International Journal of Law, Policy and Social Review
www.lawjournals.net
Online ISSN: 2664-6838, Print ISSN: 2664-682X
Received: 09-07-2024, Accepted: 08-08-2024, Published: 23-08-2024
Volume 6, Issue 3, 2024, Page No. 286-290

The concept of coercive measures in wiretapping a review of the revised draft of the Indonesian penal code in the context of human rights approaches

Heru Riyadi
Faculty of Law, Universitas Pamulang, Tangerang Selatan, Indonesia

Abstract
This research explores the concept of coercive measures in wiretapping, specifically examining the revised draft of the Indonesian Penal Code (RKUHP) through a human rights lens. As a legal state, Indonesia prioritises human rights protection within its legal framework, where the principle of equality before the law is central. However, the regulation of wiretapping in Indonesia is inconsistent, leading to varied interpretations and implementation by law enforcement agencies. This research addresses the challenges posed by these inconsistencies, particularly the lack of legal certainty and protection of privacy rights in interception practices. Using normative legal research methods, this study examines primary, secondary, and tertiary legal materials to evaluate the legal mechanisms governing wiretapping and their alignment with human rights principles. The findings highlight the critical role of wiretapping in criminal investigations while emphasising the need for strict legal standards to prevent the misuse of this intrusive measure. The study also identifies gaps in the current legal framework that allow for arbitrary wiretapping without adequate safeguards for individual rights. The research concludes that effective regulation of wiretapping requires a balance between law enforcement needs and the protection of privacy rights. It recommends the establishment of a unified legal framework that ensures accountability, transparency, and adherence to human rights in the practice of wiretapping in Indonesia. This study contributes to the ongoing debate on the legal and ethical implications of coercive surveillance measures, particularly in the context of the Indonesian legal system.

Keywords: Wiretapping, human rights, legal framework

Introduction

The Unitary State of the Republic of Indonesia is a legal state where, through both the rule of law and *rechtsstaat* concepts, the recognition and protection of human rights are central concerns. To safeguard human rights, the rule of law emphasises the principle of equality before the law, prioritising legality [1], which subsequently evolves into the principle of justice. Speaking of justice, it is also pertinent to consider the legal context in Indonesia, where interception is regulated by various laws and regulations, ranging from statutes to ministerial regulations. Consequently, the mechanisms for interception and its duration vary depending on the type of crime addressed and the applicable regulations. Currently, there are several regulations in Indonesia that govern interception, including:

1. Law No. 5 of 1997 on Psychotropics;
2. Law No. 31 of 1999 on the Eradication of Corruption Crimes, as amended by Law No. 20 of 2001 on Amendments to Law No. 31 of 1999;
3. Law No. 36 of 1999 on Telecommunications;
4. Law No. 19 of 2019 on the Second Amendment to Law No. 30 of 2002 on the Corruption Eradication Commission;
5. Law No. 18 of 2003 on Advocates;
6. Law No. 21 of 2007 on the Eradication of Human Trafficking;
7. Law No. 35 of 2009 on Narcotics;
8. Law No. 48 of 2009 on Judicial Authority;
9. Law No. 8 of 2010 on the Prevention and Eradication of Money Laundering;
10. Law No. 17 of 2011 on State Intelligence;
11. Law No. 18 of 2011 on Amendments to Law No. 22 of 2004 on the Judicial Commission;
12. Law No. 19 of 2016 on Amendments to Law No. 11 of 2008 on Electronic Information and Transactions;
13. Law No. 5 of 2018 on Amendments to Law No. 15 of 2003 on the Stipulation of Government Regulation in Lieu of Law No. 1 of 2002 on the Eradication of Terrorism into Law;
14. Government Regulation No. 19 of 2000 on the Joint Team for the Eradication of Corruption Crimes;
15. Government Regulation No. 52 of 2000 on the Provision of Telecommunications Services;
16. Presidential Regulation No. 50 of 2011 on the Procedures for the Implementation of the Authority of the Financial Transaction Reporting and Analysis Centre;
17. Chief of the Indonesian National Police Regulation No. 5 of 2010 on the Procedures for Interception at the Indonesian National Police Monitoring Centre;
18. Operational Standards of the Corruption Eradication Commission (KPK) on Interception.

