JLPH: Journal of Law, Politic and Humanities
E-ISSN: 2962-2816
P-ISSN: 2747-1985
https://dinastires.org/JLPH dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jlph.v6i1

Interception at A Crossroads: Juridical And Strategic Perspectives on Wiretapping In Indonesia's Counter-Terrorism Framework In The Digital Era

Ade Artya[1*], Sapto Priyanto[2], Imam Subandi[3]
[1] Sekolah Kajian Stratejik dan Global, Universitas Indonesia, Depok, Indonesia, ade.artya@ui.ac.id
[2] Sekolah Kajian Stratejik dan Global, Universitas Indonesia, Depok, Indonesia, sapto.priyanto09@ui.ac.id
[3] Sekolah Kajian Stratejik dan Global, Universitas Indonesia, Depok, Indonesia, imam.subandi@ui.ac.id

[*]Corresponding Author: ade.artya@ui.ac.id

Abstract: This research investigates the critical crossroads in Indonesia's counter-terrorism strategy, where success in suppressing terrorist attacks coincides with the expansion of a dual surveillance apparatus in the digital era. Employing a qualitative approach with juridical normative analysis and the Actor-Network Theory (ANT) framework, this study examines the strategic and legal dimensions of wiretapping. Findings indicate that the formal legal framework, particularly Law No. 5 of 2018, provides a basis for effective proactive interception but contains ambiguities that grant broad discretionary power. Crucially, the research uncovers a parallel, unregulated surveillance regime involving invasive spyware procurement and extra legal agreements that bypass judicial oversight, thereby threatening civil liberties. The study concludes that this duality creates a security paradox, where tactical success masks systemic risks to the rule of law. Comprehensive legislative reform is imperative to establish a singular, proportional, transparent, and accountable framework.

Keyword: Wiretapping, Counter Terrorism, Digital Terrorism, Privacy Rights

INTRODUCTION

Threats of terrorism today are no longer static; they are constantly evolving. This change is evident in the increasingly diverse methods used, the widening impact, and the growing variety of scales and types of targets in current global terrorist attacks (Bobic, 2014). The transnational nature of terrorism, which is not bound by national borders, presents a unique challenge: a confrontation between state actors and non-state entities (Permono, 2019). Transnational terrorist actors are not bound by national ties or sentiments but are loosely organized in networks with their own financial channels. This differs from traditional terrorism, which is characterized by a purely national and territorial focus, as well as an organizational structure that tends to be hierarchical (Duyvesteyn, 2004). Besides that, the digital era, marked by the dominance of the internet, has revolutionized how society interacts and accesses

information, transforming the social order. While often seen as a driver of progress, on the other hand, the digital era is frequently misused by violent extremist groups to spread radical ideologies more widely (Do, Gomez-Parra, & Rijkers, 2023). This indicates a trend where modern terrorist organizations have transformed to leverage current state-of-the-art information and communication technology.

Given the trend of terrorist organizations becoming transnational and exploiting technology, conventional counter-terrorism approaches are no longer relevant. As a result, policymakers are required to formulate new strategies and tactics to face these threats. The constant threat of terrorism against sovereign nations demands that the state, as a sovereign entity, has the inherent right to use repressive measures as part of its national legal and security policy instruments (Permono, 2019). In public policy studies (Cristol, 2009), national interest is consistently positioned as a significant independent variable in the formulation and implementation of national security policy. This concept indicates that all actions taken by a state in the security domain are fundamentally directed towards achieving the goals that have been established as its national interest

The urgency of this phenomenon is partially addressed through the adoption of wiretapping as a modern surveillance instrument within counter-terrorism efforts, positioned as both a legal and security policy to combat contemporary forms of terrorism. In this context, the utilization of technology serves as a crucial mechanism for intelligence gathering, occupying a central role in contemporary policing practices. This method is deemed the most effective, as it reflects a proactive operational framework rather than a passive, reactive stance (Congram; Mitchell, Bell, Peter, 2010). The strategies, methods, techniques, and policies of wiretapping are delineated in the journal (Mersky & Price, 2006), This historical precedent illustrates how electronic surveillance, initially legitimized and widely accepted as a response to organized crime, gradually evolved into a critical instrument in broader law enforcement and security practices. In contemporary contexts, particularly within counter-terrorism efforts, wiretapping and other forms of electronic monitoring are no longer confined to combating organized crime but have become integral to proactive strategies aimed at preventing acts of terrorism before they occur (Rachmad, 2016). However, over time, the use of wiretapping methods particularly within the context of counter-terrorism has sparked intense debate concerning potential violations of human rights, most notably the right to privacy.

In his work entitled “Data Gathering, Surveillance, and Human Rights: Recasting the Debate” (Bernal, 2016), Paul Bernal critiques the flawed public perception of surveillance particularly wiretapping which is often narrowly framed as merely conflicting with the right to privacy. In reality, its impact is far broader, encompassing freedom of expression, freedom of assembly, protection from discrimination, and even the right to security. This misconception, which Bernal refers to as “mis-casting,” produces a Panopticon effect, wherein individuals restrict their own behavior not because they are actively being monitored, but because they feel they could be monitored at any time. Bernal further highlights two additional common errors: first, the artificial separation between state surveillance and corporate surveillance, despite their interconnectedness; and second, the framing of privacy and security as mutually exclusive choices, overlooking the fact that the erosion of privacy can, in fact, undermine security itself.

Meanwhile, in their work “The Perils of Hyper-Vigilance: The War on Terrorism and the Surveillance State in South-East Asia” (Jones & Smith, 2007) Jones and Smith demonstrate that hyper-strict surveillance models, such as those implemented in Singapore and Malaysia, have in fact generated a security paradox. Rather than effectively detecting transnational terrorist networks such as Jemaah Islamiyah, these surveillance practices were more frequently directed toward controlling domestic political opposition. Consequently, the capacity of intelligence agencies to accurately assess real threats became blunted. The regimes’ obsession with the notion of “total defence” fostered a climate of perpetual fear, undermining public

participation and suppressing criticism elements that should form an integral part of any early-warning system. This situation, in turn, enabled groups such as Al-Qaeda to establish operational nodes in Mindanao, Johor, and even Solo, remaining undetected until the occurrence of the 9/11 attacks.

