

# Privacy Protection Against Forced Wirebreaking Attempt by Law Enforcement Officials

Bagus Oktafian Abrianto<sup>1</sup>, Dharma Setiawan Negara<sup>2</sup>, Samuel Dharma Putra Nainggolan<sup>3</sup>, Vivi Ayudya Permatasari<sup>4</sup>

<sup>1</sup>Faculty of Law, Universitas Airlangga, Indonesia, [bagusoa@fh.unair.ac.id](mailto:bagusoa@fh.unair.ac.id)

<sup>2</sup> Faculty of Law, Universitas Sunan Giri Surabaya, Indonesia, [dharmajournal@gmail.com](mailto:dharmajournal@gmail.com)

<sup>3</sup>Faculty of Law, Universitas Airlangga, Indonesia, [snainggolan43@gmail.com](mailto:snainggolan43@gmail.com)

<sup>4</sup>School of International Law, Southwest University of Political Science and Law, China, [ayuvivi412@gmail.com](mailto:ayuvivi412@gmail.com)

Corresponding Author: [bagusoa@fh.unair.ac.id](mailto:bagusoa@fh.unair.ac.id)

---

## *Abstrak*

*The law permits coercive measures in law enforcement, one of which is telephone tapping. Initially, telephone tapping was closely linked to the protection of privacy as a human right; however, such protection can be limited when necessary and is regulated by law. In Indonesia, regulations governing telephone tapping remain fragmented, as several law enforcement agencies authorized to conduct telephone tapping regulate the mechanism independently through different legal frameworks. This situation has the potential to create legal uncertainty and raise concerns about the protection of citizens' privacy rights. This study uses normative legal research with a legal and conceptual approach. This study aims to analyze the authority of several state institutions to conduct telephone tapping and to examine the mechanisms governing telephone tapping to ensure the protection of the right to privacy as a human right in the law enforcement process.*

**Keywords:** *Wiretapping, Authority, Human Rights*

## **A. INTRODUCTION**

Regulations on the protection of human rights within a state based on the rule of law are absolutely necessary, especially in Indonesia.(Reza & Kamila, 2025) Furthermore, according to Soerjono Soekanto, it is also necessary to increase legal awareness within the community and, indirectly, to improve the attitudes of law enforcement officers (Law Enforcement Officers) toward upholding the law, justice, and protecting human dignity, order, and legal certainty in accordance with the 1945 Constitution of the Republic of Indonesia (UUD NRI 1945) (Soekanto, 1986).The explanation of the Criminal Procedure Code (KUHP) stipulates the principles of Human

Rights, which should serve as guidelines for understanding and interpreting the provisions contained in the articles of the KUHAP. This is often overlooked by law enforcement officials (Djurian, 2025).

In line with the essence and goals of long-term national development, legal development and development are activities and efforts that support, accompany, and direct societal change within the framework of the holistic development of Indonesians and the development of all Indonesian society. These activities and efforts also mean that the future must be a period of legal authority. The law must be well-developed and maintained. It must be authoritative, meaning that respect and obedience to the law are enforced because it truly manifests the aspirations of the people and society. Likewise, law enforcement officers must also be clean and authoritative, meaning they are capable of implementing it and providing services to those seeking justice as fairly as possible based on applicable legal provisions and free from external influences, thus creating a climate of complete order (Bawengan et al., 1989).

The Criminal Procedure Code (KUHAP) itself does not explicitly define coercive measures. However, it can be concluded that coercive measures are actions taken by law enforcement officers to arrest, detain, search, confiscate, inspect documents, etc., against someone suspected of committing a crime. Wiretapping is not actually listed in the KUHAP as a coercive measure under criminal procedure law. This is because wiretapping is essentially a violation of a person's right to privacy. However, wiretapping can be used for certain specific crimes. This is because, under specific criminal laws, wiretapping can be used as a coercive measure to obtain information that will later be used as evidence in court.

In *Criminology, Second Edition (1995)*, Piers Beirne and James Messerschmidt explained that wiretapping cases captured the attention of the American public in the 1970s. At that time, US President Richard Nixon wiretapped the conversations of his political opponents at the Watergate Hotel ahead of the presidential election. Richard Nixon subsequently resigned before being impeached, as the wiretapping was considered a despicable act and a violation of human rights (Watch, 2009). In Indonesia, Article 40 in conjunction with Article 56 of Law Number 36 of 1999 concerning Telecommunications (Law 36/1999) stipulates that any person is prohibited from intercepting information transmitted through telecommunications networks in any form. Anyone who violates the provisions referred to in Article 40 shall be subject to a maximum prison sentence of 15 (fifteen) years. The explanation of Article 40 of Law 36/1999 states that interception is the activity of installing additional devices or equipment on a telecommunications network for the purpose of obtaining information through illegal means.

On the other hand, Article 42 paragraph (2) of Law 36/1999 stipulates that telecommunications service providers may record information sent and/or received by telecommunications service providers and may provide information for the purposes of criminal justice proceedings based on a written request from the Attorney General and/or the Chief of the Indonesian National Police for certain crimes, as well as requests from investigators for certain crimes in accordance with statutory provisions.