The lack of harmony in the regulation of interception procedures in Indonesia has serious consequences, creating space for interpretation among law enforcement agencies such as the police, prosecutors, and the KPK. This results in inconsistencies in implementation, which in turn highlights violations of the principles of legal certainty and equality before the law [2]. In addition to facing issues with the diversity of regulations, the interception procedures in Indonesia are also problematic because they have failed to protect those who may be harmed by arbitrary interception actions. Individuals targeted by interception cannot challenge the legality of the procedures applied to them. Moreover, the results of interceptions used as evidence in

court cannot be contested, as there is no unified mechanism that clearly and definitively regulates them.

Currently, interception has also become an issue within the provisions of the Draft Penal Code (Rancangan Undang-Undang Kitab Undang-Undang Hukum Pidana) and the National Penal Code Draft (RUUKHP Nasional). Interception is one of the tools used by law enforcement to obtain evidence in the investigation of certain crimes. It involves monitoring or acquiring information from an individual's private communications without their knowledge or consent.

Several important aspects regarding interception in the National Penal Code Draft (RUUKHP Nasional) include:

1. **Purpose of interception:** Interception may only be carried out for clear and limited purposes, such as investigation, prosecution, or legal action related to crimes specified by law;

2. **Conditions and procedures:** The RUUKHP Nasional establishes strict conditions and procedures for interception. For example, it requires a court order permitting interception after considering sufficient evidence regarding serious alleged crimes;

3. **Human rights protection:** Interception must respect human rights, including the right to privacy and freedom of communication. The RUUKHP ensures that interception tools are not misused and that the information obtained is kept confidential;

4. **Technical Provisions:** The RUUKHP may also regulate the technical aspects of interception, such as the types of communication that can be intercepted, the time limits for interception, and the appropriate technology to be used.

5. **Penalties for Violations:** The RUUKHP Nasional typically includes stringent penalties for those who misuse or violate interception provisions, to ensure fair and transparent law enforcement;

These points highlight that interception under the National RUUKHP should be used with careful consideration and in strict adherence to legal standards to protect individual rights while supporting effective law enforcement. The discussion of the Interception Bill has been included in the National Legislative Programme (Prolegnas) priority list since 2018 and continues to be part of the long list for Prolegnas 2020-2024.

Therefore, this research is expected to contribute by providing insights into regulations concerning coercive interception efforts that align with human rights principles and possess a robust accountability system. Based on the above background, several issues arise, including:

1. What is the concept of limiting the right to privacy in interception carried out for law enforcement purposes?.
2. What is the mechanism for protecting the right to privacy in coercive interception efforts?.

Research method

The research method employed in this study is normative legal research. Normative legal research, also known as doctrinal legal research, is a type of legal research conducted through the examination of library materials or secondary data. Generally in research, there is a distinction between data obtained directly from the community, referred to as primary data, and data obtained from library sources, known as secondary data. In the context of legal research, secondary data includes primary legal materials (such as statutes, case law, and so forth), secondary legal materials (which provide explanations of primary legal materials, such as research findings or scholarly works), and tertiary legal materials (which offer guidance or additional explanations about primary and secondary legal materials, such as dictionaries or encyclopaedias). This study will utilise primary, secondary, and tertiary legal Materials [3].

Result and discussion

The role of interception in investigations and as evidence

In Indonesia, regulations concerning wiretapping are found in several laws. There are 12 (twelve) laws that govern wiretapping, namely the Psychotropic Substances Law, the Telecommunications Law, the Anti-Terrorism Law, the Corruption Eradication Law, the Advocates Law, the Trafficking in Persons Law, the Information and Electronic Transactions Law, the Narcotics Law, the Anti-Terrorism Court Law, the Criminal Code, the Money Laundering Law, and the Judicial Commission Law. These twelve laws only regulate the authority to conduct wiretapping, while formal law, as a form of enforcing substantive law regarding wiretapping, is not covered by these laws. Therefore, formal law still refers to the provisions in the Criminal Procedure Code (KUHAP). The role of wiretapping in investigations is as a tool to gather evidence related to suspected criminal activities or other criminal acts. Wiretapping involves monitoring or recording someone's conversations or private communications without their consent, and the results of such wiretapping can be used by investigators to strengthen a case or obtain the necessary evidence for prosecution in court.