This underscores that the investigation of terrorism through wiretapping cannot be understood solely from the perspective of national security interests. A disciplinary paradigm or segmented perspective is insufficient to accurately and comprehensively explain terrorism in terms of its root causes, strategies, and appropriate countermeasures (Youngman, 2018). Therefore, while taking into account the prevailing legal framework, human rights considerations, and national interests particularly within the Indonesian context this paper seeks to examine the justification and strategic optimization of wiretapping methods as a consequence of the urgency posed by globalization, evolving social dynamics, technological developments, and the maneuvers of modern terrorist networks.

METHOD

This study employs a qualitative approach with a juridical normative and descriptive analytical research design. Data were collected through a literature review (library research), drawing from primary sources, namely laws and regulations (specifically Law No. 5 of 2018 and the new Criminal Code), and secondary sources, including scholarly journals, books, and relevant institutional reports. All data were analyzed using qualitative content analysis to systematically synthesize the findings. The primary analytical framework is Actor Network Theory (ANT), which is utilized to dissect the evolution of the digital terrorism threat as a dynamic network of human and non-human actors (e.g., propaganda, algorithms). This analysis is further supported by Situational Crime Prevention Theory (SCPT), Social Contract Theory, and Utilitarianism to evaluate the strategic and ethical aspects of wiretapping.

RESULTS AND DISCUSSION

Wiretapping from a Legal Perspective

Based on Law No. 17 of 2011, wiretapping is defined as the activity of listening to, recording, diverting, altering, obstructing, and/or documenting the transmission of electronic information and/or electronic documents, whether conducted through cable-based communication networks or wireless networks such as electromagnetic or radio frequency transmissions, including the examination of packages, mail, correspondence, and other documents. In principle, wiretapping is an activity that is generally prohibited. Certain regulations even stipulate criminal sanctions for conducting wiretapping, as provided in Law No. 11 of 2008 on Electronic Information and Transactions and Law No. 1 of 2023 on the Indonesian Penal Code. Nevertheless, this does not mean that wiretapping is absolutely impermissible. In fact, statutory authority to conduct wiretapping has been granted to several institutions in Indonesia for different purposes. Among these are: maintaining and upholding the honor, dignity, and conduct of judges (Law No. 18 of 2011); safeguarding state intelligence interests (Law No. 17 of 2011); and serving the purposes of criminal justice (Yuvens, Widigda, & Sharifa, 2017).

The definition of terrorism under the revised Law No. 1 of 2023 (the National Criminal Code) is as follows: any person who employs violence or threats of violence that create an atmosphere of terror or widespread fear among the public, cause mass casualties by depriving others of liberty or resulting in loss of life and property, or inflict damage or destruction upon strategic vital objects, the environment, public facilities, or international facilities, shall be subject to imprisonment for a minimum of five (5) years and a maximum of twenty (20) years, life imprisonment, or the death penalty. This definition does not significantly differ from the earlier formulation under Law No. 5 of 2018 on the Eradication of Terrorism Crimes. A

comparison between Article 600 of the National Criminal Code and Article 6 of Law No. 5 of 2018 demonstrates alignment with the general pattern of the Code. One notable change, however, is the removal of the explicit element of "intentionally" as a written component of the offense. The question of whether intent must be proven has been addressed in the new Code, which stipulates that all criminal acts are presumed to be committed intentionally, except where negligence is expressly provided (DA, 2023).

The urgency of terrorism is further underscored by the inclusion of specific provisions in Article 187 of the National Criminal Code, which regulates particular categories of crime, including terrorism and the financing of terrorism. These offenses are distinguished on the basis of their severe victimization impact; their frequent transnational and organized character; the application of special procedural rules; their frequent derogation from general principles of substantive criminal law; the existence of specialized law enforcement bodies with exceptional authority; their grounding in international conventions, both ratified and unratified; and their characterization as crimes deemed especially heinous and universally condemned by society. On this basis, terrorism is classified within a separate chapter entitled Special Crimes (Chapter XXXV), formulated as a core crime serving as bridging provisions between Law No. 1 of 2023 and related lex specialis statutes, such as Law No. 5 of 2018 on the Eradication of Terrorism Crimes and Law No. 9 of 2013 on the Prevention and Eradication of Terrorism Financing Crimes.

With respect to wiretapping in the context of counter-terrorism, Law No. 5 of 2018 establishes a legal foundation for the conduct of interception in the investigation of terrorism-related offenses. This provision grants investigators special authority to intercept communications, including letters, shipments, and conversations conducted via telephone or other communication devices, provided that sufficient preliminary evidence exists. The mechanism of interception is strictly regulated, encompassing the requirements for authorization, the duration of implementation, and accountability for the results obtained. Similarly, Law No. 8 of 2010 on the Prevention and Eradication of Money Laundering, which also addresses terrorism financing, recommends that law enforcement agencies employ interception of electronic information and/or electronic documents in accordance with statutory provisions.

In relation to Law No. 1 of 2023, the element of "intentionally" is no longer required to be explicitly stated in every formulation of a criminal offense, although it remains a prerequisite that must be proven by the public prosecutor. Moreover, the recognition of terrorism as an extraordinary crime through its classification under the chapter on Special Crimes provides justification for the necessity of equally extraordinary law enforcement approaches. One such approach is the authority to conduct wiretapping, which is regarded as an integral component in combating threats of this extraordinary nature. Nevertheless, it must be emphasized that such authority should be exercised in strict adherence to prevailing legal principles, particularly those relating to the protection of human rights, most notably the right to privacy. Furthermore, it should be underscored that all intelligence information obtained through wiretapping is to be treated as confidential (Gardner, 2017).

