Kawanua International Journal of Multicultural Studies
Vol. 6, No. 1, June 2025, p. 51~66
ISSN: 2797-5460, E-ISSN: 2797-359X, DOI: 10.30984/KIJMS.v6i1.1347

Electronic Information Interception from the Perspectives of Positive Law and Islamic Criminal Law: A Multicultural Study on Privacy Protection in Indonesia

M. Hasan Ubaidillah
Universitas Islam Negeri Sunan Ampel Surabaya, Indonesia
Email: ubaidillah_mhasan@uinsby.ac.id

Article Info

Article history:
Received Feb 13, 2025
Revised Apr 21, 2025
Accepted Jun 29, 2025

Keywords:
Interception
Electronic Information
Positive Law
Islamic Criminal Law
Privacy

ABSTRACT

The criminal offense of interception of electronic information constitutes a violation of privacy rights in digital communication as regulated in Indonesian positive law, particularly in the Information and Electronic Transaction Law (ITE Law). Illegal interception, or wiretapping without authorization, can result in violations of human rights and entail legal consequences for the perpetrator. From the perspective of Islamic criminal law, this action can also be categorized as an act that violates principles of justice, protection of individual honor, and the prohibition of tajassus (spying) as mentioned in the Qur'an and hadith. This research analyzes regulations regarding interception in Indonesian positive law and reviews their conformity with the principles of Islamic criminal law. Furthermore, this research also examines the implementation of these regulations in the context of Indonesia's multicultural society, which consists of diverse religions, ethnicities, and cultures, in order to assess the extent to which law enforcement can guarantee justice and protection of privacy rights for all levels of society. The findings indicate that both positive law and Islamic law equally emphasize protection of individual privacy rights and provide sanctions for parties who violate these rules. Therefore, there is a need for strengthening of regulations and oversight mechanisms to ensure that interception actions are only conducted within the limits permitted by law and for legitimate purposes, such as law enforcement and state security.

This is an open access article under the CC BY license.

Corresponding Author:
M. Hasan Ubaidillah,
Universitas Islam Negeri Sunan Ampel Surabaya, Indonesia,
Jl. Ahmad Yani No.117, Jemur Wonosari, Kec. Wonocolo, Surabaya, Jawa Timur 60237
Email: ubaidillah_mhasan@uinsby.ac.id

1. INTRODUCTION

In Indonesia, information is believed to be one of the important agendas of the global community in the third millennium, among others characterized by the increasingly widespread use of information technology in various activities of human life, not only in developed countries but also in developing countries including Indonesia (Gul et al., 2025). This phenomenon, in turn, has positioned information as an extremely important and profitable economic commodity (Mukharrom & Abdi, 2023). The sophistication of information technology has provided facilities and conveniences that greatly assist human work and other needs. As expressed by Soejono Soekanto that "development is planned and orderly change which among others encompasses political, economic, demographic, psychological, legal, intellectual, and information technology aspects (Soekanto, 1989). The phenomenon of crime in information technology must indeed be watched carefully because such crime is considered different from

As a multicultural country, Indonesia is inhabited by a very diverse society in terms of religion, ethnicity, language, and cultural values. This diversity becomes both a wealth and a challenge in the formulation and implementation of legal policy, including regulations related to interception or wiretapping of electronic information (Fadhil, 2020). Each community group has different views regarding the concept of privacy, state authority, and limitations on intervention in private life. Therefore, the implementation of interception regulations cannot be carried out uniformly without considering the social and cultural context that exists in society (Dewi, 2018; Hairong & Ma, 2008). Regulations that are not sensitive to this diversity of values risk causing resistance, distrust, or even horizontal conflict. In this context, the government and policymakers are required to design legal mechanisms that are not only normatively valid, but also accommodative of local values, uphold the principles of social justice, and are able to maintain a balance between security needs and protection of human rights (Appelstrand, 2002; Craig et al., 2008; Nour, 2024). Crime in information technology can be committed without recognizing territorial boundaries and direct interaction between the perpetrator and the victim of the crime is not required. It can be ascertained that with the global nature of information technology, particularly the internet, all countries conducting activities utilizing information technology, particularly the internet, can almost certainly experience both positive and negative impacts including crime attempts carried out by utilizing information technology that are very dangerous to the State and society at large (Soekanto & Mamudji, 1994).