Essentially, the information held by a person is a personal right that must be protected, so wiretapping must be prohibited. Information is part of the rights of citizens, which are also protected in Article 28F in conjunction with Article 28G of the 1945 Constitution of the Republic of Indonesia (UUD NRI 1945), which states that everyone

has the right to communicate and receive information to develop their personality and social environment, and has the right to seek, obtain, possess, store, process, and convey information using all available channels. It is also added that everyone has the right to protection of themselves, their family, their honor, their dignity, and their property under their control, and has the right to feel safe and protected from the threat of fear to do or not do something that is a human right (UDHR, 1948).

Wiretapping is an effective technological tool for uncovering systemic crimes, such as corruption, narcotics, organized crime, and other crimes. Wiretapping in English is called "bugging," which means a form of electronic surveillance in the form of electronically capturing, listening to, or recording conversations, usually secretly through electronic devices (Rachmad, 2016). On Black's Law Dictionary, the term "Bugging" is defined as "A form of electronic surveillance by which conversations may be electronically intercepted, overheard, or recorded, Covertly; eavesdropping by electronic means" (Garner, 2004). Amanda Hale and John Edwards further relate wiretapping to "interception" or "wiretapping." Wiretapping generally means secretly listening to another person's conversations through telephone tapping or other electronic interception. Amanda Hale explains that "Interception: a person intercepts a communication in the course of its transmission if, as a result of their interference in the system or monitoring of the transmission, some or all of the contents are made available, while being transmitted, to a person other than the sender or the intended recipient of the communication." (Hale & Edwards, 2006).

The scope of communication wiretapping is divided into several forms: First, individual, targeting only certain individuals (targeted use of offensive technology); Second, targeting individuals within a specific scope (targeted and semi-targeted use of

mobile phone surveillance); and Third, mass surveillance, encompassing a wide network (mass surveillance of network activity). Generally, coercive wiretapping is carried out through this third type of coverage, and ironically, only a few countries clearly regulate its implementation (Hosein & Palwo, 2013).

Regulations regarding the procedures and mechanisms for wiretapping are also still diverse and differ, therefore, it is necessary to standardize the rules regarding wiretapping. Based on Constitutional Court Decision Number 5/PUU-VIII/2010 dated February 2, 2011, the Court considers the need for a specific law that regulates wiretapping in general, including the procedures for conducting wiretapping at each authorized institution. This regulation in law is urgently needed because, to date, there are no appropriate regulations regarding wiretapping, which has the potential to harm the constitutional rights of citizens in general. The single regulation as referred to in Constitutional Court Decision Number 5/PUU-VIII/2010 must contain the following provisions: (1) The existence of an official authority designated in the law, such as a reason or judge for granting permission or authority to conduct, order, or request wiretapping; (2) The categories of legal subjects authorized to conduct wiretapping; (3) The specific purpose of the wiretapping; (4) Wiretapping procedures; (5). A guaranteed timeframe for conducting wiretapping; (6). Restrictions on handling of wiretapping material; (7). Restrictions on who can access the wiretapping; and; (8). Supervision of wiretapping.

The issue of wiretapping by law enforcement officers lies at the intersection of state interests in law enforcement and the right to privacy as a human right. In modern practice, digital communication technology allows the state to conduct extensive communications surveillance for the purposes of investigating crimes such as terrorism, corruption, and

cybercrime. However, this practice is often viewed as a potential violation of individuals' privacy rights because it involves interference with private communications. Previous research has shown that surveillance technology offers benefits in crime prevention and prosecution, but it has also raised serious debates regarding the protection of citizens' privacy rights.(Cindropole & Rosmini, 2024)

Several previous studies have examined the legal aspects of wiretapping in the context of law enforcement. For example, Dewi's research examines lawful interception as a legal mechanism that allows authorities to intercept communications based on statutory provisions. The study emphasized that wiretapping can only be considered legal if it is conducted in accordance with strict legal procedures and has a clear legal basis.(Dewi, 2018) Another study by Aidil Putra Dalimunthe highlighted that wiretapping by law enforcement officers is an effective investigative method for uncovering serious crimes, but also raises controversy because it has the potential to violate citizens' right to privacy, particularly regarding personal lives and correspondence. (Dalimunthe, 2024) In the Indonesian context, Putri, Rahayu, and Lasmadi examined the authority of investigators in conducting lawful interception and found that the regulation of wiretapping is still scattered across various laws, thus not forming a comprehensive regulatory framework regarding the procedures and limits of the authorities' authority.(Putri et al., 2025)

However, most of these studies focus more on analyzing the regulation or legality of wiretapping, rather than on models of privacy protection against coercive wiretapping by law enforcement. Meanwhile, this study not only discusses the legality of wiretapping but also examines the mechanisms for protecting privacy rights as a constitutional limit to coercive state action.

Based on the background presented, there are two problem formulations: Which law enforcement officers have the authority to use coercive measures? What is the mechanism for wiretapping that does not violate human rights?

