

Reimagining Wiretapping: Ensuring Fairness in the Law Enforcement Process

Mohamad Mahdy

Faculty of Law, Universitas Sebelas Maret, Indonesia
mohamad.mahdy@student.uns.ac.id

Hartiwiningsih

Faculty of Law, Universitas Sebelas Maret, Indonesia

Isharyanto

Faculty of Law, Universitas Sebelas Maret, Indonesia

Abstract:

Wiretapping plays a crucial role in the detection of criminal activities such as corruption, terrorism, and drug trafficking. However, inconsistencies and the absence of comprehensive norms in wiretapping regulations in Indonesia present significant legal challenges. The ambiguity surrounding the legitimacy of authority granted to law enforcement agencies creates the potential for abuse of power and infringes upon citizens' privacy rights. Additionally, legal uncertainties regarding the admissibility of evidence obtained through wiretapping can undermine the integrity of the criminal justice process. This study aims to develop a model for wiretapping regulations that ensures fairness in the law enforcement process. The research employs a doctrinal approach, utilizing both statutory and conceptual analysis. The findings suggest that a well-defined legal framework is essential to ensure wiretapping is conducted in accordance with legal standards and the principle of due process. Furthermore, a robust system of checks and balances must be established to prevent the abuse of authority, through clear limitations on the scope of wiretapping powers.

Keywords: wiretapping; law enforcement; fairness; criminal justice.

Introduction

The rapid advancement of technology has significantly influenced the modus operandi of criminal activities, particularly those involving digital tools (Franssen and Tosza 2025; Kulshrestha 2022). In response to the evolving nature of crime, wiretapping has emerged as one of the more effective investigative methods for uncovering and resolving criminal cases. It serves as a means of obtaining evidence that can substantiate criminal allegations. As a technologically driven investigative technique, wiretapping plays a crucial role in crime detection. When employed against organized and complex crimes—such as corruption, narcotics trafficking, and other serious offenses—wiretapping, alongside countermeasures against anti-surveillance tactics, proves to be especially valuable (Diffie and Landau 2008). In this context, individuals involved in serious criminal conduct can be prosecuted, with wiretapping evidence serving as a key component in legal proceedings.

Wiretapping can serve as a crucial instrument for detecting criminal activity, addressing serious and extraordinary crimes, and combating new and technologically sophisticated forms of criminal conduct. It also plays a role in safeguarding national defense and security, preventing large-scale criminal acts, and monitoring communications that may threaten public order or moral standards. However, the increased reliance on wiretapping—particularly in the context of combating corruption and terrorism—has significantly influenced its practice and, in many cases, has led to a reduction in the protection of individual privacy rights. (Theacornelia and Latifah 2022).

In principle, communication tapping is prohibited by law. However, exceptions are made when wiretapping is conducted for the purpose of law enforcement, typically at the request of a prosecutor or another law enforcement agency authorized by law. Consequently, wiretapping must be carried out in accordance with the principle of equality before the law, ensuring that it is applied fairly and without discrimination (Purwadi et al. 2022; Sakti, Aprianingsih, and Nufus 2022). This principle guarantees the rights of citizens who are the subjects of wiretapping, requiring law enforcement officers to uphold and implement it within national governance. Failure to adhere to this principle constitutes a violation of the constitution. Although such violations may not always appear overt, the public is acutely aware that legal inequality leads to prolonged emotional distress (Isharyanto and Lestari 2020). Therefore, it is essential for authorities and law enforcement to provide guarantees that citizens' rights will not be infringed upon through misuse of wiretapping powers (Stoykova 2023).

The implementation of wiretapping remains a contentious issue, with debates surrounding the clarity of its legal basis, the authority to conduct wiretapping, and concerns over privacy violations. Interception is widely viewed as an infringement on human rights, particularly the right to privacy in communication. In the context of Supreme Court Decision No. 1429 K/Pid/2010, in conjunction with Decision No. 117 PK/Pid/2011, the leadership of the Corruption Eradication Commission was accused of violating the Interception Law. Additionally, the Constitutional Court has recognized that wiretapping constitutes a violation of the right to privacy, contravening the 1945 Constitution of the Republic of Indonesia. Although the right to privacy is a fundamental human right, it is subject to certain limitations. However, any restrictions on this right must comply with legal provisions, as outlined in Article 28J, Paragraph 2 of the Indonesian Constitution, which stipulates that such limitations cannot contravene the law.

As criminal activities become increasingly complex, the use of wiretapping has gained prominence, particularly in conjunction with technological advancements. This method has proven to be highly effective in detecting sophisticated crimes, making the regulation of wiretapping a critical component of legal procedures. It must be acknowledged that wiretapping can play a pivotal role in uncovering criminal activities. Law enforcement agencies often rely on wiretapping as part of their investigative efforts, as detecting such crimes can be challenging. The evidence obtained from wiretapping is admissible in court, despite the fact that, under traditional evidentiary laws, recorded conversations were not initially accepted as

evidence. However, as criminal law has evolved, so too have the methods of proving difficult-to-detect crimes. Today, wiretapping results, which are stored as recorded conversation data, are recognized as valid evidence, provided they adhere to the standards for electronic data and other forms of admissible evidence (Surya Atmaja 2019).