The debate regarding interception of communication or what is more commonly known as communication wiretapping has become increasingly heated recently following the emergence of a wiretapping case by the intelligence agencies of the United States and Australia against President Susilo Bambang Yudhoyono and several ministers of Indonesia United Cabinet II, which of course this is a crime that endangers state sovereignty (Aspinall et al., 2015). This incident constitutes an insult and simultaneously a very harsh slap to the government of the Republic of Indonesia, because important conversations of a head of state and other high officials in this country could be known by others. As if there were no efforts by this government in addressing this matter, except with a strong protest attitude and withdrawing the Ambassador of the Republic of Indonesia from Australia.

In a different context, interception or wiretapping can also be seen in legal cases that can endanger the state, among them is the case of KPK wiretapping recording results at the Constitutional Court (MK) such as the interception case or wiretapping results of

Antasari with who was suspected to be Anggoro in Singapore, wiretapping of Al Amin Nasution in the corruption case known as the "white dress girl scandal", recording of Artalyta Suryani's conversation with several officials allegedly from the Attorney General's Office in the bribery scandal of Artalyta Suryani and prosecutor Urip Tri Gunawan, also the bribery case that befell former member of the Business Competition Supervisory Commission (KPPU) Muhammad Iqbal.

Wiretapping conducted by law enforcement officials or official state institutions becomes controversial because it is considered by some parties as an invasion of citizens' privacy rights which includes privacy over personal life, family life, and correspondence, but on the other hand wiretapping is also very useful as one of the investigation methods, because wiretapping is an accurate alternative in criminal investigations against the development of crime modus operandi and very serious crimes (Hochman, 2022). In this case, wiretapping is a crime prevention and detection tool. Many perpetrators of serious crime cases can be brought to the green table as a result of the wiretapping process.

Considering these aspects, certainly without the wiretapping instrument, it would be very difficult for KPK to detect perpetrators of corruption crimes and simultaneously prosecute them in court. Without wiretapping, it would also be difficult for Detachment 88 to uncover various terrorism cases, likewise for the National Narcotics Agency in psychotropic and narcotics cases. However, interception as a crime prevention and detection tool also has dangerous tendencies for human rights if it is in improper law due to weak regulation and will be dangerous if it is in the hands of untrustworthy officials because it will be vulnerable to misuse, especially if the rules and regulations on this interception matter have the potential to violate human rights (Dewi, 2018; Fadhil, 2020).

Basically, the State of Indonesia has formulated regulations and rules on interception or wiretapping scattered in various laws and regulations, such as Law No. 36 of 1999 concerning Telecommunications, Law No. 30 of 2002 concerning KPK, Law No. 11 of 2008 concerning Information and Electronic Transactions, and Law No. 35 of 2009 concerning Narcotics up to the level of regulations under laws such as Ministerial Regulation of Communication and Information No. 11/PER/M.KOMINFO/020/2006, or at certain law enforcement agencies such as KPK which has standard operating procedures regarding technical wiretapping.

In Law Number 11 of 2008 concerning Information and Electronic Transactions Article 31, it is explained that Interception or wiretapping is an activity to listen, record, deflect, modify, obstruct, and/or record the transmission of electronic information and/or electronic documents that are public in nature either using cable communication networks or wireless networks, such as electromagnetic radiation or radio frequency.

This article explains what forms of crimes in interception of electronic information are, so that if there is someone who does what is mandated by Article 31 of Law Number 11 of 2008 concerning Information and Electronic Transactions, then this can already be categorized as a perpetrator of criminal interception of electronic information that exists within the scope of the State of Indonesia (Raharjo, 1983).