## **B. METHOD**

This research is a normative legal (Hezron Sabar Rotua Tinambunan et al., 2025) study with a primary focus on the search for primary, secondary, and tertiary legal materials to identify relevant laws and regulations used to assess and determine the extent to which law enforcement officers can engage in coercive wiretapping. This normative legal research is qualitative in nature, referring to legal norms contained in laws and court decisions, as well as prevailing norms within society (Ali, 2009). This research uses a legislative and conceptual approach. The legislative approach is conducted by examining all laws and regulations related to the legal issue being addressed and understanding the hierarchy and principles within these laws and regulations (P. M. Marzuki, 2019). Furthermore, the conceptual approach departs from the views and doctrines that have developed in legal science. (Sabar et al., 2025)

## **A. RESULTS AND DISCUSSION**

### **Wiretapping Mechanism by Law Enforcement Officials Based on Human Rights Protection**

Law and human rights are like two sides of the same coin, inseparable. Law and norms or rules are constructs of values of goodness and truth, intended to protect and uphold that goodness and truth. (Pratama & Yuliani, 2024) Meanwhile, human rights are constructs of human values as creations of God and social beings. Rights that exist naturally or socially are only moral rights. These rights do not yet have any protective

power other than their own moral power. Violations will be morally condemned. These rights only have legal force when they become norms or legal rules containing commands, prohibitions, and sanctions. These rights are binding and must be respected, protected, and enforced by the existing state apparatus (S. Marzuki, 2017).

Wiretapping is a criminal offense, as regulated in Article 285 paragraph (1) of the Criminal Code as follows:

Article 285 of the New Criminal Code:

- (1) Any person who unlawfully listens to, records, diverts, alters, obstructs, and/or records the transmission of electronic information and/or electronic documents that are not public, whether using a cable communication network or a wireless network, shall be punished with a maximum imprisonment of 10 (ten) years or a fine of Category VI.
- (2) Any person who broadcasts or disseminates the results of a conversation or recording as referred to in paragraph (1) shall be punished with a maximum imprisonment of 10 (ten) years or a fine of Category VI.
- (3) The provisions referred to in paragraph (1) do not apply to any person who implements the provisions of statutory regulations or carries out official orders as referred to in Article 31 and Article 32.

Wiretapping under criminal law must be conducted through lawful interception.

This means that the wiretapping and monitoring must be carried out jointly and legally, and carried out by a state institution with the right and authority, as determined by specific regulations, for individuals or groups. For wiretapping to be lawful, it must be based on adequate laws and technical procedures. This guides law enforcement officials to conduct wiretapping within permitted corridors, thus preventing unlawful interception (Widodo et al., 2013).

Several weaknesses in the authority granted by state officials to conduct wiretapping need to be addressed. Regulation of wiretapping must be comprehensive and grounded in the spirit of human rights protection and law enforcement. (Amanda Putri et al., 2024) This is because wiretapping regulations have so far only been contained in regulations, such as internal regulations of law enforcement agencies. Wiretapping

regulations must be placed within a legal framework. Furthermore, laws governing wiretapping for state institutions must emphasize the obligations and limitations of state officials' authority, rather than restrictions on the privacy rights of individuals or citizens (Paripurna et al., 2012).

Clear rules are not solely for the protection of individual privacy; they are more than just to uphold due process of law. Marc Webber Tobias and Roy Davis Peterson, in *\*Pre-Trial Criminal Procedure: A Survey of Constitutional Rights\**, define due process of law as the constitutional guarantee that every citizen has the right to protection against arbitrary government action (Salim et al., n.d.).

### **Wiretapping Authority by Law Enforcement Officials in the Criminal Justice System**

In general, criminal law enforcement efforts are outlined in a series of processes, known as formal criminal law, that begin with the investigation and end with the execution of a legally binding judge's decision (Hamzah et al., 2001). Criminal justice is a system. A simple explanation of this concept is that it begins with a criminal investigation, followed by prosecution, court hearing, and finally, the execution of the verdict. This series is divided into four stages: investigation, prosecution, court hearing, and the implementation of the court decision. Although there are differences in the stages and the law enforcement officers who implement them, they are interdependent and influence each other to produce a common output or product, as is the result of a system. If criminal justice is a system, then the 4 (four) stages are sub system which is the foundation of the system building as expressed below: "A system is an entity that maintains its existence and function as a whole through the interaction of its parts.

Interconnecting parts functioning as a whole. Changed if you take away pieces or add more pieces. If you cut a system in half, you don't get two smaller systems, but a damaged one system that probably won't function. The arrangement of the pieces is crucial. Its behavior depends on the total structure. Change the structure and the behavior changes" (O'Connor & McDermott, 1997).

Even in the context of law enforcement, the granting of wiretapping authority should be strictly limited to avoid the potential for arbitrary use. Therefore, wiretapping must be carried out with great care to ensure that citizens' privacy rights, as guaranteed by the constitution, are not violated. Regarding the actions of law enforcement officers in human rights-based law enforcement, the international principle of Due Process of Law can be referred to. Under Due Process of Law, a criminal process must be controlled to prevent abuse of power and authoritarianism for maximum efficiency. Due Process of Law enforces what is called the Presumption of Innocence, often referred to as the "presumption of innocence," so that law enforcement procedures are synergistic with human rights protection (Bryandono & Beny, 2021).