Indonesia currently lacks a unified regulation governing wiretapping procedures, which creates vulnerabilities regarding the surveillance of citizens' private communications, including internet-based communications such as email and various social media platforms. The Constitutional Court, in its ruling, emphasized that, from the perspective of criminal law reform, there is a need for the establishment of specific legislation that addresses wiretapping comprehensively, taking into account existing regulations. The term "special" in this context refers to a standalone law that exclusively governs wiretapping activities. However, Indonesia currently has at least twelve separate laws and regulations that address wiretapping in various ways, leading to a confusing and often overlapping regulatory framework. This lack of clarity has posed a significant threat to human rights, particularly the right to privacy.

In addition to the absence of a cohesive regulatory framework, there remains an ongoing issue with the uncertainty surrounding the authority to conduct wiretapping. Given the complexity of the issue, it is imperative that clear and unambiguous regulations be put in place to define and regulate wiretapping authority (Hafizhah, Leviza, and Mulhadi 2024). Additionally, there is significant uncertainty regarding which individuals or institutions are authorized to conduct wiretapping. This ambiguity has led to complications in the granting of wiretapping authority, as outlined in various laws and institutional regulations, resulting in overlapping legal frameworks and disputes over jurisdiction. These issues have, in turn, triggered extensive litigation and challenges to the legality of wiretapping procedures due to the lack of clear legal definitions. The absence of a legitimate and well-defined framework for wiretapping represents a critical concern in a rule-of-law system.

Given that wiretapping can potentially infringe upon human rights—particularly the right to privacy—its use must be approached with utmost caution to prevent misuse or arbitrary actions by law enforcement agencies (Amir et al. 2023). Therefore, it is essential to establish clear procedures and limitations regarding wiretapping authority. These procedures and limitations must be defined by laws that ensure legal certainty while safeguarding citizens' privacy rights. To address this, the scope of wiretapping authority should be firmly, clearly, and measurably regulated. For instance, the authority to conduct wiretapping by prosecutors should be strictly confined to law enforcement purposes. Without such limitations, there is a risk of power abuse, with wiretapping potentially being justified under the guise of law enforcement (Slamet Riyadi 2022). This concern is particularly pressing given the absence of specific laws and regulations governing wiretapping. The lack of legal clarity could lead to uncertainty regarding the authority to conduct wiretapping and the admissibility of wiretap-derived evidence in legal proceedings.

Previous research by (Kalumata and Kirana 2025), found that the regulation of wiretapping remains fragmented and lacks a dedicated legal framework. This study differs from theirs by not only advocating for the creation of a special law but

also emphasizing the legitimacy of wiretapping authority, with particular attention to human rights considerations. In another study, (Taufik et al. 2024) noted that, in the context of countering terrorism, wiretapping is recognized as valid evidence if conducted pursuant to a court order or specific legal procedures. While this study also highlights the importance of legitimacy and human rights, it specifically focuses on terrorism-related cases.

Similarly, local research by (Kusuma, Sihotang, and Saputra 2025) pointed out the dual nature of wiretapping, recognizing it as both a valuable law enforcement tool and a potential violation of individual privacy rights, particularly in the case of police wiretapping in Bali. In the broader context of criminal justice, the law serves to resolve conflicts, uphold truth and justice, and regulate society. This study aims to propose a model for regulating wiretapping that prioritizes justice and equality before the law, ensuring the protection of privacy rights and safeguarding against unlawful wiretapping of communication devices.

Result and Discussion

Absence of Norms and Conflict of Wiretapping Norms

Regulations regarding wiretapping are contained in several laws. There are at least 12 (twelve) laws that regulate wiretapping, namely the Psychotropic Law, Telecommunications Law, Corruption Law, Corruption Eradication Commission Law, Advocate Law, Human Trafficking Law, Electronic Information and Transactions Law, Narcotics Law, Corruption Court Law, Citizenship Law, Money Laundering Law, and Judicial Commission Law.. The twelve laws only regulate the authority to carry out wiretapping, while formal law as a form of material law enforcement regarding wiretapping is not regulated in these regulations. Therefore, the formal law still refers to the provisions in the Criminal Procedure Code. The regulations regarding wiretapping are still partial or still at the needs of each law enforcement institution, which should be regulated in one law that specifically regulates wiretapping so as not to give rise to multiple interpretations regarding the wiretapping mechanism.

Wiretapping is a means of gathering evidence in the trial process. Evidence of wiretapping can be in the form of electronic evidence. Evidence plays a significant role in law enforcement because by having evidence, an incident can be revealed. Evidence is the provision that contains the procedures for proving the guilt of the accused, and it is also a provision that regulates evidence that is permitted by law. (Febriani, Haryadi, and Rakhmawaty 2021). Wiretapping in law enforcement has significant implications for several agencies, including the police, prosecutors, the Corruption Eradication Commission, and the National Narcotics Agency. For the police, wiretapping is a vital tool in uncovering serious crimes such as terrorism, cybercrime, and drug trafficking. Prosecutors, as key players in the prosecution process, also rely on wiretapping results as evidence in trials, particularly in cases where it is challenging to gather sufficient evidence through witnesses or conventional methods. In such cases, wiretapping can expedite investigations and strengthen charges against offenders.