In the context of Islamic criminal law, interception or wiretapping can be categorized as an act or action of tajassus or spying which of course has been explicitly prohibited by religion so that the perpetrator can be given sanctions or punishment. The application of sanctions or punishment given to perpetrators of interception of electronic information according to Islamic criminal law can be given *ta'zir* punishment, in which this *ta'zir* punishment is not determined by nash or hadith but is left to *ulil amri* (Lestari, 2024).

Although the criminal act of interception of electronic information is not found sharikh or explicitly in the nash of the Qur'an and al-hadith, it does not mean that there are no provisions that can be used as a basis for prohibition of the criminal act of interception of electronic information considering that Islamic law is a law built based on human understanding that applies universally, is relevant at all times (time), and space (place) of humans (An-Na'im, 2017). In An-Nabhani's view, interception in the view of Islamic criminal law can be categorized as an activity of investigating or examining a news to examine it further. In this context, such action is categorized as *tajassus*, namely conducting activities that spy on someone to obtain information or data with a specific purpose (Amiri, 2025). An-Nabhani's opinion has strong naqliyah legitimacy if connected with the word of Allah, SWT which means "

> "O you who believe, avoid most of the suspicion towards fellow believers, because suspicion among believers is a sin. Do not spy on fellow believers..." (Departemen Agama RI, 2002, p. 35)

The prohibition of tajassus against Muslims in the verse above is general in nature, applicable to individuals, groups, and states. Whether tajassus is done for one's own interest or for the interest of others. The prohibition law of tajassus against Muslims also applies to non-Muslim citizens (kafir dzimmi). Because a disbeliever who is subject to the Islamic state and has the status of a protected citizen, all Islamic laws apply to him except laws relating to aqidah and worship, and the issue of tajassus is not included in that.

2. METHODS

The research method used in this study is library research with a juridical-normative and comparative approach. This research examines relevant laws and regulations, particularly the Information and Electronic Transaction Law (ITE Law), as well as literature related to Islamic criminal law (Cownie & Bradney, 2013). In addition, this study also involves analysis of sources from the perspective of customary law and the views of various cultural groups in Indonesia regarding the concept of privacy, in order to obtain a more holistic understanding in the context of a multicultural society. This approach aims to assess the conformity and acceptability of interception regulations in diverse social realities, as well as provide inclusive recommendations in the development of legal policy in Indonesia (Huda, 2022).

3. RESULTS AND DISCUSSION

3.1 Definition and Description of Interception

The definition and meaning of interception in a linguistic perspective is wiretapping which according to English etymology is called interception, while in Kamus.net, intercept is translated as to hold, to catch, to intercept or to bypass, while in the Oxford dictionary it is defined as to cut off from access or communication. While in the Big Indonesian Dictionary, wiretapping is interpreted as the activity of listening to other people's conversations (secretly), such as telephone conversations. In the context of this discussion, the wiretapping referred to is wiretapping on communication devices, both communication tools using cables and cable-free communication.

In the perspective of Islamic criminal law, interception or wiretapping is equated with *tajassus*. The word *tajassus* literally comes from the word *jassa* which means to hide. It is also said that *jassa al-khabara* means to search for news, and the word jassus is taken from the word jassasa which means to seek. These three words can basically be said to be

almost the same. If referring to the understanding of *tajassus* in Islamic criminal law, interception activities can be categorized as investigating or examining news to investigate it further, the form of the activity is to spy on someone to obtain information or data with a specific purpose (Kamali, 2019).

An explanation related to this can also be seen in the statement of Al-Zamakhsyari in his book entitled "Al-Kashaf an Haqaiq Ghawamidh al-Tanzil wa 'Uyun al-Aqawil fi Wujuh al-Ta'wil" which explains that tajassus means investigating the defects and disgrace of others, which is sometimes used to mean gathering information and news. In his explanation, Al-Zamakhsyari provided an understanding and differentiation between the meaning of tajassus and tahassus with an expression of "the word tajassus generally leads to evil or bad things while the word tahassus is generally used in the context of good or virtuous things (Azizi, 2020)."