Here are some important aspects regarding the role of wiretapping in investigations:

1. **Obtaining Information Not Otherwise Accessible:** Investigators often encounter situations where the evidence required is difficult to obtain openly. Wiretapping can provide access to relevant information that might not be available through other sources.

2. **Strengthening Evidence:** The results of wiretapping can be used to reinforce other evidence collected during an investigation, such as physical evidence or witness testimony. Having recordings of conversations or communications that support the case can make the investigation stronger.

3. **Providing Details and Context:** Recorded conversations or communications through wiretapping can offer additional details and context essential for understanding events or actions that are suspected to be illegal. This can aid investigators in comprehending how a crime was committed or planning a more effective prosecution [4].

4. **Enabling Identification of Criminal Networks:** Through wiretapping, investigators can identify criminal networks or relationships between individuals involved in illegal activities. This helps in understanding the structure and dynamics of criminal groups and pursuing the entire criminal network.

5. **Legally Regulated Use:** While wiretapping can be a powerful tool in investigations, its use must be regulated and closely supervised by applicable laws. In many jurisdictions, wiretapping can only be conducted with permission from a court or authorised legal authority, and must meet stringent standards to protect individual privacy.

6. **Controversy and Ethics:** The use of wiretapping in investigations is often controversial due to its potential to infringe on individual privacy and raise questions about the validity of the evidence obtained. Therefore, it is crucial for investigators to adhere to legal and ethical standards to ensure that wiretapping is used only when absolutely necessary and within regulated boundaries.

Thus, wiretapping is an important tool in criminal investigations for gathering necessary evidence; however, its use must be conducted carefully and in accordance with the applicable legal provisions to ensure compliance with individual rights and the integrity of the legal process. The evidence tools outlined in the Criminal Procedure Code (KUHAP) do not specifically address wiretapping as an evidence tool. However, Law No. 20 of 2001 concerning Amendments to Law No. 31 of 1999 on the Eradication of Corruption (hereinafter referred to as the Amendments to the Anti-Corruption Law), Article 26A states that indicative evidence, as referred to in Article 188(2) of KUHAP, can also be obtained through electronic recordings or wiretapping. Therefore, in certain cases, such as corruption cases, wiretapping can be used as evidence in court [5].

Article 5 of the Information and Electronic Transactions Law (UU ITE) also explains that electronic information/documents are considered valid evidence and represent an extension of legitimate evidence according to the procedural law in Indonesia. The proposed amendments to the Criminal Procedure Code have included specific provisions regarding evidence obtained through wiretapping. Such evidence is classified as electronic evidence. Article 175(1) of the proposed KUHAP states that legitimate evidence includes: (1) Physical Evidence; (2) Documents; (3) Electronic Evidence; (4) Expert Testimony; (5) Witness Testimony; (6) Defendant's Testimony; and (7) Judge's Observations.

This article clarifies that electronic evidence, including that obtained through wiretapping, is considered valid evidence under criminal procedural law. Previously, the existing KUHAP did not specify electronic evidence as admissible in court, but it did refer to the UU ITE, which recognises electronic evidence as a legitimate form of evidence, thus extending the scope of criminal procedural law.

Interception as a form of limitation on the right to privacy

In the legal framework of Indonesia, the right to privacy is protected both through national law, namely the 1945 Constitution and Human Rights Laws, as well as through international legal instruments such as the UN's Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). However, this protection is not absolute, as it can still be limited by certain factors that are also regulated by these laws.

For instance, Article 28J, paragraph (2) of the 1945 Constitution states: **"**In exercising his or her rights and freedoms, every person shall be obliged to adhere to the restrictions stipulated by law solely to ensure recognition and respect for the rights and freedoms of others and to meet just demands in accordance with moral considerations, religious values, security, and public order in a democratic society."

In several subsequent articles, such as Article 70, which is worded similarly to Article 28J, paragraph (2) of the 1945 Constitution mentioned above, and Article 73, which essentially states that limitations on the rights and freedoms of others are implemented to ensure the recognition and respect for human rights, basic freedoms, public morality, public order, and national interests. One form of limitation on the right to privacy is the use of compulsory measures such as interception. Interception can be considered a specific type of compulsory measure because, unlike other forms of compulsory actions such as searches and seizures, interception is not carried out physically, visibly, or tangibly [6]. However, it still constitutes an intrusion into a person's privacy, as it involves secret surveillance of their communications. The English terms used to refer to interception include interception, wiretapping, eavesdropping, and electronic surveillance. Although these terms essentially have the same meaning, the distinctions lie in the technical implementation and the tools or technologies used.