The Corruption Eradication Commission, in particular, uses wiretapping as a central strategy in combating corruption, as many acts of bribery and illicit gratification occur in secret and are challenging to detect without communication

recordings. However, using wiretapping by the Corruption Eradication Commission is often controversial, as it is perceived to infringe on privacy rights, necessitating stringent oversight of its regulations. Similarly, the National Narcotics Agency heavily depends on wiretapping to dismantle drug trafficking networks both nationally and internationally. By intercepting communications among perpetrators, the BNN can trace drug distribution routes and apprehend major dealers who are otherwise difficult to target. While wiretapping is effective across various institutions, it must always be balanced with appropriate oversight to prevent abuses of power.

The authority to conduct wiretapping is granted to specific law enforcement agencies under various laws: (a) According to Law No. 15 of 2003, which stipulates the Government Regulation instead of Law No. 1 of 2002 concerning the Crime of Terrorism, police investigators are authorized to conduct wiretapping, but it requires approval from the Chief Justice and is limited to a maximum duration of one year; (b) Under Law No. 12 of 2007 on the Eradication of Human Trafficking, police investigators are also granted wiretapping authority; (c) Law No. 35 of 2009 on Narcotics grants wiretapping authority to BNN and POLRI investigators, with or without Chief Justice approval, as outlined in Articles 75, 77, and 78; (d) Law No. 17 of 2011 concerning State Intelligence grants wiretapping authority to the National Intelligence Agency (BIN); and (e) According to Article 12(a) of Law No. 30 of 2002 concerning the Corruption Eradication Commission, the Corruption Eradication Commission is authorized to conduct wiretapping.

The procedural law governing interception procedures has yet to be fully finalized. However, numerous laws and regulations grant interception authority to law enforcement officers, creating a need for clear procedural guidelines to ensure the proper implementation of such authority. Currently, law enforcement officers' regulation of the technical procedures for interception is based on the Regulation of the Minister of Communication and Information No. 11/PERM.KOMINFO/02/2006 outlines that lawful interception is conducted for the investigation, prosecution, and trial of a criminal act, as stated in Article 3. Based on the authority granted by this regulation, the National Police have established a guideline for investigators through the Regulation of the Chief of Police No. 5 of 2010, which explicitly addresses wiretapping procedures at the National Police Monitoring Center.

Additionally, according to Sulistyo, Deputy for Cyber Security and Government Codes and Human Development, strict supervision is essential from the outset of wiretapping procedures. Prior to conducting wiretapping, law enforcement agencies are required to obtain permission from the relevant authority. The licensing mechanism and procedures must be rigorously regulated to prevent haphazard use of wiretapping authority. The authority granted to prosecutors to carry out wiretapping also requires comprehensive regulation, including apparent limitations on its use, defined procedures, and the involvement of relevant institutions in the execution of wiretapping. To address these concerns, the House of Representatives (DPR) and the government must finalize the preparation and discussion of the Wiretapping Bill. The creation of this Bill is a mandate from three Constitutional Court rulings that collectively reinforce the need for such legislation, including Constitutional Court Decision No. 006/PUU-I/2003, Constitutional

Court Decision No. 012-016-019/PUU-IV/2006, and Constitutional Court Decision No. 5/PUU-VIII/2010.

According to Constitutional Court Decision No. 5/PUU-VIII/2010, wiretapping is considered a violation of privacy rights, which contradicts the provisions of the 1945 Constitution. Privacy rights are part of human rights, and although they are fundamental, they can be subject to limitations (derogable rights) under specific circumstances (Alibeigi, Munir, and Karim 2019). However, restrictions on privacy rights can only be imposed by law, as stipulated in Article 28J, paragraph (2) of the 1945 Constitution. This was further emphasized in Constitutional Court Decision No. 20/PUU-XIV/2016, which affirmed that, in the context of protecting human rights, all wiretapping activities are prohibited as they violate the constitutional rights of citizens, particularly the right to privacy in communication as guaranteed by Article 28F of the 1945 Constitution. Even within the scope of law enforcement, the granting of wiretapping authority should be strictly limited to prevent the potential for arbitrary surveillance.

Consequently, wiretapping must be conducted with utmost caution to ensure that citizens' privacy rights, as guaranteed by the 1945 Constitution, are not infringed upon. In relation to law enforcement actions, the principles of human rights can be guided by the international standard of Due Process of Law, which ensures legal procedures are followed in accordance with human rights protections (Solum and Crema 2022). In the context of due process, the criminal justice process must be regulated to prevent the abuse of power and authoritarian practices, while maximizing efficiency. Due process enforces the principle of the "presumption of innocence," ensuring that individuals are treated as innocent until proven guilty. This principle helps ensure that legal procedures are designed in a way that aligns with the protection of human rights (Diffie and Landau 2007).

Concerning the privacy of citizens' data, Article 1, number 27 of the Law on Information and Electronic Transactions and the Minister of Communication and Informatics Regulation No. 20 of 2016, which addresses the Protection of Personal Data in Electronic Systems, defines "Personal Data" as any individual data that is stored, maintained, and protected for confidentiality. "Certain Personal Data" refers to any accurate and identifiable information directly or indirectly linked to an individual whose use must comply with applicable laws and regulations. The personal data owner is the individual to whom this data is attached.