Wiretapping is essentially a prohibited activity. Some regulations even impose criminal penalties for wiretapping, even the New Criminal Code (KUHP) does so. Despite being a prohibited activity, the authority to conduct wiretapping is granted by law to several state institutions in Indonesia, each with its own specific objectives. There are at least three objectives of wiretapping: first, to maintain and uphold the honor, dignity, and behavior of judges; second, for the benefit of state intelligence; and third, for the benefit of criminal justice (Yuvens, 2017).

Regulations regarding wiretapping are limited to granting authority to law enforcement officers, not to the wiretapping mechanism or the protection of privacy rights

related to wiretapping. Therefore, wiretapping is highly vulnerable to violations of citizens' privacy rights by law enforcement officers. Legislation governing interception or wiretapping in Indonesia is scattered across several laws and regulations. These varying regulations governing the same subject can lead to differing interpretations from the perspectives of law enforcement officers and the public (Manthovani, 2015).

### **Republic of Indonesia National Police (Polri)**

Article 31 paragraph (3) of the ITE Law stipulates that law enforcement officers are authorized to conduct wiretapping for the purposes of resolving legal cases. Except for interceptions referred to in paragraphs (1) and (2), interceptions conducted for law enforcement purposes are permitted at the request of the police, prosecutors, and/or other law enforcement institutions as determined by law. Furthermore, Article 83 of the Criminal Procedure Code also limits investigators' authority to conduct wiretapping. Wiretapping may only be conducted by investigators upon written orders from their superiors after obtaining a permit from the previous examining judge.

At the institutional level, the Regulation of the Chief of the Indonesian National Police No. 5 of 2010 concerning Wiretapping Procedures at the National Police Monitoring Center of the Republic of Indonesia (Perkap 5/2010), based on Law No. 2 of 2002 concerning the National Police (UU 2/2002) and Presidential Decree No. 70 of 2002 concerning the Organization and Work Procedures of the Indonesian National Police (Keppres 70/2002), provides the legal standing for the National Police to conduct wiretapping. Wiretapping must be conducted in accordance with the main principles of human rights protection, legality, legal certainty, consumer protection, participation of

telecommunications service providers, and maintaining the confidentiality of the information obtained.(Tinambunan et al., 2025)

Wiretapping by the Indonesian National Police (Polri) is carried out by the National Police Monitoring Center, which is led by a Daily Chief Executive appointed by the Chief of the Criminal Investigation Unit of the Indonesian National Police (Kabareskrim Polri). Therefore, it can be said that the National Police Monitoring Center is tasked with supporting the implementation of wiretapping duties at the request of investigators, in accordance with all applicable procedures. The Daily Chief Executive reports directly to the Chief of the Criminal Investigation Unit of the Indonesian National Police (Kabareskrim Polri) (Koyongian, 2021).

Based on Article 9 of Regulation 5/2010, requests for wiretapping operations by investigators and/or investigators must be submitted in writing, containing:

- a. The police report number, a brief description of the crime that occurred, including the article suspected, and an explanation containing the intent, purpose, and reasons for conducting the wiretapping operation, including the substance of the information sought;
- b. Telephone numbers/other telecommunications device identifiers and a brief description of the identity of the person to be targeted in the wiretapping operation;
- c. The period/time the wiretapping operation will be conducted, and/or will be conducted, in accordance with the period stipulated in the laws and regulations; and
- d. The name, rank, Main Registration Number (NRP), position, and unit of the investigator designated to liaise with the National Police Monitoring Center,

along with a telephone number and/or email address where they can be contacted.

The Indonesian National Police conduct wiretapping simultaneously with surveillance, as regulated in Article 13 in conjunction with Article 14 of Perkap 5/2010 as follows:

**Table 1**

**Implementation and Supervision of National Police Wiretapping**

Implementation of Wiretapping Operations	Wiretapping Surveillance
<p>(1) The operation begins through provisioning between the National Police Monitoring Center and other telecommunications service providers targeted by the wiretapping operation;</p>	<p>(1) The Head of the National Police Monitoring Center provides information regarding the targets of the wiretapping operation to the Head of the Monitoring Team;</p>
<p>(2) The provisioning referred to in paragraph (1) is carried out by the Official of the System Control and Procedures Sub-Division of the National Police Monitoring Center on the orders of the Head of the National Police Monitoring Center after obtaining permission from the Chief of Criminal</p>	<p>(2) The Head of the Monitoring Team, as referred to in paragraph (1), distributes the wiretapping targets to the monitoring members;</p> <p>(3) The monitoring members referred to in paragraph (1) are required to listen to, read, and record every detail of the</p>