The outcomes of interception activities may include recordings of conversations, video footage, or other electronic forms, which can then be used as evidence in court proceedings. However, it is important to note that the results of interception do not always end up being used as evidence in trials. For example, in practice in the UK, interception is often used primarily for information gathering, with the collected information then used to find evidence to be presented in court. Nonetheless, if the results of interception are to be used directly as admissible evidence in court, then the entire process of interception must adhere to certain principles, such as legality, legitimate aim, necessity, proportionality, and due process [7].

Restrictions on the right to privacy in the context of surveillance conducted for law enforcement purposes are crucial for maintaining a balance between the need to protect society from crime and individuals' rights to their privacy. Here are some relevant concepts of restriction [8]:

1. **Requirement for Warrant or Court Order:** In many countries, surveillance may only be conducted if a proper warrant or court order has been obtained. Such authorisation is typically granted based on sufficient evidence demonstrating that surveillance is necessary to investigate serious crime or for urgent national interests.

2. **Specific Purpose and Limited Duration:** Surveillance must have a specific purpose, such as obtaining evidence related to a particular criminal case. The duration of the surveillance is also usually limited to ensure that unnecessary monitoring of private communications is avoided.

3. **Proportionality of Methods:** The methods used for surveillance should be proportional to the objective to be achieved. For instance, the use of invasive

surveillance technology should be justified by the severity of the case and should not be employed excessively or without substantial grounds.

4. **Protection of Irrelevant Information:** During the surveillance process, measures must be taken to ensure that information not relevant to the purpose of the surveillance is neither retained nor used improperly.

5. **Clear Legal Provisions and Transparency:** The laws governing surveillance should be clear and transparent, so that individuals can understand when and how surveillance may be conducted, as well as their rights concerning privacy and data protection.

6. **Oversight and Accountability:** Surveillance processes must be closely monitored by independent authorities, such as courts or specialised oversight bodies. This includes periodic reviews of surveillance practices to ensure compliance with legal and ethical standards.

7. **Destruction and Exclusion of Unlawfully Obtained Evidence:** If it is found that surveillance was conducted without the appropriate authorisation or infringed on individual privacy rights, any evidence obtained through such surveillance should be destroyed and must not be used in legal proceedings.

These restrictions are designed to protect individual rights from unlawful invasions of privacy, while still allowing authorities to use necessary tools for law enforcement. They are a crucial element of fair legal principles and human rights protection in the modern era, which is shaped by advancing technology.

Mechanisms for protecting privacy rights in coercive surveillance efforts

Discussing Mechanisms for Protecting Privacy Rights in Coercive Surveillance The mechanisms for protecting privacy rights in coercive surveillance generally involve several steps and controls to ensure that surveillance is conducted lawfully and proportionately. Here are some of the protection mechanisms that are commonly implemented:

1. **Court Orders or Official Authorisations:** Surveillance should only be conducted if a court order or official authorisation from the relevant authorities has been obtained. This order is issued after investigators or prosecutors present sufficient evidence that surveillance is necessary for investigating serious crimes or for urgent national interests.

2. **Specific Objectives:** Surveillance orders must specify the exact objectives, such as obtaining evidence related to a particular criminal case or uncovering a complex criminal network. This helps ensure that surveillance is not used indiscriminately or for irrelevant purposes.

3. **Proportionality of Methods:** Surveillance should be carried out using methods proportional to the objectives intended. For example, the use of invasive surveillance technology should be justified by the severity of the case and should not be used excessively or without strong justification.

4. **Deletion of Irrelevant Information:** During and after the surveillance process, measures should be taken to ensure that information that is irrelevant or not related to the objectives of the surveillance is not retained or used unlawfully. This involves procedures for removing irrelevant data from investigative records [9].

5. **Oversight and Accountability:** The surveillance process should be closely monitored by independent authorities, such as courts or specialised oversight bodies. This oversight includes regular reviews of surveillance practices to ensure they remain in compliance with laws and ethical standards. Oversight authorities are also responsible for assessing compliance with legal provisions and ensuring that individual rights are protected.