It is anticipated that various laws across multiple sectors will address the obligation to protect individuals' rights, including provisions that prohibit unlawful interception of communications and require data collectors to safeguard the confidentiality of the personal data they collect. Specifically, Article 26 of Law No. 11 of 2011, concerning Electronic Information and Transactions, stipulates that an individual's personal data may not be transferred arbitrarily without the data owner's consent. There are at least 32 laws that contain provisions related to the regulation of citizens' data. Most of these laws grant authority to both public (government) and private entities to collect and manage personal data, including the authority to conduct intrusions under certain exceptions. The sectors regulated by these laws are diverse, covering areas such as telecommunications, finance and banking, taxation, population management, archiving, law enforcement, security, and the health sector.

Law enforcement officials will not engage in wiretapping indiscriminately. The potential for misuse of data when wiretapping is conducted without adherence to Law No. 27 of 2022 concerning the Protection of Personal Data poses significant risks of human rights violations. Wiretapping may be carried out for law enforcement or national security, but it must follow a strict procedure to prevent arbitrary actions. Wiretapping involves installing additional tools or devices on a telecommunications network to obtain information illicitly. As the information owned by an individual is considered a personal right, it must be protected, and wiretapping is, therefore, prohibited. The prohibition on wiretapping is outlined in Article 40, and its explanation is in Law No. 36 of 1999 concerning Telecommunications. Furthermore, the penalty for wiretapping is a maximum imprisonment of 15 years, as stipulated in Article 56 of the Telecommunications Law. The lack of specific legal norms regulating wiretapping, coupled with the varied regulations governing the authority to conduct it, creates a legal loophole that may infringe upon the human rights of civilians during the legal process.

Formulating Ideal Legal Provisions for Wiretapping

Fundamentally, rights are categorized into two types: rights that can be limited (derogable rights) and rights that cannot be limited (non-derogable rights). According to Article 4 of the Human Rights Law, non-derogable rights include the right to life, the right not to be subjected to torture, the right to personal liberty, freedom of thought and conscience, the right to religion, the right not to be enslaved, the right to recognition as a person before the law, and the right not to be prosecuted based on retroactive laws. The right to privacy, however, is considered a personal right that falls under derogable rights (Shehu and Shehu 2023).

This is explicitly articulated in the Telecommunications Law, specifically in the explanation of Article 40, which asserts that information owned by an individual is a personal right that must be protected. Consequently, the right to privacy is one of the fundamental rights that must be safeguarded. Article 28J, paragraph (2) of the 1945 Constitution stipulates that any restrictions on the exercise of a person's rights and freedoms must be prescribed by law. Thus, special regulations regarding wiretapping actions, as stipulated in legislation, are necessary. While Indonesia has enacted laws that regulate wiretapping actions, these regulations are not yet comprehensive. Furthermore, the existing norms do not fully reflect the principles of respect for human rights as outlined in the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) (Lubin 2020). Indonesian law regulates interception authority and fulfills the principle of legality, but it does not apply the due process of law principle. This suggests that Indonesia operates primarily based on law or rule by law, which does not guarantee that activities are free from government intervention or interference. A law that fails to incorporate good moral standards and respect for human rights is prone to misuse.

Compliance with due process for wiretapping in Indonesia only addresses the principles of legality and legitimate aim. However, this only pertains to the legality of the law's material form and does not extend to its formal application. Therefore, Indonesian legislation regulating interception fails to meet the standards of human rights protection and is susceptible to misuse by certain parties for specific interests.

A critical issue that requires further examination is why interceptions governed by Indonesian legislation that does not fully respect human rights still allow the results, such as recorded conversations or other forms of communication, to be accepted as valid evidence in the criminal justice system. While wiretapping is regulated by the Criminal Procedure Code (KUHAP), the existing regulations are limited and lack detail, particularly concerning law enforcement officers' procedures and oversight of wiretapping actions (Febryan Alam Susatyo and Muksin 2024).

To better understand this issue, it is essential to examine relevant points from the Criminal Procedure Code and other regulations governing wiretapping in Indonesia. One significant change in the Draft Criminal Procedure Code involves the introduction of a new institution, the Preliminary Examining Judge, which replaces the pretrial system. The pretrial institution, unique to the Criminal Procedure Code, proved ineffective as it remained passive, waiting for the parties to initiate lawsuits. Moreover, it was not an independent body, as the head of the district court appointed a judge to serve as the pretrial judge upon receiving a request. The concept of the Preliminary Examining Judge differs from the pretrial system but is not identical to the *rechtercommissaris* in the Netherlands or the *juge d'instruction* in France. The Preliminary Examining Judge, as outlined in the Draft Criminal Procedure Code, does not lead investigations. It represents revitalizing the existing pretrial institution within the current Criminal Procedure Code. In this sense, it bears similarities to the *Giudice per le indagini preliminari* in Italy, especially after Italy abolished the *Giudice Istruttore*, which is akin to the *juge d'instruction* in France and the *rechtercommissaris* in the Netherlands.

The role of the *Giudice per le indagini preliminari*, who oversees investigations and prosecutions, is similar to that of the Preliminary Examining Judge in the Draft version of the Criminal Procedure Code. Some of the authorities traditionally held by District Court judges, such as issuing search warrants, authorizing seizures, approving wiretaps, and extending detention, would now be transferred to the Preliminary Examining Judge. This transfer of authority aims to expedite the process and alleviate the burden on district court judges, who are otherwise engaged in criminal, civil, and other case hearings. The Academic Manuscript of the Draft Criminal Procedure Code states that the authority to extend detention, for example, would shift from 40 days to 25 days under the jurisdiction of the Preliminary Examining Judge.