To situate wiretapping within a broader legal context, it is essential to examine international human rights standards that have become reference points for state practices in communications surveillance. A particularly relevant framework is found in Article 8 of the European Convention on Human Rights (ECHR). As (Bernal, 2016) explains, the retention of metadata or, in the context of this paper, wiretapping is regarded as a form of interference with privacy, as affirmed in Malone v. United Kingdom (1984). Bernal argues that the dichotomy between content and metadata is merely semantic, since metadata can be equally intrusive and is, in fact, easier to analyze. Consequently, the "gather in bulk, access in detail" approach requires strict proportionality testing, as underscored in the Digital Rights Ireland decision of

the Court of Justice of the European Union (CJEU), which rejected bulk data retention on the grounds that it constituted a serious violation of the right to privacy. Indonesia may draw upon these standards as a reference point in striking a balance between the practice of wiretapping and the protection of human rights.

The Threat of Terrorism in the Digital Era

Furthermore, Article 15 (1) of the National Criminal Code stipulates that the preparation of a criminal offense occurs when an individual seeks to obtain or prepare means such as tools, gathers information or formulates plans of action, or undertakes similar measures intended to create the conditions necessary for the direct commission of an offense. These preparatory acts may be construed as forms of criminal conduct where they demonstrably constitute part of the preparation of a terrorism offense. Although such actions may not inherently constitute criminal acts under normal circumstances, they are deemed punishable insofar as they establish the preconditions for the commission of a crime. Nevertheless, an exception to liability exists if the suspect ceases the preparatory conduct or otherwise prevents the conditions envisaged in Article 15(1) from materializing. Consequently, this provision requires law enforcement authorities to conduct in-depth examinations to establish the appropriateness of imposing criminal liability.

This concept signifies a paradigm shift, wherein preparatory acts that were previously beyond the reach of criminal law are now explicitly criminalized under the statute. The primary focus of this provision lies in addressing serious and/or exceptional offenses that may cause significant harm to the state and society, such as terrorism. In this regard, the legislation demonstrates a strong preventive orientation aimed at thwarting the commission of terrorist acts in Indonesia. At the same time, it is necessary to further examine the evolving challenges and opportunities associated with surveillance in the digital era, particularly in relation to counter-terrorism efforts.

According to the report by the National Counterterrorism Agency (BNPT, 2023), the Ministry of Communication and Information Technology (Kemenkominfo) has actively engaged in blocking websites associated with extremism, violence, and terrorism. Nevertheless, research conducted by Tech Against Terrorism highlights persistent gaps in these blocking efforts. Data from Tech Against Terrorism (Terrorism, 2023), indicate that although the majority of terrorist-related links have been removed by technology companies and/or governments, there remains a significant disparity between global takedown levels and those observed in Indonesia. For instance, Telegram channels affiliated with ISIS have remained active for several years, exposing weaknesses in Indonesia's content blocking measures. One such channel, created on 11 June 2018 and containing reference material on the manufacturing of explosives, was still publicly accessible as late as the end of 2022, even though it had been cited in an initial court ruling in 2019 and repeatedly referenced in subsequent terrorism-related court decisions.

A release by Tech Against Terrorism reported that, out of 39,964 links identified in 2023, the majority originated from file-sharing and video-sharing platforms, which serve as digital repositories for disseminating terrorist propaganda (Terrorism, 2023). The group most actively distributing online content was ISIS, with more than 4,364 pieces of material detected. By the end of the same year, however, approximately 12% of those links remained publicly accessible (BNPT, 2023). The persistence of such content is compounded by the use of highly encrypted private communications on social media, as well as the creation of hundreds of backup accounts by ISIS supporters in Indonesia to ensure the continuity of propaganda messages (IPAC, 2018). In addition, more sophisticated methods have been employed, including advanced cryptography, strong encryption, and even the exploitation of the dark web. Techniques such

as steganography where video, photographic, or textual data are concealed within another file were previously documented in the operations of Al Qaeda (Weimann, 2016).

The implications of online radicalization are increasingly alarming. Cases involving lone-actor terrorism demonstrate that the internet has become a primary medium through which individuals are exposed to extremist ideologies without the need to formally join a terrorist organization. For instance, ZA, the female assailant in the 2021 attack on Indonesia's National Police Headquarters, underwent a process of self-radicalization. This was confirmed through her social media posts, which displayed the ISIS flag accompanied by a caption about jihadist struggle just hours before the attack (Chew, 2021) (Yudhistira, 2021) Similarly, a 14-year-old student in Subang, arrested in 2017 for assembling a homemade bomb, was found to have been radicalized through ISIS publications and radical narratives circulated online (BNPT, 2023). These cases underscore how digital propaganda can transform vulnerable individuals into active perpetrators of terrorism, even in the absence of direct organizational ties.

Empirical studies indicate that the majority of lone-actor terrorists (lone wolves) have undergone ideological indoctrination influenced by ISIS and experienced self-radicalization through the internet. This phenomenon represents the efficacy of ISIS propaganda in penetrating individuals and initiating acts of violence. Data from 2023 recorded at least seven cases of lone-wolf attacks in which perpetrators were exposed to radical propaganda via social media platforms and online domains without direct affiliation with organized terrorist groups. This process, identified as self-radicalization, occurs virtually and reflects a significant departure from the conventional radicalization trajectory, which typically relies on interpersonal interactions and group dynamics (the "staircase of terrorism" model). The dominance of ISIS's ideological influence within this lone-actor radicalization process emerges as a critical finding in understanding the group's ability to effectively reach and mobilize its propaganda targets (Riyanta, 2022).

The phenomenon of individual terrorism, commonly referred to as "lone-wolf" attacks, is not new in history. Perpetrators often act independently without direct affiliation to organized terrorist groups. However, advances in information technology, particularly the internet, have transformed the landscape of radicalization and accelerated the growth of this phenomenon. Digital platforms, as broad social contexts, can significantly shape individual behavior (Cahyaningsih, Ati, & Abidin, 2019). For extremist virtual communities, digital platforms function as incubators where radicalized individuals inspire one another, exchange ideology, and gain knowledge of attack tactics without requiring direct physical interaction. The internet also enables jihadist groups to disseminate ideological propaganda, as well as information on weapons, ammunition, and explosives (Khoiri, 2023), while constructing online narratives that exploit and politicize grievances related to racial, religious, and social issues. Such narratives, particularly those propagated by ISIS, have proven highly effective in attracting potential recruits, especially in Southeast Asia (Arianti, et al., 2020). Even in highly developed and modern countries such as Singapore, these narratives have begun to draw women into playing more significant roles within terrorist networks. Urban social dynamics such as marginalization, discontent with prevailing social values, and the search for identity play a pivotal role in these radicalization processes (Dewi & Sadadi, 2021). Virtual environments, reinforced by intensive interactions, provide a space where individuals who are exposed to extremist content and integrated into such communities become increasingly convinced to commit acts of violence and terrorism.