6. **Erasure of Illegally Obtained Evidence:** If it is discovered that surveillance was conducted without proper authorisation or in violation of individual privacy rights, the evidence obtained from such surveillance must be deleted and not used in legal proceedings. This is crucial for maintaining the integrity of the justice system and protecting individual rights.

7. **Complaints and Legal Remedies:** Individuals who believe their privacy rights have been infringed by surveillance can file complaints with the relevant courts or oversight authorities. This provides a legal avenue for challenging the legality of surveillance and ensuring that their rights are respected.

These protection mechanisms aim to maintain a proper balance between law enforcement interests and the protection of individual privacy [10]. By implementing strict and transparent procedures, the legal system can use tools such as surveillance in a fair manner that complies with applicable legal principles.

Conclusion

1. Overall, the concept of restricting privacy rights in surveillance conducted for law enforcement purposes emphasises the importance of balancing the protection of individual privacy with the need to uncover crimes and maintain public security. Legality and Authorisation are essential; surveillance should only be conducted under a court order or official authorisation from the appropriate authorities. This ensures that any surveillance action is based on sufficient evidence and a clear objective, and is legally accountable. Furthermore, the process of surveillance must be strictly overseen by independent authorities, such as courts or specialised oversight bodies. This includes regular reviews of surveillance usage to ensure compliance with laws and protection of individual privacy rights. By implementing these restrictions, the legal system can ensure that surveillance for law enforcement purposes is conducted fairly, in accordance with human rights principles, and with respect for individual privacy. This is an integral part of the effort to maintain a balance between public security and civil rights in a democratic and legal society.

2. The legal system can use surveillance as an effective tool in law enforcement without compromising individuals' fundamental privacy rights. Adequate protection of privacy in the context of surveillance is crucial for maintaining justice, transparency, and respect for human rights in a democratic society. Properly regulated and supervised mechanisms are necessary. Transparency regarding surveillance policies and practices is important for building public trust. Those affected by surveillance should be provided with a clear understanding of their rights and the procedures followed in surveillance cases.

Recomendation

To address these challenges, a planned and systematic effort is needed to meet new challenges. A grand design for the reform of the criminal justice system and the legal framework in general should be initiated. As is known, the criminal justice system occupies a strategic position in the framework of building the Rule of Law and respecting human rights. Democracy can only function properly when there is institutionalisation of the Rule of Law. Thus, reforming the criminal justice system with a focus on human rights protection is a "*conditio sine qua non*" for the democratic institutionalisation process in the current transition period.

References

1. MD Moch Mahfud. Hukum dan Pilar-Pilar Demokrasi. Yogyakarta: Gama Media, 1999.
2. Manthovani R. Penyadapan VS. Privasi. Jakarta: PT. Bhuana Ilmu Populer, 2015.
3. Mamudji SS. Penelitian Hukum Normatif, Suatu Tinjauan Singkat. Jakarta: RajaGrafindo Persada, 2007.
4. Komisi Nasional Hukum dan Hak Asasi Manusia Republik Indonesia. Komentar Umum Kovenan Internasional Hak Sipil dan Politik. Jakarta: Komnas Ham, 2009.
5. Rusli M. Hukum Acara Pidana Kontemporer. yogjakarta: PT. Citra Aditya Bakti, 2001.
6. Manthovani R. Penyadapan VS. Privasi. Jakarta: PT. Bhuana Ilmu Populer, 2015.
7. Kristian. Kristian, Sekelumit Tentang Penyadapan Dalam Hukum Positif Di Indonesia. Bandung: Nusa Auliam, 2013.
8. Smith R. Hukum Hak Asasi Manusia. Yogyakarta : PUSHAM UII, 2008.
9. Dewan Perwakilan Rakyat, P. L.-2. (2024). Prolegnas-Long-Lis. Jakarta: www.dpr.go.Id.
10. Peter R. Baehr, (. H.-H. Peter R. Baehr, (1998), Hak-Hak Asasi Manusia dalam Politik Luar Negeri [The Role of Human Right in Foreign Policy]. Jakarta : Yayasan Obor Indonesia, 1998.