An essential institution to consider between the public prosecutor and the judge is the Preliminary Examining Judge, as proposed in the Draft Criminal Procedure Code. In the discussion section, the differences between the *Rechtercommissaris* in the Netherlands and the *Juge d'instruction* in France will be highlighted, particularly in contrast to the Preliminary Examining Judge introduced in the Draft Criminal Procedure Code. Several issues arise in the relationship between investigators and public prosecutors, which are regulated within an integrated justice system that should ideally function cohesively. However, this system has often been disjointed, leading to a back-and-forth of case files between investigators and public prosecutors, resulting in many cases being delayed or lost altogether.

Wiretapping is introduced in the Draft with stringent requirements. According to Article 83, paragraph (1), wiretapping of conversations via telephone or other

telecommunications devices is prohibited, except when the conversations are related to serious crimes or when there is strong suspicion that serious crimes will occur, which cannot be uncovered without wiretapping. In essence, wiretapping is considered an exception, not a rule. The definition of serious crimes is provided in Article 83, paragraph (2) of the Draft, which includes criminal acts such as: crimes against state security (Chapter I, Book II of the Criminal Code); deprivation of liberty/kidnapping (Article 333 of the Criminal Code); theft with violence (Article 365 of the Criminal Code); extortion (Article 368 of the Criminal Code); threats (Article 368 of the Criminal Code); human trafficking; smuggling; corruption; money laundering; counterfeiting; immigration-related offenses; explosives and firearms offenses; terrorism; serious human rights violations; psychotropic drugs and narcotics offenses; and rape.

Wiretapping must be conducted with a written order from the local investigator's superior, following approval from the Preliminary Examining Judge. This procedure applies universally, including to the Corruption Eradication Commission, which also requires the permission of the Preliminary Examining Judge before carrying out any wiretapping. However, in urgent circumstances, exceptions to obtaining authorization from the Preliminary Examining Judge are allowed, though these must be reported to the judge via the public prosecutor. The authority to conduct wiretapping is strictly limited to specific crimes, including those related to state security, deprivation of liberty/kidnapping, theft with violence, extortion, threats, human trafficking, smuggling, corruption, money laundering, counterfeiting, immigration, explosives and firearms offenses, terrorism, serious human rights violations, narcotics and psychotropic substances, as well as rape, murder, illegal mining, illegal fishing, and illegal logging.

In law enforcement, wiretapping can be used to expedite investigations, provided it is carried out with extreme caution and adherence to due process of law. The draft Criminal Procedure Code stipulates that all wiretapping actions must be reported, and permission must be received from the Preliminary Examining Judge, with special regulations guiding the judge's decision on whether the wiretapping is legally justified. Currently, the regulations concerning wiretapping primarily focus on granting authority to law enforcement officers but do not sufficiently address the detailed mechanisms of wiretapping or the protection of privacy rights related to this practice. As a result, wiretapping remains vulnerable to violations of citizens' privacy rights by law enforcement agencies.

According to the principle of a state governed by law, as enshrined in Article 1, paragraph (3) of the 1945 Constitution, Indonesia upholds the rule of law. Indonesia is also a signatory to the International Covenant on Civil and Political Rights (ICCPR), which was ratified through Law Number 12 of 2005. Following Article 17, paragraph (1) of the ICCPR, it is stated that no individual shall be subjected to arbitrary or unlawful interference with their privacy, family, home, or correspondence, nor to unlawful attacks on their honor and reputation. (Sule, Zennaro, and Thomas 2021).

Article 12 of the Universal Declaration of Human Rights (UDHR) 1948 states, "No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence; nor shall he be permitted to commit violations of his honor and good name. Everyone has the right to legal protection against such interference or

violations." Similarly, Article 28G, paragraph (1) of the 1945 Constitution of Indonesia emphasizes that every individual has the right to the protection of their person, honor, dignity, and property, and is entitled to a sense of security and protection from threats that may instill fear or coercion regarding their actions or inactions. These provisions collectively underscore that the right to privacy is a fundamental human right that the State must safeguard. Any actions undertaken by the State or its apparatus must adhere to these human rights principles, ensuring that they do not infringe upon the constitutional rights of its citizens. As such, protecting privacy and other fundamental rights is a key responsibility of the State, and any violations of these rights constitute a breach of the law (Natamiharja et al. 2022).

The rapid development of technology has led to new challenges in law enforcement, as traditional methods are often inadequate in addressing modern crimes. To keep pace with technological advancements, law enforcement agencies are increasingly relying on methods like wiretapping, which has proven to be an effective tool in crime detection. Wiretapping plays a critical role in uncovering serious crimes, making it a valuable asset for law enforcement officers. However, the legal framework governing wiretapping in Indonesia is fragmented across several laws and regulations. This pluralism can lead to varied interpretations from both law enforcement and the public. For instance, Article 26A of the Amendment to Law Number 31 of 1999 on the Eradication of Corruption recognizes wiretapping as a valid form of evidence, alongside electronic recordings, under the Criminal Procedure Code. Similarly, Article 5 of the Electronic Information and Transactions Law affirms that electronic information and documents are valid forms of evidence, reinforcing their role in the legal process.