A slightly different explanation is given by Abdul Rahman bin Nasir Al-Sa'di in his book entitled Taisir al-Karim ar-Rahman fi Tafsir Kalam al-Mannan. He explained that Allah SWT forbids His servants from spying on Muslims and revealing their defects and searching for their disgrace. The prohibition of tajassus towards fellow Muslims is narrated in the hadith of the Prophet SAW which explains: "O people who believe with their tongues, but faith has not entered their hearts, do not backbite Muslims and do not search for their disgrace. For indeed whoever searches for the disgrace of his Muslim brother, Allah will search for his disgrace. And whoever Allah searches for his disgrace, He will expose it even if he is in the middle of his house."

A more specific opinion regarding the prohibition of tajassus was expressed by Al-Utsaimin who stated that tajassus is seeking the defects of others or investigating the wrongdoings of one's brother, and this is a despicable act and must be punished for whoever commits it.(Al-Utsaimin, n.d.) While according to Abdullah bin Muhammad bin Abdurrahman bin Ishaq, he also stated when interpreting the above verse as follows, "the meaning is that the word 'tajassus' is more often used for an evil, while the word 'tahassus' is often used for good things. As Allah Ta'ala spoke, which tells about the prophet Ya'qub 'alaihissalam, as the Word of Allah SWT which states

> “O my sons, go and seek news about Yusuf and his brother and do not despair of Allah's mercy. Indeed, no one despairs of Allah's mercy except the disbelieving people.”

However, sometimes both words are used to indicate bad things, as stated in the sahih hadith above. Imam Abu Hatim al-Busti rahimahullah said, "tajassus is a branch of hypocrisy, as conversely good assumptions are a branch of faith. A wise person will have good assumptions about his brother, and will not want to make him sad and grieved. While a foolish person will always have bad assumptions about his brother and will not hesitate to do evil and make him suffer (Amiri, 2025).

Sufficient for us is a string of words from an imam, namely Imam Abu Hatim bin Hibban Al-Busthi, who said in one of his books quoted by Shaykh Abdul Muhsin bin Hamd al-'Abbad al-Badr in his writing as follows, "A wise person is obligated to seek safety for himself by abandoning the act of tajassus and always being busy thinking about his own wickedness.

Indeed, a person who is busy thinking about his own wickedness and forgetting the wickedness of others, then his heart will be calm and will not feel tired. Every time he sees the wickedness within himself, he will feel humiliated when he sees similar wickedness in his brother. Meanwhile, a person who is always busy paying attention to the wickedness of others and forgetting his own wickedness, then his heart will become

blind, his body will feel tired, and it will be difficult for him to abandon his own wickedness (Jordan et al., 2014).

In the context of statehood, wiretapping activities by utilizing information technology. Wiretapping is a "common" case especially in the arena and political battles in modern democratic countries. In cases in a number of countries, telephone wiretapping is carried out by government officials on telephones belonging to prominent politicians and journalists in their respective countries. This is usually done to control the activities of politicians and journalists. The case of leaked documents by Wikileaks is a factual example in uncovering this activity.

Therefore, from the facts of telephone wiretapping, which is none other than to know the contents of secret conversations between two people who are making phone calls, we can categorize that telephone wiretapping is one type of espionage or spying activity or tajassus. In giving legal status to this act, Taqiyuddin An-Nabhani (2003) gives emphasis that tajassus activities have laws according to the facts of their activities. If the activity is directed at Muslims, whether citizens or rulers, it is haram.

Furthermore, Nabhani is of the opinion that the prohibition of tajassus against Muslims in the Qur'an is general in meaning, applicable to individuals, groups, and states whether carried out for personal, group, or state interests. The law prohibiting tajassus also applies to non-Muslim citizens, because a non-Muslim who is subject to the regulations of an Islamic state and has the status of a citizen has the same right to obtain legal protection except for laws related to aqidah and worship, while the issue of tajassus is not included in that category (Berween, 2017).