- 
- Investigation of the National Police;
- (3) Wiretapping operations conducted for reasons of extreme necessity and urgency must be reported to the Head of the Criminal Investigation Agency (Kabareskrim) within 24 hours to determine whether the operation is appropriate to continue.
- (4) The Official of the System Control and Procedures Sub-Division of the National Police Monitoring Center, as referred to in paragraph (2), reports the success or failure of the Provisioning between the National Police Monitoring Center and the Telecommunications Service Provider.
- (5) The Head of the National Police Monitoring Center notifies the Investigator and/or Investigator who submitted the request, along with a Minutes of the conversation conducted by the target of the wiretapping operation, and then immediately report it to the Head of the Monitoring Team and/or the Head of the Indonesian National Police Monitoring Center if they find the substance of the information sought.
- (4) The Head of the Monitoring Team and/or the Head of the Indonesian National Police Monitoring Center shall convey the substance of the information sought as referred to in paragraph (3) to the Investigator and/or Investigator who submitted the request.
-

---

commencement of the wiretapping  
operation, of the success or failure  
of the wiretapping operation.

---

### **Attorney General's Office of the Republic of Indonesia (AGO)**

Article 30 C letter i of Law Number 11 of 2021 concerning Amendments to Law Number 16 of 2004 concerning the Attorney General's Office of the Republic of Indonesia (the Attorney General's Office Law) stipulates that the Attorney General's Office has the authority to conduct wiretapping based on a special law governing wiretapping and to establish a monitoring center for criminal offenses. The definition explains that wiretapping is the activity of listening to, recording, diverting, altering, intercepting, and/or recording the transmission of electronic information and/or electronic documents, whether using wired communication networks or wireless networks, such as electromagnetic or radio frequency transmissions, including examining packages, post, correspondence, and other documents.

At the institutional level, the legal standing of the Prosecutor's Office in conducting wiretapping is regulated in the Prosecutor's Office Standard Operating Procedure (SOP) Number: PER-046/A/JA/12/2011 as follows:

- (1) Requests for assistance are executed based on the decision of the case handling controller in the implementing division, whose decision-making procedures are regulated by the Standard Operating Procedures of each division;
- (2) The case handling controller sends a letter requesting assistance addressed to another division no later than 3 (three) working days after the decision, with a copy sent to the supervisory division;
- (3) Requests for assistance as referred to in paragraph (2) include support for: a). Issuance of letters or documents; b). Personnel; c). Information and/or data; d). Infrastructure and/or facilities;
- (4) Requests for assistance as referred to in paragraph (3) include: a). Arrest; b). Detention; c). Confiscation; d). Search; e). Preventive and deterrent measures; f). Wiretapping; g). Capture and escort actions; h). Summons; i). Monitoring

actions; j). Search actions/interviewing fugitives; k). Security and fundraising actions; l). Auction actions for evidence/confiscated objects/found goods or confiscated goods; m). Custody/storage actions for evidence/confiscated objects/found goods or confiscated goods; n). Return actions for evidence/confiscated objects/found goods or confiscated goods; o). Research actions for evidence/confiscated objects/found goods or confiscated goods; p). Search actions and/or salvage of assets of suspects/defendants/convicts; q). Other legal actions;

- (5) The letter requesting assistance referred to in paragraph (2) shall be accompanied by: a). Explanation of the case's position; b). Supporting documents or data; c). Matters required according to the purpose and purpose of the request for assistance;
- (6) Correspondence as referred to in paragraphs (1), (2), (3), (4) and (5) is carried out by the sector requesting assistance with the Technical Officer and Administrative Officer as the responsible parties.

The Prosecutor's Office Standard Operating Procedure (SOP) Number PER-046/A/JA/12/2011 is limited to the investigation stage of general crimes, not corruption (specific crimes). The Prosecutor's Office does not have wiretapping authority in this regard. Only with the revision of Law Number 11 of 2021 concerning Amendments to Law Number 16 of 2004 concerning the Prosecutor's Office of the Republic of Indonesia (the Prosecutor's Office Law) does prosecutors have the authority to wiretap for corruption crimes. However, this provision has shortcomings, namely, it does not fulfill the mandate stipulated in Constitutional Court Decision Number 5/PUU-VIII/2010. Most recently, the Attorney General's Office officially signed a Memorandum of Understanding (MoU) with several telecommunications operators, namely PT. Telekomunikasi Indonesia, Tbk; PT. Telekomunikasi Selular; PT. Indosat, Tbk; and PT XLSmart Telecom Sejahtera, Tbk on Wednesday, June 25, 2025 (Elsam, 2025).

### **Corruption Eradication Commission (KPK)**

In its task of eradicating corruption, the Corruption Eradication Commission (KPK) is granted wiretapping authority based on Article 1 number 5 in conjunction with Article 12 paragraph (1) of Law Number 19 of 2019 concerning the Second Amendment

to Law Number 30 of 2002 concerning the Corruption Eradication Commission (KPK Law), which states that in carrying out its investigative, inquest, and prosecution duties as referred to in Article 6 letter c, the Corruption Eradication Commission has the authority to wiretap and record conversations. Furthermore, the KPK's guidelines for wiretapping are based on Article 9 of the Minister of Communication and Information Regulation Number 11/PER/M.KOMINFO/02/2006 concerning Technical Interception of Information, which stipulates that wiretapping is legal if carried out directly by authorized personnel based on Standard Operating Procedures (SOPs), and that such wiretapping must not disrupt the smooth communication of the person being wiretapped (Laurencia, 2019).