Despite its importance in modern law enforcement, wiretapping poses significant risks to individuals' right to privacy. Both the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, as well as the 1945 Constitution of Indonesia, emphasize that the right to privacy is a fundamental human right that must be protected by the State. This creates a delicate balance between the need for effective law enforcement and the protection of individual privacy.

Table 1 Model of wiretapping policy

No	About	Explanation	Current Condition	Recommendation
1	Wiretapping implementation period	The wiretapping implementation period is calculated from the date it is granted. Until the end of the validity period of the permit.	1. 30 days (Psychotropic Law) 2. 1 Year (Anti-Terrorism Law) 2. 1 year (Human Trafficking Eradication Law) 3. 3 months and can be extended again 1 x 3 months (Narcotics Law)	30 days and can be extended 1 x 30 days.
2	Law Enforcement Officers Who Conduct	Authorities of Officers Who Conduct Wiretapping	1. Police Investigators (Psychotropics Law) 2. Investigators (Corruption Crime Law, Terrorism	1. Corruption Eradication Commission Investigators 2. Intelligence (in cases where there is a

			Eradication Law, and Human Trafficking Eradication Law)	connection with state security)
3	Licensing Authority	The institution or agency authorized to grant permission to law enforcement officers to conduct wiretapping also assumes the role of a supervisory body by virtue of its administrative authority.	3. Corruption Eradication Commission (Corruption Eradication Commission Law) 4. Police and National Narcotics Agency Investigators (Narcotics Law)	
4	Purpose/reason	Some reasons or purposes for which authority can be requested	1. Chief of Police (Psychotropic Law) 2. Attorney General and/or Chief of Police (Telecommunication Law) 3. Order of the Chief Justice (Anti-Terrorism Law) 4. Written Order of the Chief Justice (Narcotics Law) 5. Order or permission from the Attorney General (Government Regulation of the Joint Corruption Eradication Team) 6. Request from the Attorney General, Chief of Police, Investigator (Government Regulation of Telecommunication)	The court has administrative authority, this licensing institution automatically becomes a supervisory institution.
5	Requirements	Having the authority re	1. Interests of Investigation (Anti-Terrorism Law) 2. Implementation of criminal case investigation duties, 3. For investigation, prosecution interests (National Security Commission Law on Corruption Eradication) 4. Interests of Investigation (Narcotics Law) 5. Interests of investigation (Joint Team Government Regulation, Corruption Eradication)	1. For the purpose of criminal investigation 2. For the purpose of national security

gulated in each Law				
6	Accountability/Reporting	What are the limits in conducting wiretapping	No accountability	Regulation of accountability in every unlawful wiretapping action
7	Wiretapping Mechanism and Technique	Standard Wiretapping Actions	Regulated in Every Law Enforcement	Agency Regulation Integrated in the Wiretapping Bill
8	Wiretapping Application Procedure	Wiretapping Standards	-	Integrated in the Wiretapping Bill
	Types of prohibited acts related to wiretapping	Circumstances in which wiretapping is not permitted	Not regulated	In diplomatic circumstances, without court permission and related to intelligence activities
9	Complaint Mechanism	Complaint mechanism for people who feel aggrieved by the wiretapping Court process. Criminal charges have been or are being made	Not regulated	1. Pretrial if the case has not been transferred to the Court 2. Criminal charges for malfeasance
10	Legal Instruments	Forms of legislation used as a legal umbrella for wiretapping carried out by law enforcement officers	Still scattered in various Legislations ranging from Laws to Ministerial Regulations	Laws and Government Regulations on Wiretapping

An ideal legal framework for effective wiretapping by due process should encompass several key principles and considerations. Wiretapping must be governed by clear and specific laws that outline when, how, and under what circumstances it can be performed. The law should ensure that wiretapping is only permitted in particular, strictly regulated situations, such as investigating serious crimes or threats to national security. Additionally, the law must require that individuals subject to wiretapping be notified after the fact unless there are compelling reasons to maintain confidentiality for the ongoing investigation.

Wiretapping must also adhere to the principle of proportionality, meaning that it should only be taken if no other effective investigative methods are available (Mousmouti 2018). Furthermore, the law must protect the privacy of those being wiretapped by imposing limits on the types of information that can be collected and stored and by restricting the duration of the wiretapping process. These measures are essential to balancing the need for effective law enforcement with the protection of individual rights and freedoms.

An independent oversight mechanism is essential to ensure that wiretapping is conducted in compliance with the law and is not abused. Lawmakers who violate wiretapping regulations must be held accountable for their actions. Individuals subject to wiretapping should have access to a fair and effective legal process to challenge the lawfulness of the wiretapping and seek redress if it is found to have been carried out illegally. The law must account for specific contexts, such as the wiretapping of advocates, journalists, or members of parliament, which require special consideration to prevent interference with their freedom to perform their duties. By addressing these elements, an ideal legal framework can regulate wiretapping effectively, ensuring that it serves investigative and security purposes while safeguarding individual human rights and adhering to the principle of due

process.

