jakarta: Kencana, 2022.

- Soekanto, S. 2006. *Pengantar Penelitian Hukum*. Jakarta: UI Press.
- Journal**
- Astuti, Sri Ayu. “Literasi Kemanfaatan Teknologi terhadap Cyber Terrorism di Era Disrupsi dengan AI (Artificial Intelligence).” *Indonesian Journal of Criminal Law & Criminology* 5, no. 3 (2024): 1–12. <https://doi.org/10.18196/ijclc.v5i3.24225>.
- Budiono, Arief, Absori, Kelik Wardiono, Wardah Yuspin, and Said Saidakhrarovich Gulyamov. “Cyber Indoctrination Victims in Indonesia and Uzbekistan: Victim Protection and Indoctrination in Practice.” *Journal of Human Rights, Culture and Legal System* 3, no. 3 (2023): 85–102. <https://doi.org/10.53955/jhcls.v3i3.127>.
- Brunner, Franziska. “Human Rights and Cybersecurity Due Diligence.” *Human Rights Law Review* 18, no. 4 (2018): 783–807.
- Conway, Maura. “Determining the Role of the Internet in Violent Extremism and Terrorism.” *Studies in Conflict & Terrorism* 40, no. 1 (2017): 77–98.
- Floridi, Luciano. *The Ethics of Information*. Oxford: Oxford University Press, 2013. <https://doi.org/10.1093/acprof:oso/9780199641321.001.0001>.
- Khoirunnisa, K., & Didi Jubaidi. 2024. “Indonesia’s Digital Security Strategy: Countering the Threats of Cybercrime and Cyberterrorism.” *Politeia : Journal of Public Administration and Political Science and International Relations* 2, no. 2: 62–82. <https://doi.org/10.61978/politeia.v2i2.211>.
- Marsudianto, Dwi Nugroho, dan Herman Bakir. 2024. “Reconstruction of Criminal Law to Address Cyber Terrorism in Indonesia.” *Journal of Social Science (JoSS)* 3, no. 11: 765–771. <https://doi.org/10.57185/joss.v3i11.382>.
- Patria, Widya Nusa, Md. Shodiq, & Supot Rattanapun. “The Political Role of Criminal Law in Shaping Counter-Terrorism Policy in Indonesia.” *PENA LAW: International Journal of Law* 3, no. 1 (2025): 1–23. <https://doi.org/10.56107/penalaw.v3i1.222>.
- Rachovitsa, Adamantia. 2016. “Engineering and lawyering privacy by design: understanding online privacy both as a technical and an international human rights issue.” *International Journal of Law & Information Technology* 24, no. 4: 374–399. <https://doi.org/10.1093/ijlit/eaw012>.
- Ramadhan, Iqbal. “Cyber-Terrorism in The Context of Proselytizing, Coordination, Security, and Mobility,” *Journal of Islamic World and Politics* 3, no. 1 (2024): 45–63. <https://doi.org/10.18196/jiwp.4252>.
- Rovida, Khofidhotur, and Sasmini. 2023. “Digital Human Rights Protection: Legal Transplantation Strategies to Realize Sustainable Development in Indonesia’s Digitalization Era.” *Domus Legis Cogitatio* 1, no. 2: 35–50. <https://doi.org/10.24002/dlc.v1i2.9926>.
- Situmeang, Ampuan; Ninne Zahara Silviani; Satria Unggul Wicaksana Prakasa; David Tan; Emiliya Febriyani. 2024. “Balancing Human Rights and Cybersecurity: Analyzing Indonesia’s Legal Framework.” *Jurnal Hukum Novelty* 15, no. 2: 200–214. <https://doi.org/10.26555/jhn.v15i2.28738>.

- Syamsurrijal, M., A. Nurmandi, H. Jubba, M. Hidayati, & B. Hariyanto. "De-radicalization through Social Media: Social Media Literacy in Countering Terrorism in Indonesia." *Wawasan: Jurnal Ilmiah Agama dan Sosial Budaya* 9, no. 1 (2024): 1–12. <https://doi.org/10.15575/jw.v9i1.16788>.
- Yüksel, Saadet. 2022. "New Technologies through a Human Rights Lens: Reflecting on Personal Autonomy and Non Discrimination." *Journal of Penal Law and Criminology* 10, no. 2: 281–305. <https://doi.org/10.26650/JPLC2022-1213410>.
- Yüksel, Sezgin. "Digital Rights and Freedom of Expression in the Internet Age." *Computer Law & Security Review* 45 (2022): 105658.
- Internet**
- Agatha Olivia Victoria. "Terror arrests surge, as 1,703 suspects detained in 2018-2024: BNPT". <https://en.antaranews.com/news/336825/terror-arrests-surge-as-1703-suspects-detained-in-2018-2024-bnpt> . diakses 30 Oktober 2025.
- Norbertus Arya Dwiangga Martiar. "Sebarkan Paham Kekerasan Melalui Internet, Terduga Teroris di Purworejo Ditangkap". <https://www.kompas.id/artikel/sebar-paham-kekerasan-melalui-internet-terduga-teroris-di-purworejo-ditangkap> . diakses 30 Oktober 2025.
- Rikke Frank Jørgensen, *Human Rights in the Age of Platforms* (Cambridge: MIT Press, 2019). <https://mitpress.mit.edu/9780262039055>
- Law and Regulation**
- Indonesia. The 1945 Constitution of the Republic of Indonesia.
- Law Number 5 of 2018 concerning the Amendment to Law Number 15 of 2003 on the Eradication of Criminal Acts of Terrorism. State Gazette of the Republic of Indonesia.
- Constitutional Court of the Republic of Indonesia. Decision Number 73/PUU-XVI/2018 concerning the Judicial Review of Law Number 5 of 2018 against the 1945 Constitution of the Republic of Indonesia. Jakarta, 2018.
- Constitutional Court of the Republic of Indonesia. Decision Number 103/PUU-XXI/2023 concerning the Judicial Review of Law Number 5 of 2018 against the 1945 Constitution of the Republic of Indonesia. Jakarta, 2024.