The regulation of wiretapping by the Corruption Eradication Commission (KPK) through Law 19/2019 is considered more advanced than the previous regulations, which were internal to the KPK. This is based on two aspects: First, the legality aspect. The regulation of wiretapping by the KPK is regulated through a law that aligns with the provisions of Law 12/2011 and Article 28J of the 1945 Constitution of the Republic of Indonesia, which is appropriate for regulating restrictions or reductions on human rights. Second, there have been additions and improvements to the substance, although they are far from ideal from a legal and human rights perspective. At the very least, it includes the licensing mechanism, wiretapping period, reporting, and destruction of wiretapping results that are not related to the main case (Suntoro, 2020). The licensing mechanism is regulated in Article 12B of Law 19/2019, which stipulates that wiretapping must be carried out after obtaining written permission from the Supervisory Board. Permission is granted upon a written request from the KPK leadership. Written permission from the Supervisory Board is then granted upon a written request from the KPK leadership. The

Supervisory Board can grant written permission for wiretapping requests within 24 hours of the request being submitted. This mechanism was subsequently overturned by Constitutional Court Decision No. 70/PUU-XVII/2019, meaning that the KPK leadership no longer requires written permission from the Supervisory Board to conduct wiretapping; instead, it is sufficient to notify the KPK Supervisory Board of the wiretapping, search, and seizure.

The wiretaps used by the Corruption Eradication Commission (KPK) to uncover corruption cases are based on provisions regarding valid evidence, which then determine the strength of that evidence. Wiretaps conducted by the KPK are considered indicative evidence as defined in Article 26A of Law 31/1999 in conjunction with Law 20/2001. Wiretaps conducted by the KPK only have value or utility if they meet two requirements. First, the information obtained must be natural evidence; second, the substance of the information must be relevant to the case being handled or to be handled. Natural information means that at the time of the wiretapping, the party being wiretapped is completely unaware that their conversation is being tapped. The prerequisite for obtaining natural information is that the wiretapping must be independent and confidential. Independence means that KPK auditors or investigators must be free from interference from other parties. In investigative audits, auditors, using their intuition and instincts, should be given the freedom to determine who should be tapped and when. This is likely what has led some parties to consider it a human rights violation (Laia, 2020).

### **State Intelligence Agency (BIN)**

Article 31 letter b of Law Number 17 of 2011 concerning State Intelligence (Law 17/2011) states that the State Intelligence Agency (BIN) has the authority to conduct

wiretapping, examine the flow of funds, and gather information on targets related to activities that threaten national interests and security, including ideology, politics, economics, social affairs, culture, defense and security, and other sectors of public life, including food, energy, natural resources, and the environment, and/or terrorism, separatism, espionage, and sabotage activities that threaten national safety, security, and sovereignty, including those undergoing legal proceedings. The State Intelligence Agency's (BIN) authority to conduct wiretapping is further regulated by the limitations of Article 32 of Law 17/2011. Wiretapping is carried out on targets with indications as referred to in Article 31, subject to the following provisions: a). For the purpose of carrying out intelligence functions; b). Upon the order of the Head of the State Intelligence Agency; and c). The wiretapping period is a maximum of 6 (six) months and can be extended as needed. Wiretapping of targets that have been legally established as sufficient preliminary evidence is carried out by a determination by the Chief Justice of the District Court based on Article 26 of Law Number 15 of 2003 concerning Terrorism (Law 15/2003).

The Chief Justice's determination of the validity of the intelligence report as sufficient preliminary evidence is a form of the investigating judge's oversight function in determining the validity of the intelligence report as supporting evidence for initiating a terrorism investigation (Kaligis, 2001). The explanation of Article 26 of Law 15/2003 states that an intelligence report is preliminary evidence to suspect a crime, indicating that a person, due to their actions or circumstances, based on preliminary evidence, is reasonably suspected of being the perpetrator of a terrorist act. Based on this, Article 26 paragraphs (1) and (2) of Law 15/2003 state that intelligence reports can only be direct information reports that have been approved by the Head of the State Intelligence Agency.

The use of such intelligence reports must be based on a determination that sufficient preliminary evidence has been obtained, and an examination by the Chief Justice of the District Court must be conducted. This is intended to verify and clarify the intelligence report. Therefore, the examination process is only conducted on intelligence documents. Article 27 of Law 15/2003 states that evidence for the investigation of terrorism crimes includes:

- a. Evidence as referred to in criminal procedure law;
- b. Other evidence in the form of information spoken, sent, received, or stored electronically using optical devices or similar devices; and
- c. Data, recordings, or information that can be seen, read, and/or heard, and that can be retrieved with or without the aid of a device, whether written on paper, any physical object other than paper, or recorded electronically, including but not limited to: 1). Writing, sound, or images; 2). Maps, designs, photographs, or similar materials; 3) Letters, signs, numbers, symbols, or perforations that have meaning or can be understood by a person who is able to read or understand them.