The Wiretapping Bill is designed to serve as a unifying regulation. While it aims to consolidate existing laws, careful drafting is crucial. This Bill should harmonize wiretapping regulations across various Special Laws (such as those addressing corruption) without narrowing the scope or complicating enforcement. It must align with the legal requirements of these Special Laws, ensuring that law enforcement can still address criminal acts detrimental to the public interest.

Wiretapping cannot be considered a law violation unless a specific law thoroughly regulates the mechanism and limitations of its implementation. This aligns with Indonesia's legal system, which adheres to the principle of legality, meaning that no act is prohibited unless explicitly defined by law (nullum delictum nulla poena sine praevia lege). It's important to note that in the investigative and inquiry process, there is a distinction from the due process of law, particularly regarding the paradigm of the presumption of innocence. Investigators, in this context, must operate under an assumption of potential guilt to explore the modus operandi and gather evidence to fulfill the necessary elements of proof (Laputigar, Suhadi, and Rodiyah 2024).

To ensure proper checks and balances in law enforcement and prevent the potential for arbitrary wiretapping, it is crucial to impose clear limitations on wiretapping regulations. The authority to conduct wiretapping must be explicitly defined in the law, accompanied by a stringent oversight system. This system should cover every stage, from the application for wiretapping permission, through its implementation, to the termination of the wiretapping. Such measures are essential to safeguard individuals' rights and prevent abuses of power.

Conclusion

The legitimacy of law enforcement's authority to conduct wiretapping remains ambiguous. This lack of clarity undermines fundamental principles of governance and creates the potential for abuse of power due to the absence of legally sanctioned duties. Citizens' rights to privacy are inadequately protected, as there are no clear regulations delineating the scope and limitations of wiretapping practices. Consequently, the public may experience a sense of insecurity, perceiving a loss of personal privacy. Furthermore, such ambiguity can affect the admissibility of evidence in judicial proceedings. Evidence obtained through unlawful wiretapping lacks legal evidentiary value and should, therefore, be excluded by the court or deemed inadmissible by the presiding judge. To establish an ideal and practical legal framework, it is essential to implement a system of checks and balances in law enforcement to prevent arbitrary or excessive use of surveillance powers. Accordingly, legislative limitations on wiretapping must be clearly defined. The law should stipulate that wiretapping must be proportionate to its intended objectives. This necessitates a clear and authoritative regulation governing wiretapping and a robust oversight mechanism comprising internal, external, and independent supervision. Such oversight should encompass all stages of the wiretapping process, including the request for authorization, implementation, and

termination, while prioritizing protecting personal data and citizens' privacy rights.

Bibliography

Alibeigi, Ali, Abu Bakar Munir, and Md. Ershadul Karim. 2019. "Right to Privacy, A Complicated Concept to Review." *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3537968>.

Amir, Firman, Marina Tresna Ayu MEIFANI, SATRIADI, Aries SETIYONO, MIKO, and Mutia Evi KRISTHY. 2023. "Implementation of the Legality Principle in the Criminal Justice System of Indonesia." *Journal of Political And Legal Sovereignty* 1 (2): 123–29. <https://doi.org/10.38142/jpls.v1i2.139>.

Diffie, Whitfield, and Susan Landau. 2007. *Privacy on the Line*. The MIT Press. <https://doi.org/10.7551/mitpress/5572.001.0001>.

———. 2008. "Brave New World Of Wiretapping." *Scientific American* 299 (3): 56–63. <https://doi.org/10.1038/scientificamerican0908-56>.

Febriani, Nadia, Haryadi Haryadi, and Dassy Rakhmawaty. 2021. "Penggunaan Saksi Mahkota (Kroongetuige) Dalam Pembuktian Di Persidangan Terhadap Tindak Pidana Narkotika." *PAMPAS: Journal of Criminal Law* 1 (2): 43–67. <https://doi.org/10.22437/pampas.v1i2.9614>.

Febryan Alam Susatyo, and Muchlas Rastra Samara Muksin. 2024. "Constructing the Concept of Commissioner Judge in Enforcing the Exclusionary Rules Principle in Indonesia." *JUSTISI* 10 (3): 505–17. <https://doi.org/10.33506/js.v10i3.2607>.

Franssen, Vanessa, and Stanisław Tosza, eds. 2025. *The Cambridge Handbook of Digital Evidence in Criminal Investigations*. Cambridge University Press. <https://doi.org/10.1017/9781009049771>.

Hafizhah, Annisa, Jelly Leviza, and Mulhadi Mulhadi. 2024. "An Overview of the Principle of Legality: Common Law VS Civil Law." *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal* 4 (1): 38–47. <https://doi.org/10.15294/ipmaphi.v4i1.76875>.

Isharyanto, Isharyanto, and Dwi Lestari. 2020. "IZIN PEMERIKSAAN TERHADAP ANGGOTA DPR OLEH APARAT PENEGAK HUKUM DIKAITKAN DENGAN PRINSIP NEGARA HUKUM." *Res Publica: Jurnal Hukum Kebijakan Publik* 1 (1): 57–73. <https://doi.org/10.20961/RESPUBLICA.V1I1.46705>.

Kalumata, Stella Maris Widiana, and Gandes Candra Kirana. 2025. "Comparative Study Of Wiretapping As Electronic Evidence In The Legal Systems Of Indonesia And The Netherlands." *Reformasi Hukum Trisakti* 7 (1): 353–64. <https://doi.org/10.25105/REFOR.V7I1.22326>.