The act of wiretapping, spying or seeking the faults of others secretly, as well as monitoring the defects of others is an action that can be categorized as tajassus which is haram in law and its perpetrator must be severely punished according to the level of harm caused, except if there is already clear evidence that can endanger the ummah in general (Widiawan & Junaidi, 2024).

A similar opinion is also expressed by al-Zamakhsyari who states that if the target of the act of tajassus is the enemy of the state with the status of kafir harbi who can endanger the state, then such action is permitted. This permission is based on the narration when the Messenger of Allah sent a troop led by Abdullah bin Jahsy with a letter whose contents were: If you read my letter, then continue walking until you reach the date palm plantation location between Mecca and Taif. From there, spy on the Quraysh people and immediately report to me the information you know about the activities they are doing (Azizi, 2020).

Based on the above narration, the act and activity of interception or tajassus against enemies who endanger Muslims is a permitted act and even at a certain level is obligatory on the basis of protecting state security from enemies whose actions can be categorized as part of jihad fi sabilillah to protect the Religion of Allah SWT. For this purpose, the existence of the State Intelligence Agency is a necessity and obligation considering that the state intelligence agency has a strategic function in fortifying the state from external attacks.

However, if the act of tajassus is carried out against fellow believers and for personal interests, then such action is not permitted for any reason, so that such action is an action that can be categorized as criminalization of other people's freedom so that such action is a form of criminal act whose perpetrator deserves punishment from ulil amri according to the level of fault committed and the level of harm caused.

3.2 Interception in the Perspective of Indonesian Legal Pluralism

Indonesia is a country with a pluralistic legal system, where positive law, religious law, and customary law live and interact in the same social space. In the context of regulating privacy and interception of electronic information, these three legal systems have their respective views and regulatory mechanisms, which reflect the basic values of the society they represent.

Indonesian positive law, particularly through Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law) and its amendments, explicitly prohibits interception actions without permission and stipulates criminal sanctions for violators. This regulation aims to protect individual privacy rights in digital space and ensure the security of personal information from misuse. Meanwhile, Islamic criminal law also views illegal interception as a form of tajassus (spying), which is prohibited in the Qur'an surah Al-Hujurat verse 12 and in the hadiths of the Prophet which emphasize the importance of maintaining the secrets and honor of individuals.

In the perspective of customary law, various indigenous communities in Indonesia have their own norms regarding the concept of privacy and surveillance. For example, in Balinese society, the concept of *krama* (etiquette) and social harmony is an important part of the customary structure. Acts of wiretapping or disclosure of personal information without permission are seen as violations of the principle of *rwa bhineda* (balance of two elements), and can be subject to customary sanctions such as community reprimand, temporary ostracism, or reduction of social status in the banjar system (Praditha, 2024). Privacy is not only about individuals, but also closely related to the good name of the family and community.

Meanwhile, in Aceh, which implements Islamic law specificity in the regional government system, the issue of wiretapping or interception is also viewed within the framework of sharia. Aceh's Jinayat Law does not specifically regulate electronic interception, but general sharia principles that prohibit ghibah, slander, and tajassus are used as ethical foundations. The religious Acehnese society tends to be sensitive to privacy violations, especially if they impact the honor of individuals or families. In this context, religious norms, state law, and Acehnese customs interact in forming protection mechanisms for privacy rights (Feener, 2013).

In Papua, indigenous communities have a social system based on collectivity and customary deliberation. Personal information is often considered common property of the community, especially concerning community figures or tribal leadership. However, limits on supervision or intervention in personal matters are also strictly maintained through local values such as siri (sense of shame), self-esteem, and community secrets. Violation of someone's privacy in a community can cause conflicts between families or clans, and is resolved through customary mechanisms, such as tribal council meetings, provision of customary fines (compensation), or mediation by customary chiefs (Hammar, 2018). The concept of privacy in Papua is very contextual and cannot be separated from social relations in indigenous communities.