#### **National Narcotics Agency (BNN)**

Article 75, letters h, i, and j of Law Number 35 of 2009 concerning Narcotics (Law 35/2009) regulates the authority of the National Narcotics Agency (BNN) to conduct investigations, conduct interdictions against the illicit trafficking of narcotic precursors throughout national jurisdiction, and conduct wiretapping related to the abuse and illicit trafficking of narcotics and narcotic precursors after sufficient initial evidence has been obtained, and to employ investigative techniques such as undercover purchases and

supervised deliveries. The explanation to Article 75, letter i, states that wiretapping is an activity or series of investigative activities conducted by BNN investigators or investigators from the Indonesian National Police using electronic devices in accordance with technological advances for the recording and/or sending of messages via telephone or other electronic communication devices. Wiretapping includes electronic monitoring by, among other means:

- a. Installing a transmitter in the target room to listen to/record all conversations (bugging);
- b. Installing a transmitter in a car, person, or object whose location can be tracked (bird-dog);
- c. Internet interception;
- d. Cloning pagers, short message service (SMS), and faxes;
- e. Closed-Circuit Television (CCTV);
- f. Direction finder

Wiretapping by the National Narcotics Agency (BNN), based on Article 77 paragraph (2) of Law Number 35 of 2009, stipulates that wiretapping must be carried out after obtaining written permission from the Chief Justice of the District Court. However, in urgent circumstances, wiretapping may be carried out without prior written permission from the Chief Justice of the District Court, provided that the BNN investigator must request written permission from the Chief Justice of the District Court within 24 hours.

Based on Decree of the House of Representatives of the Republic of Indonesia (DPR RI) Number 8/DPR RI/II/2021-2022 concerning the National Legislation Program for Priority Bills for 2022 and the National Legislation Program for the Third Amendment to the Draft Law for 2020-2024, dated December 7, 2021, the Draft Law on Wiretapping

is included in the 2019-2024 National Legislation Program List, but is not included in the list of Priority Bills for 2022.

## **B. CONCLUSION**

Wiretapping is a criminal offense. However, there are justifications for wiretapping when used by law enforcement officers in criminal proceedings. Wiretapping is considered a coercive measure not regulated in the Criminal Procedure Code (KUHAP). Wiretapping is used in line with developments and advancements, especially in technology. Criminal acts are becoming increasingly complex and diverse, significantly impacting the law enforcement process. Wiretapping authority is granted to several state institutions in Indonesia, namely the Police, the Prosecutor's Office, the Corruption Eradication Commission (KPK), the State Intelligence Agency (BIN), and the National Narcotics Agency (BNN) in law enforcement. To date, Indonesia does not have a law specifically governing wiretapping.

As a basis for future improvements, the regulation regarding the process of granting wiretapping permits must be regulated as strictly as possible in a special regulation (preferably in the form of a law) to specifically state the limitations of wiretapping and its permissibility in relation to specific crimes. Furthermore, the granting of wiretapping permits is not merely an administrative requirement; the application must also state the urgency of the wiretapping and the extent to which it will be used. Furthermore, because wiretapping is part of the criminal investigation process, it can be included as an item that can be submitted for pretrial if the wiretapping is conducted outside of the scope of applicable laws.

## **REFERENCE**

- Ali, Z. (2009). *Metode Penelitian Hukum*. Sinar Grafika.
- Amanda Putri, N. G., Dea Avita, F., & Vindi Putri, H. J. (2024). Perlindungan Hak Asasi Manusia Dalam Konteks Hukum. *Indonesian Journal Of Legality Of Law*, 1(2), 1–13.
- Bawengan, G. W., Interogasi, P. P. P. D. T., Ketiga, C., Paramita, P., & Jakarta. (1989). *Penyidikan Perkara Pidana Dan Teknik Interogasi* (Cetakan Ke). Pradnya Paramita.