The urgency of this issue is further underscored by Actor-Network Theory (ANT), which conceptualizes the world as a complex, interconnected network. Within ANT (Luppicini, 2014), the framework provides valuable insights into how terrorist indoctrination proliferates across social media through the interplay of actors, intermediates, and actants. In this context, actors include individuals, groups, or states that actively disseminate extremist ideology.

Intermediates consist of influencers, group administrators, bots, algorithms, and social media platforms, functioning as conduits that link actors to broader audiences. Meanwhile, actants may take the form of extremist social media accounts, as well as file-sharing and video-sharing platforms used for propaganda non-human entities endowed with agency to act and influence within the network. The dynamic interplay between actors, intermediates, and actants creates a highly complex system in which extremist messages can spread rapidly, widely, and with great resistance to disruption.

A study by (Atari, et al., 2022), demonstrates that moral homogeneity within extremist social networks or homogeneous networks significantly increases both radical intentions and the volume of hate speech posted online. The research reveals that individuals who perceive their moral views as aligned with those of their group members are more inclined to undertake extreme actions in defense of the group. Such homogeneous extremist networks often materialize in the form of radical groups on online platforms, functioning as intermediates between terrorist ideologies and broader audiences. This phenomenon is further exacerbated by social media algorithms, which operate on personalization and relevance determined by multiple factors such as user interactions, followed accounts, visited content, as well as temporal and geolocation data.

As an illustration, the dissemination of disinformation surrounding the Southport incident amplified by influential accounts across social media has contributed to deepening societal divisions. False narratives framing the perpetrator as a Muslim asylum seeker with extremist political affiliations spread extensively across multiple platforms, including closed or private digital communication groups with thousands of members (Hall, 2024). One notable manifestation was the mobilization call for demonstrations targeting local mosques. Furthermore, hyperlinks embedded in various YouTube sermon videos redirected viewers to Telegram groups where ISIS sympathizers underwent processes of introduction, discussion, radicalization, and even pledging allegiance (bai‘at) within the span of just one week. This phenomenon gave rise to a new terminology coined by Anshar Daulah Media, whereby ISIS sympathizers could be recognized as “internet jihadis” merely by sharing terrorist ideological content and its technical manuals. Such developments underscore how terrorist ideologies have become increasingly accessible and reinforced through algorithmic amplification that revolves around commonly used keywords (BNPT, 2023).

Meanwhile, in the context of terrorism financing, evidence has been found of fundraising activities conducted openly via Telegram groups, with donations transferred directly to the bank accounts of sympathizers supporting terrorist organizations. These fundraising efforts were often framed as humanitarian relief for conflict-affected regions such as Syria, yet the collected funds were ultimately diverted to finance terrorism in those areas. Conflict-related issues are frequently exploited as bait to attract donations, which are subsequently misappropriated by terrorist groups (BNPT, 2023). This phenomenon underscores the role of virality and algorithmic recommendations in amplifying divisive narratives during times of crisis or even perceived crises which can be strategically exploited by terrorist networks to advance their political objectives.

All of these elements interact and coalesce into a dynamic network, each actively shaping contemporary social realities. Within the aforementioned context, doctrines disseminated through downloadable filesharing and video-sharing platforms manifest and persist as actants. These actants continuously radicalize individuals, recruit new members, propagate violent ideologies, and generate new actors unless decisive measures are taken to disrupt such networks. This process endures even after the original propagators or actors have been deradicalized or have died. For instance, despite the organizational collapse of ISIS and the demise of its founding leadership, the group’s ideology continues to persist through sporadic attacks and propaganda disseminated by its supporters (Rehman, 2022).

The IPAC report (IPAC, 2019) indicates a marked emergence of independent cells that are not directly affiliated with Jamaah Ansharul Daulah (JAD), the largest pro-ISIS coalition in Indonesia. These independent cells are motivated not only by ISIS's directives to wage domestic attacks, but also by a desire to demonstrate that they can execute acts of violence surpassing those of JAD. "These groups generally coalesce without extensive vetting, training, indoctrination, weaponry, or operational experience. According to Sidney Jones (director of IPAC), their greatest asset is the spirit and desire for recognition." They have also relied on instructional bomb-making material attributed to the late Bahrun Naim an Indonesian who joined ISIS in Syria in early 2015 and was killed in an airstrike in November 2018. His online manual, originally posted on a blog, later circulated across social media and was ultimately compiled into an e-book that became required reading for any prospective terrorist interested in planning an attack.

In the era of transnational crime, the concept of endogenous leadership has emerged, which in the context of Actor-Network Theory (ANT) may be understood as the rise of new actors. According to (Cheng & Suen, 2021), endogenous leadership refers to citizens with radical preferences who assume leadership roles previously held by pioneering or parent actors such as ISIS or Al-Qaeda leaders. Radical leaders as pioneering actors tend to inflate the level of radicalism within their agendas to convince followers that the current situation is dire, a process referred to as the signaling role of radicalism. Within mass movements, this signaling functions as a strategic cue by leaders to persuade followers of the severity of circumstances. The emergence of endogenous leadership as new actors frequently occurs among followers within online media spaces, reinforcing radicalism both in movements and ideologies. Unsurprisingly, while some case studies suggest the decline of parent transnational terrorist organizations such as ISIS, empirical evidence demonstrates the ease with which new cells emerge (IPAC, 2021). These cells continue to proliferate including some formed through social media reaching regions with no prior history of extremist violence (IPAC, 2020).

Justification and Enhancement of Wiretapping Effectiveness

The action taken by Kominfo in blocking websites and online sources related to violent extremism and terrorism has slightly minimized the influence of intermediates based on Actor-Network Theory (ANT). However, what needs to be further examined is whether the removal of these intermediates, particularly extremist websites, has actually resolved the network problem. Considering the existence of platforms that disseminate doctrines through downloadable file-sharing and video-sharing platforms, and referring to ANT, such cases potentially give rise to new actors as a result of actants that have been stored and are most likely studied by prospective new terrorist actors. The concern is that with such a pattern, the dissemination of doctrines and technical preparations for terrorist acts will become more widespread through networks that continue to generate new ones.