Kulshrestha, Prof. Dr. Pradeep. 2022. *Cyber Crime, Regulations and Security - Contemporary Issues and Challenges*. Law brigade publishers. <https://doi.org/10.55662/CCRSbook.2022>.

Kusuma, Dedy Parta, Erikson Sihotang, and Komang Edy Dharma Saputra. 2025. “Juridical Review of Wiretapping Based on Law Number 1 of 2024 Amending Law Number 11 of 2008 on Electronic Information and Transactions Related to Criminal Acts at Bali Regional Police.” *Journal of Social Science (JoSS)* 4 (1): 35–42. <https://doi.org/10.57185/JOSS.V4I1.413>.

Laputigar, Rendy, Suhadi Suhadi, and Rodiyah Rodiyah. 2024. “Integrating Due Process Into The Enforcement Framework of Criminal Law Politics.” *IJCLS (Indonesian Journal of Criminal Law Studies)* 9 (1): 133–56. <https://doi.org/10.15294/ijcls.v9i1.50293>.

Lubin, Asaf. 2020. “The Rights to Privacy and Data Protection Under International Humanitarian Law and Human Rights Law.” <https://papers.ssrn.com/abstract=3622061>.

Mousmouti, Maria. 2018. “Drafting Legislation. Art and Technology of Rules and Regulation Helen Xanthaki London: Hart Publishing, 2014, 402 Pp. £51.70.” *European Journal of Risk Regulation* 9 (1): 177–79. <https://doi.org/10.1017/err.2018.6>.

Natamiharja, Rudi, Febryani Sabatira, Desia Rakhma Banjarani, Orima Melati Davey, and Ikhsan Setiawan. 2022. “Balancing Two Conflicting Perspectives on Wiretapping Act: Rights to Privacy and Law Enforcement.” *Al-Risalah: Forum Kajian Hukum Dan Sosial Kemasyarakatan* 22 (1): 18–30. <https://doi.org/10.30631/alrisalah.v22i1.1226>.

Purwadi, Wira, Mohamad Ali Akbar Djafar, Gilang Fatirah Densi, Anika Zaitun Tumiwa, and Arum Salsabila Yieputri Langkamane. 2022. “Application Of The Principle Of Equality Before The Law To Law Enforcement For The Realization Of Justice In Society.” *JURNAL LEGALITAS* 15 (1): 59–75. <https://doi.org/10.33756/jelta.v15i1.14772>.

Sakti, Agam, Nina Aprianingsih, and Saifun Nufus. 2022. “Implementation of the Principle of Equality Before The Law in Corruption Court Decisions.” *JURNAL RUANG HUKUM* 1 (1): 17–22. <https://doi.org/10.58222/juruh.v1i1.251>.

Shehu, Vlona Pollozhani, and Visar Shehu. 2023. “Human Rights in the Technology Era – Protection of Data Rights.” *European Journal of Economics, Law and Social Sciences* 7 (2): 1–10. <https://doi.org/10.2478/ejels-2023-0001>.

Slamet Riyadi, Bambang. 2022. “Culture of Abuse of Power in Indonesia from the Perspective of Criminology and Law.” *International Journal of Criminology and Sociology* 9 (April):274–84. <https://doi.org/10.6000/1929-4409.2020.09.26>.

Solum, Lawrence B., and Max Crema. 2022. “The Original Meaning of ‘Due Process of Law’ in the Fifth Amendment.” <https://papers.ssrn.com/abstract=4101815>.

Stoykova, Radina. 2023. “The Right to a Fair Trial as a Conceptual Framework for Digital Evidence Rules in Criminal Investigations.” *Computer Law & Security*

Review 49 (July):105801. <https://doi.org/10.1016/J.CLSR.2023.105801>.

Sule, Mary-Jane, Marco Zennaro, and Godwin Thomas. 2021. "Cybersecurity through the Lens of Digital Identity and Data Protection: Issues and Trends." *Technology in Society* 67 (November):101734. <https://doi.org/10.1016/j.techsoc.2021.101734>.

Surya Atmaja, Putu Oka. 2019. "Comparative Study Mekanisme Penyadapan Dalam Sistem Peradilan Pidana Indonesia Dan Inggris." *Jurnal Magister Hukum Udayana (Udayana Master Law Journal)* 8 (1): 90. <https://doi.org/10.24843/JMHU.2019.v08.i01.p07>.

Taufik, Moh, Andre Khalil, M Putera Lato, Renda Aranggraeni, and Coresponding Author. 2024. "Legal Implications of Wiretap Evidence in the Terrorism Investigation Process." *Lex Journal: Kajian Hukum Dan Keadilan* 8 (1): 108–15. <https://doi.org/10.25139/LEX.V8I1.9362>.

Theacornelia, Christella Jessicha, and Emmy Latifah. 2022. "The Violation of Immunity and Diplomatic Rights: A Study of Indonesian Embassy Wiretapping Case In Myanmar 2003-2004 in The Asean Community Security Resistance Based on The 1961 Vienna Convention." *Journal of ASEAN Dynamics and Beyond* 3 (1): 10. <https://doi.org/10.20961/aseandynamics.v3i1.52145>.