- Bryandono, & Beny. (2021). Legalitas Penyadapan Oleh Jaksa Dalam Penanganan Perkara Tindak Pidana Korupsi. *Jurnal Hukum Pidana & Krimonologi*, 3(1).
- Cindropole, A. C., & Rosmini, S. (2024). The Legal And Ethical Implications Of Surveillance In Criminal Law: A Literatur Review. *EScience Humanity Journal*, 4(1), 452.
- Dalimunthe, A. P. (2024). Legalitas Praktik Metode Penyadapan Terhadap Pelaku Tindak Pidana Korupsi Dalam Ketentuan Hukum Tindak Pidana Korupsi. *Al-Qanun: Jurnal Kajian Sosial Dan Hukum Islam*, 5(2), 83.
- Dewi, S. (2018). Privacy: An Overview of Indonesia Statutes Governing Lawful Interception. *Central European Journal of International and Security Studies*, 12(4), 586–597.
- Djurian, J. D. et. a. (2025). *Sistem Peradilan Pidana Dalam Penegakan Hukum Sebagai Perwujudan Hak Asasi Manusia* (Vol. 13, Issue 3).
- Elsam. (2025). *Kejaksanaan Agung Teken MoU Penyadapan dengan Operator Telekomunikasi, Privasi Warga Dikorbankan atas Nama Penegakan Hukum*.
- Garner, B. A. (2004). *Black's Law Dictionary*, St. Paull Thomson.
- Hale, A., & Edwards, J. (2006). Getting Its Taped. *Computer and Communications Law Review*.
- Hamzah, A., Indonesia, H. A. P., Revisi, E., Grafika, S., & Jakarta. (2001). *Hukum Acara Pidana Indonesia* (Edisi Revi). Sinar Grafika.
- Hezron Sabar Rotua Tinambunan, Istislam, Hadiyantina, S., Kusumaningrum, A., & Tajudin, A. A. (2025). Recentralization of Mining Licensing Authority and Its Impact on Local Autonomy in Indonesia. *Jurnal Suara Hukum*, 7(2), 533.
- Hosein, G., & Palwo, C. W. (2013). Modern Safeguards For Moders Surveillance: An Analysis of Innovations in Communications Surveillance Techniques". *Ohio State Law Journal*, 76(6).
- Kaligis, O. C. (2001). *Perlindungan Hukum Atas Hak Asasi Tersangka, Terdakwa dan Terpidana*.
- Koyongian, R. R. (2021). Penyadapan Oleh Penyidik Dalam Upaya Pemberantasan Tindak Pidana Korupsi". *Lex Privatum*, 9(8).
- Laia, F. (2020). Penyadapan Yang Dilakukan KPK Dalam Perspektif Hak Asasi Manusia Di Indonesia". *Jurnal Education and Development*, 8(3).
- Laurencia, T. (2019). Penyadapan Oleh KPK Dalam Perspektif Due Prooess of Law". *Jurnal Mercatoria*, 12(2).
- Manthovani, R. (2015). *Penyadapan vs Privasi, Bhuana Ilmu Populer*.
- Marzuki, P. M. (2019). PENELITIAN HUKUM. *Edisi Revisi. Prenadamedia Grup*.
- Marzuki, S. (2017). *Hukum Hak Asasi Manusia*. Pusham UII.
- O'Connor, J., & McDermott, I. (1997). *The Art of Systems Thinking, Essential Skills for*

*Creativity and Problem Solving, Thorson.*

- Paripurna, A., Purwoleksono, D. E., Korupsi, M. K. P. B. H. A. M. D. P. T. P., & Anggaran, L. H. P. H. B. T. (2012). *No Title*. Universitas Airlangga.
- Pratama, W. A., & Yuliani, A. N. (2024). Hukuman Mati Bagi Bandar Narkotika Dalam Perspektif Hukum dan Ham. *Realism: Law Review*, 2(3), 200–218.
- Putri, E. A., Rahayu, S., & Lasmadi, S. (2025). Tindakan Lawful Interception oleh Penyidik dalam Penegakan Hukum. *PAMPAS: Journal of Criminal Law*, 6(3), 329.
- Rachmad, A. (2016). Legalitas Penyadapan Dalam Proses Peradilan Pidana di Indonesia". *Jurnal Hukum Samudera Keadilan*, 11(2).
- Reza, M. H. M., & Kamila, S. (2025). Chemical Castration Punishment: an International Human Rights Law Perspective. *Realism: Law Review*, 3(1), 18–30. <https://doi.org/10.71250/rlr.v3i1.54>
- Sabar, H., Tinambunan, R., Istislam, Hadiyantina, S., Kusumaningrum, A., & Nte, N. D. (2025). Governance of Mineral and Coal Mining Permits : Legal Dynamics in Indonesia and Nigeria. *Diponegoro Law Review*, 10(2), 234–253. <https://doi.org/10.14710/dilrev.10.2.2025.234-253>
- Salim, H., Kurnia, M., & Azhari, N. D. (n.d.). Analisis Keabsahan Penyadapan Yang Dilakukan Oleh Komisi Pemberantasan Korupsi Tanpa Izin Pengadilan". *ADIL: Jurnal Hukum*, 9(2).
- Soekanto, S. (1986). *Pengantar Penelitian Hukum*. UI Press.
- Suntoro, A. (2020). Penyadapan dan Eksistensi Dewan Pengawas Komisi Pemberantasan Korupsi. *Jurnal Legislasi Indonesia*, 17(1).
- Tinambunan, H. S. R., Kusuma, F. I. S., Permatasari, V. A., Sugiarto, A. F., & Tajudin, A. A. (2025). Legal Protection Policy for the People in Handling Covid-19: A Comparison of Indonesia and Australia. *Realism: Law Review*, 3(1), 31–43. <https://doi.org/10.71250/rlr.v3i1.55>
- UDHR. (1948). *Article 12 Universal Declaration of Human Right (UDHR) 1948*.
- Watch, I. C. (2009). *Penyadapan dalam Hukum Pidana*.
- Widodo, S., Napitupulu, E. A. T., & KUHAP, K. A. P. P. D. R. (2013). *Institute for Criminal Justice Reform*.
- Yuvens, D. A. (2017). Dilema Upaya Hukum Terhadap Penyadapan". *Jurnal Hukum & Pembangunan*, 47(3).