Cases of terrorist attacks that occurred prior to the era of intensive surveillance serve as empirical evidence that traditional investigative approaches were unable to keep pace with the speed and complexity of modern terrorism threats. This is reinforced by the study of (Mulya, Ismail, Yuliantoro, & Kandati, 2022), which reveals that conventional, manual investigative methods have proven to be inefficient in uncovering terrorist networks. The emergence of intermediates, actants, and new actors in the dissemination of radical ideologies and the exponential expansion of terrorist networks further underscores the urgency of employing surveillance technology as a more sophisticated and responsive investigative tool to address the dynamics of contemporary threats. Such an approach is regarded as the most effective method, as it embodies a proactive framework rather than a passive, wait-and-see stance (Congram; Mitchell, Bell, Peter, 2010).

Several forms of behavior involving the provision and retrieval of information via the internet that indicate intent or action toward terrorism merit legal follow-up. The act of seeking out such information even to the extent of consciously downloading filesharing and video-sharing materials, along with the inherent risks of such actions should at least be considered as grounds for inclusion under the criminal preparation offense of conspiracy as stipulated in Article 15 of Law No. 1 of 2023. It may also be classified as preliminary evidence under Article 31 of Law No. 5 of 2018, thereby providing a legal basis for the conduct of surveillance. However, in order to ensure legal certainty and protect the right to privacy, a reinforcing element of argumentation is required, one that can be grounded in the degree of active involvement. This includes indicators such as active membership, possession of radical materials, and communication with other members. Such an approach is deemed effective in ascertaining mens rea (criminal intent) as well as actus reus (criminal act). Moreover, the confidentiality of surveillance results is guaranteed under Article 31 of Law No. 5 of 2018, which stipulates that such information is to be used solely for the purposes of investigation and the resolution of relevant criminal cases.

The diverse publications of terrorist networks ranging from e-books, filesharing, video-sharing, online content, and beyond have become key references for aspiring terrorists in Indonesia. Through social media platforms, these networks disseminate propaganda, raise funds, coordinate operations, and provide technical instructions for terrorist attacks. Furthermore, the adoption of more advanced encryption technologies, such as steganography, allows them to conceal secret messages within media files, thereby complicating law enforcement investigations. In addition, homogeneous extremist networks, often formed through social media, have successfully recruited new members across various regions, including areas previously untouched by extremist ideologies. The ease of content distribution via online platforms has facilitated the rise of virtual jihad, where individuals are considered participants simply by sharing content. Radical online “gatherings” that continuously provide indoctrination, coupled with the accessibility of downloadable extremist materials and the reinforcing nature of homogeneous networks, significantly heighten the risk of exposure to radical ideologies and self-radicalization. herefore, the author argues that such circumstances merit serious consideration for the application of surveillance measures against individuals engaged in these interactions particularly given the existing regulatory framework that accommodates such measures.

To optimize wiretapping as a method for combating terrorism, its key success factor lies in the principle of confidentiality. Unlike other investigative measures that may be open to external oversight, wiretapping must be conducted covertly to ensure the effective acquisition of critical information (Yuvens, Widigda, & Sharifa, 2017) One proposed solution is the differentiation of judicial filing locations from the geographical locus of terrorist suspects. However, this mechanism is more applicable to geographically based terrorist cells, leaving gaps when addressing geographically unbound groups or lone-wolf actors.

Therefore, law enforcement may need to rely on the urgent circumstances clause under Article 31A of Law No. 5 of 2018, particularly when there are preliminary indications that an individual has joined online groups dedicated to information-seeking, coupled with active involvement in conspiracy, recruitment, financing, or terrorist training. In such cases, the statutory three-day reporting window provides an opportunity to identify the suspect’s location and network through wiretapping before proceeding with judicial authorization outside the suspect’s immediate jurisdiction. This strategy could safeguard the secrecy of operations and prevent countermeasures by the targets. Furthermore, effective wiretapping investigations require collaboration and technical access involving Network Operators, who manage public telecommunications infrastructures facilitating data transmission through internet packages, wireless networks, optical devices, or electromagnetic signals (Mulya, Ismail, Yuliantoro, &

Kandati, 2022). The intercepted communications are subsequently relayed by access and service providers to law enforcement, serving as admissible evidence in terrorism-related prosecutions. Accordingly, stronger synergy between the government and Network Operators is indispensable to ensure the effectiveness and continuity of wiretapping policies in counterterrorism efforts.

The implementation of Law No. 5 of 2018, particularly the provisions on wiretapping under Article 31, has made a significant contribution to reducing terrorist attacks in Indonesia since its enactment. Statistical data indicate a remarkable decline: only two terrorist incidents were recorded in 2022, and in 2023 Indonesia achieved a "Zero Terrorist Attack" milestone (Ramadhan & Prabowo, 2024). This success cannot be separated from intensive preventive and repressive measures, including the strategic use of wiretapping policies. The effectiveness of these measures is further reflected in the arrest of 1,665 suspected terrorists (BNPT, 2023) (Ikhsan & Kurniati, 2023), underscoring the pivotal role of surveillance and interception in counterterrorism efforts.

The author identifies two primary anticipatory dimensions of wiretapping in the context of counterterrorism. First, wiretapping enables the early detection of terrorist activities through the direct monitoring of communications during investigation and prosecution processes. Second, surveillance via interception serves a preventive function, reducing both the motivation and the opportunity for potential perpetrators to commit acts of terrorism. This aligns with the position of (Molepo, Faimau, & Mashaka, 2020), who argue that offenders' intentions may be deterred when faced with the likelihood of apprehension, consistent with the Situational Crime Prevention Theory (SCPT). The theory posits that environmental conditions correlate with crime levels, and that increasing the likelihood of detection and punishment provides a more effective deterrent than the severity of sanctions alone. Moreover, as (Perry, Apel, Newman, & Clarke, 2017), suggest, anticipatory benefits arise when publicity surrounding the introduction of new measures such as the statutory provision for wiretapping and its subsequent implementation leads to an immediate decline in criminal activity even before the measures are fully enforced. This occurs because terrorism, like other forms of crime, is heavily dependent on both motivation and opportunity, a dynamic captured in the concept of the "thinking terrorist" (Marroni, Moreno, Tortolini, Tamburini, & Landucci, 2024). Finally, the periodic publication of reports on the implementation of wiretapping while ensuring the confidentiality of sensitive information would enhance accountability and strengthen public trust in law enforcement agencies.

Dilemma of Interception: The Right to Privacy and the Right to Life

Intelligence analysis of citizens' online behavior enables law enforcement to detect early indications of terrorist activities and predict the likelihood of future attacks. This preventive capacity often gives rise to the argument that "if one has nothing to hide, there is nothing to fear," a rationale frequently used to justify mass surveillance. However, despite the preventive intentions underpinning such practices, it is crucial to recognize that every individual is entitled to the right to privacy. This right is fundamental not only for those suspected of wrongdoing but also for law-abiding citizens engaging in activities that, while entirely legal, may be considered socially controversial or morally ambiguous (Allison, 2017). The dilemma, therefore, lies in balancing two fundamental rights: the right to privacy, which protects individual autonomy and dignity, and the right to life, which obligates the state to safeguard its citizens from terrorist violence. Excessive surveillance risks creating a "chilling effect," whereby individuals restrain their lawful behavior out of fear of being monitored, ultimately undermining democratic freedoms. Conversely, insufficient surveillance may compromise public safety by allowing terrorist threats to go undetected. This tension underscores the need for proportionality and accountability in the implementation of wiretapping regulations.

Interception should be conducted selectively and based on clear legal thresholds, subject to judicial oversight, and accompanied by transparency mechanisms to prevent abuse of power. In this way, the state can fulfill its dual mandate: protecting its citizens from terrorism while simultaneously upholding the fundamental rights that define democratic society.

The use of wiretapping in the context of terrorism investigations represents a crossroads between the need for national security and the protection of human rights. From the perspective of positive law, such as Law No. 5 of 2018 on the Eradication of Terrorism Crimes, wiretapping is justified as a preventive measure against terrorist acts that threaten the lives of many people. However, questions arise regarding the limits of the state's authority to intervene in the private lives of its citizens.

This question can be addressed through Social Contract Theory, which guides individuals to uphold social order by relinquishing certain freedoms in exchange for governance within a nation or state (Kruikemeier, Boerman, & Bol, 2020), as regulated by existing law. As a state based on the rule of law, Indonesia is obligated to uphold the supremacy of law, human rights, and equality before the law for all citizens without exception (Sriyono, 2021). Furthermore, in the context of counter-terrorism, the proportionality of criminal law must refer to the relevance and clarity of its objectives, namely the prevention of terrorist acts. Indonesia's anti-terrorism legislation is considered to have established a proportional and strictly regulated wiretapping mechanism, encompassing requirements for judicial authorization, implementation duration, and accountability for the results obtained.

From a utilitarian perspective, wiretapping can be considered an ethical action when evaluating its positive consequences. For instance, the prevention of terrorist acts yields benefits for national security, public safety, investor confidence, and the protection of citizens' right to life, objectives deemed more urgent than preserving the privacy of suspected terrorists. This reasoning is based on the principle that actions producing the greatest overall benefit for society are morally right (Pratiwi, Negoro, & Haykal, 2022). Furthermore, as discussed in (Congram; Mitchell, Bell, Peter, 2010) while privacy undeniably plays an important role in daily life, it can simultaneously provide additional protection for criminals and illicit enterprises to carry out their activities.

Grabosky dan Smith (1998) also argue that respect for individual privacy is not an absolute interest and can be subordinated to other public interests (Congram; Mitchell, Bell, Peter, 2010), particularly the right to life of the public. Indiscriminate attacks, often employed by perpetrators of terrorism (Permono, 2019), pose a tangible threat and, once executed, constitute a violation of the right to life for many individuals. In conclusion, wiretapping of suspected terrorists can be justified not only from a legal standpoint but also from a moral perspective and in terms of broader human rights for society, outweighing the potential infringement on the privacy of individual suspects. This is further reinforced by the primacy of the fundamental human right to life, as enshrined in Article 3 of the Universal Declaration of Human Rights, which explicitly states that "everyone has the right to life, liberty, and security of person."

Therefore, the handling of terrorism must be carried out in a planned and sustainable manner, with the primary goal of protecting and upholding the human rights of the public (Anggara, et al., 2017). This approach aligns linearly with the aspirations of the Indonesian nation, which are to protect all Indonesians and the entirety of Indonesian territory, advance public welfare, educate the nation, and uphold world order, as enshrined in the Preamble of the 1945 Constitution of the Republic of Indonesia.

CONCLUSION

This study demonstrates that surveillance, specifically wiretapping, plays a crucial role in addressing terrorism threats in the digital era. From a national legal perspective, wiretapping is explicitly regulated in the Criminal Code (KUHP) and Law No. 5 of 2018, providing a legal foundation for preventive measures against acts of terrorism. However, within the human rights framework, the retention of data and mass interception of communications require rigorous proportionality tests to ensure that citizens' privacy rights are not violated.

Analysis from Paul Bernal's study indicates that the distinction between content and metadata in surveillance practices is largely illusory, as both intrude on privacy when processed on a large scale. Meanwhile, research by Jones and Smith demonstrates that excessive surveillance in Southeast Asia can backfire when it is used to suppress political opposition rather than detect transnational terror networks. This underscores that the effectiveness of wiretapping heavily depends on analytical intelligence, accountability, and public engagement in early warning processes.

Thus, the conclusion regarding the focus of this study emphasizes that wiretapping, as a tool of modern surveillance, can serve as an effective counter-terrorism strategy, provided it is implemented proportionally, threat-driven rather than mere data accumulation, transparent under the law, and consistent with human rights principles. For future research, the author recommends focusing on empirical studies of wiretapping effectiveness in Indonesia, including policy analysis, institutional transparency, and the role of public oversight in ensuring accountability in state digital surveillance practices.

REFERENCE

Allison, P. R. (2017). *Upaya pemerintah melacak teroris secara online bisa melanggar privasi Anda*. Retrieved from BBC News Indonesia: https://www.bbc.com/indonesia/vert – fut – 41535747

Anggara, Wagiman, W., Wiryawan, S. M., Ahsinin, A., Oemar, E. N., Pramuditya, M. E., & Hendra, R. (2017). *Politik Kebiajakan Hukuman Mati di Indonesia dari Masa ke Masa.* Jakarta: Institute for Criminal Justice Reform.

Arianti, Sobirin, A., Yaoren, K. Y., Mahzam, R., Bashar, I., Chalerms, R., & Nasir, A. A. (2020). Southeast Asia: Indonesia, Philippines, Malaysia, Myanmar, Thailand, Singapore. *Counter Terrorist Trends and Analyses*, 5 – 39.

Atari, M., Davani, A. M., Kogon, D., Kennedy, B., Saxena, N. A., Anderson, I., & Dehghani, M. (2022). Morally Homogeneous Networks and Radicalism. *Social Psychological and Personality Science*, 999 – 1009. https://doi.org/10.1177/19485506211059329

Bernal, P. (2016). Data gathering, surveillance and human rights: recasting the debate. *Journal of Cyber Policy*, 243 – 264. https://doi.org/10.1080/23738871.2016.1228990

BNPT, I. – K. (2023). COUNTER TERRORISM AND VIOLENT EXTREMISM OUTLOOK. 1 – 63.

Bobic, M. (2014). Transnational organised crime and terrorism: Nexus needing a human security framework. *Global Crime*, 241–258. DOI: 10.1080/17440572.2014.927327

Cahyaningsih, A. A., Ati, N. U., & Abidin, A. Z. (2019). GADGET DAN MAHASISWA (Studi Tentang Dampak Penggunaan Gadget Terhadap Perilaku Mahasiswa di Universitas Brawijaya). *Respon Publik Vol 13, No 3*, 21 – 29.

Cheng, H., & Suen, W. (2021). Radicalism in Mass Movements Asymmetric Information and Endogenous Leadership. *American Political Science Review*, 286–306. DOI: https://doi.org/10.1017/S0003055420000921

Chew, A. (2021). *How middle – class Indonesian millennial Zakiah Aini became an Islamic militant*. Retrieved from South China Morning Post: https://www.scmp.com/week –

asia/people/article/3128176/how – middle – class – indonesian – millennial – zakiah – aini – became – islamic

Congram, M., & Bell, P. (2010). Laying the Groundwork for the Successful Deployment of Communication Interception Technology (CIT) in Modern Policing. *Journal of Policing, Intelligence and Counter Terrorism*, 9 – 27. https://doi.org/10.1080/18335300.2010.9686938

Congram; Mitchell, Bell, Peter. (2010). Laying the Groundwork for the Successful Deployment of Communication Interception Technology (CIT) in Modern Policing. *Modern Policing, Journal of Policing, Intelligence and Counter Terrorism*, 9 – 27. DOI: 10.1080/18335300.2010.9686938

Cristol, J. (2009). Morgenthau vs. Morgenthau? ‘‘The Six Principles of Political Realism’’ in Context. *American Foreign Policy Interests*, 238–244. DOI: 10.1080/10803920903136247

DA, A. T. (2023). *Beragam Perubahan Signifikan dalam KUHP Baru*. Retrieved from Hukumonline.com: https://www.hukumonline.com/berita/a/beragam – perubahan – signifikan – dalam – kuhp – baru – lt647f0ac6d6a99/?page=all

Dewi, V. L., & Sadadi, P. (2021). Konflik Ideologi dan Sosiologi Urban Sebagai Invitasi Terorisme di Prancis. *Jurnal Penelitian Pendidikan Indonesia, Vol 7 No 4*, 651 – 657. DOI:https://doi.org/10.29210/020211226

Do, Q. – T., Gomez – Parra, N., & Rijkers, B. (2023). Transnational terrorism and the internet. *Journal of Development Economics*, 1 – 9. DOI: 10.1016/j.jdeveco.2023.103118

Duyvesteyn, I. (2004). How New Is the New Terrorism? *Studies in Conflict & Terrorism*, 439–454. https://doi.org/10.1080/10576100490483750

Fachri, F. K. (2023). *Upaya Pemerintah Pasca Pengesahan KUHP Baru*. Retrieved from HUKUMONLINE.COM: https://www.hukumonline.com/berita/a/upaya – pemerintah – pasca – pengesahan – kuhp – baru – lt63f7ab08ebc31/

Gardner, J. V. (2017). A Duty to Share: The Opportunities and Obstacles of Federal Counterterrorism Intelligence Sharing with Nonfederal Fusion Centers . 1 – 197.

Hall, R. (2024). *Social media algorithms need overhaul after Southport stabbings riots, Ofcom says*. Retrieved from the Guardian: https://www.theguardian.com/media/2024/oct/22/social – media – algorithms – must – be – adjusted – to – prevent – misinformation – ofcom

Ikhsan, A., & Kurniati, P. (2023). *148 Teroris Ditangkap Sepanjang 2023*. Retrieved from Kompas.com: https://regional.kompas.com/read/2023/12/29/194514178/148 – teroris – ditangkap – sepanjang – 2023

IPAC. (2018). *INDONESIA AND THE TECH GIANTS VS ISIS SUPPORTERS: COMBATING VIOLENT EXTREMISM ONLINE.* Jakarta: INSTITUTE FOR POLICY ANALYSIS OF CONFLICT (IPAC).

IPAC. (2019). *THE ONGOING PROBLEM OF PRO – ISIS CELLS IN INDONESIA.* Jakarta: INSTITUTE FOR POLICY ANALYSIS OF CONFLICT (IPAC).

IPAC. (2020, 28 Februari). *LEARNING FROM EXTREMISTS IN WEST SUMATRA.* Jakarta: INSTITUTE FOR POLICY ANALYSIS OF CONFLICT (IPAC). Retrieved from IPAC: https://understandingconflict.org/en/publications/Learning – From – Extremists – in – West – Sumatra

IPAC. (2021). *THE DECLINE OF ISIS IN INDONESIA AND THE EMERGENCE OF NEW* CELLS. Jakarta: INSTITUTE FOR POLICY ANALYSIS OF CONFLICT (IPAC).

Jones, D. M., & Smith, M. (2007). The Perils of Hyper – Vigilance: The War on Terrorism and the Surveillance State in South – East Asia. *Intelligence & National Security*.

Khoiri, A. (2023). *Tafsir Kemartiran: Studi Kitab Fi Zilal Sūrah al – Taubah Karya 'Abdullah 'Azzām.* Jakarta: UIN Syarif Hidayatullah.

Khoiri, Ahmad; , Faizi; Muttaqin, Jindar. (2021). THE TRANSMISSION OF ISLAMIC POPULISM AND EXTREMIST IDEOLOGY THROUGH SOCIAL MEDIA IN INDONESIA. Jurnal Tashwirul Afkar, 1 – 21.

Kruikemeier, S., Boerman, S. C., & Bol, N. (2020). Breaching the contract? Using social contract theory to explain individuals' online behavior to safeguard privacy. *Media Psychology*, 269 – 292.

Luppicini, R. (2014). Illuminating the Dark Side of the Internet with Actor – Network Theory: An Integrative Review of Current Cybercrime Research. *Global Media Journal*, 35 – 49.

Marroni, G., Moreno, V. C., Tortolini, A., Tamburini, F., & Landucci, G. (2024). Assessing the attractiveness of chemical and process facilities to terrorism using a situational crime prevention approach. *Journal of Loss Prevention in the Process Industries*, 1 – 13.

Mersky, R. M., & Price, J. (2006). The Dictionary and the Man: The Eighth Edition of Black's Law Dictionary. *Jurnal Hukum Samudra Keadilan*, 719 – 733.

Molepo, S. P., Faimau, G., & Mashaka, K. T. (2020). CCTV PLACEMENT IN GABORONE CITY, BOTSWANA: A CRITICAL REVIEW THROUGH THE LENS OF SITUATIONAL CRIME PREVENTION THEORY. *Criminology & Social Integration*, 144 – 163. DOI: www.doi.org/10.31299/ksi.28.2.1

Mulya, A., Ismail, M., Yuliantoro, R. B., & Kandati, H. (2022). Dampak Implementasi Lawfull Interception pada Pemberantasan Tindak Pidana Terorisme. *Formosa Journal of Multidisciplinary Research*, 367 – 382. DOI: https://doi.org/10.55927/fjmr.v1i2.551

Permono, P. (2019). HUKUMAN MATI TERPIDANA TERORISME DI INDONESIA: MENGUJI PERSPEKTIF STRATEJIK DAN HAK ASASI MANUSIA (HAM). *Jurnal HAM*, 127 – 144. DOI: http://dx.doi.org/10.30641/ham.2019.10.127-142

Perry, S., Apel, R., Newman, G. R., & Clarke, R. V. (2017). The Situational Prevention of Terrorism: An Evaluation of the Israeli West Bank Barrier. *J Quant Criminol*, 727–751. DOI 10.1007/s10940-016-9309-6

Pratiwi, E., Negoro, T., & Haykal, H. (2022). Jeremy Bentham's Utilitarianism Theory: Legal Purpose or Methods of Legal Products Examination? *Jurnal Konstitusi*, 271 – 293. DOI: https://doi.org/10.31078/jk1922

Rachmad, A. (2016). LEGALITAS PENYADAPAN DALAM PROSES PERADILAN PIDANA DI INDONESIA. *Jurnal Hukum Samudra Keadilan*, 239 – 249.

Ramadhan, A., & Prabowo, D. (2024). *BNPT: 2023, Indonesia "Zero Terrorist Attack"*. Retrieved from Kompas.com: https://nasional.kompas.com/read/2024/02/20/15341091/bnpt – 2023 – indonesia – zero – terrorist – attack

Rehman, J. (2022). Revisiting the Jihad Ideology in Islamic International Law and its Appropriation by Nonstate Actors. *HUMAN RIGHTS QUARTERLY*, 417–440. DOI: 10.1353/hrq.2022.0015

Riyanta, S. (2022). Shortcut To Terrorism: Self – Radicalization And Lone – Wolf Terror Acts: A Case Study Of Indonesia. *Journal of Terrorism Studies*, 1 – 20. DOI: 10.7454/jts.v4i1.1043

Sriyono, W. (2021). *SANKSI PIDANA MATI BAGI PELAKU TINDAK PIDANA TERORISME BERDASARKAN HUKUM POSITIF DI INDONESIA DAN DALAM PANDANGAN HUKUM ISLAM.* SEMARANG: PROGRAM MAGISTER (S2) ILMU HUKUM FAKULTAS HUKUM UNIVERSITAS ISLAM SULTAN AGUNG SEMARANG.

Terrorism, T. A. (2023). PATTERNS OF ONLINE TERRORIST EXPLOITATION. *TCAP INSIGHTS*, 1 – 39.

Weimann, G. (2016). Going Dark: Terrorism on the Dark Web. *STUDIES IN CONFLICT & TERRORISM*, 195–206. https://doi.org/10.1080/1057610X.2015.1119546

Youngman, M. (2018). Building Terrorism Studies as an Interdiscilinary Space: Addressing Recurring Issues in the Study of Terrorism. *Terrorism and Political Violence*, 1091–1105. https://doi.org/10.1080/09546553.2018.1520702

Yudhistira, W. A. (2021). *Perempuan dan Milenial dalam Aksi Teror di Indonesia*. Retrieved from Katadata.co.id: https://katadata.co.id/ariayudhistira/analisisdata/607049e153f0d/perempuan – dan – milenial – dalam – aksi – teror – di – indonesia

Yuvens, D. A., Widigda, R. S., & Sharifa, A. (2017). DILEMA UPAYA HUKUM TERH A HUKUM TERHADAP PENYADAPAN. *JURNAL HUKUM DAN PEMBANGUNAN, 47*, 289 – 311. https://scholarhub.ui.ac.id/jhp/vol47/iss3/2