These three examples show that interception, although technically a digital law issue, has very strong sociocultural and religious dimensions in various regions in Indonesia. Therefore, the application of positive law related to interception must consider this diversity so as not to injure local values, cause social tensions, or ignore legal systems that have long lived in the midst of society.

Thus, within the framework of Indonesian legal pluralism, it is important for policymakers and law enforcement officials to understand the interaction between state law, religious law, and customary law holistically. Harmonization efforts among the three will create interception regulations that are not only legally normative, but also contextual, fair, and accepted by all elements of Indonesia's very diverse society.

Indonesian positive law, particularly through the ITE Law, explicitly prohibits interception actions without permission. In Islamic criminal law, the practice of spying without basis is known as *tajassus*, and is explicitly prohibited in the Qur'an surah Al-Hujurat verse 12. This prohibition is enforced to maintain the dignity and privacy of individuals, which is part of maqāṣid al-sharī'ah.

However, in Indonesian local culture, the concept of "spying" has a more contextual meaning and is often intertwined with communalism values. For example, in Javanese culture, social harmony (rukun) and maintaining others' feelings (tepa salira) are primary values. Although Javanese society lives in a tight social structure and mutually attentive, behavior that excessively interferes with personal matters is considered a violation of social ethics (ora ilok). Peeking into personal affairs, spreading personal information without permission, or being too curious is considered to damage social harmony and can trigger gossip (gunem) which has a bad impact on someone's reputation and their family.

On the other hand, in Batak culture, particularly in the dalihan na tolu kinship system, the social structure is very open and collective. Interaction among extended family members is very intensive, and information about community members tends to be open. However, this does not mean that all forms of intervention or personal investigation are justified. When intervention is carried out without permission or with bad intentions (marsirikkot), it is considered a form of violation of someone's dignity (hasuhuton) and can trigger conflict between clans. Therefore, in the Batak context, there are unwritten boundaries between social concern and actions of interfering with private matters.

Meanwhile, in Minangkabau culture, which is known for the philosophy *adat basandi syarak, syarak basandi Kitabullah*, Islamic values are very integrated in the customary structure. Individual privacy is maintained within the framework of collective values and social decency. Acts of tajassus or spying are considered contrary to the high value of shame (sense of self-esteem) in Minangkabau culture. Even negative talk about other people's affairs that may not necessarily be true can be considered a violation of the honor of a clan or tribe (Aldi & Kawakib, 2025). Such settlement is often left to ninik mamak through customary deliberations that uphold the principles of justice and social balance.

These three examples show that although communalism values are high in many Indonesian cultures, the act of "spying" is still recognized as a violation of social ethics and community morality, especially when done secretly or without legitimate purpose. Therefore, the approach to interception regulation in the Indonesian legal system should not only be based on formal legal aspects, but must also pay attention to how local communities interpret the boundaries between social concern and privacy violation.

3.3 Analysis of Implementation of 17 Wiretapping Regulations in the Context of Indonesia's Cultural Diversity

In laws and regulations in Indonesia, not many of these regulations provide a definition of interception or wiretapping. Of a number of existing rules and regulations,

only a few Laws provide a definition of interception or wiretapping, some of which are the Narcotics Law and ITE Law. Article 1 Number 19 of Law No. 35 of 2009 concerning Narcotics states that Wiretapping is an activity or series of investigation or investigation activities by wiretapping conversations, messages, information, and/or communication networks conducted through telephones and/or other electronic communication devices.

As a comparison, the ITE Law provides a sharper definition regarding Wiretapping. The explanation of Article 31 paragraph (1) of Law No. 11 of 2008 concerning ITE states that what is meant by "interception or wiretapping" is an activity to listen, record, deflect, modify, obstruct, and/or record the transmission of Electronic Information and/or Electronic Documents that are not public in nature, either using cable communication networks or wireless networks, such as electromagnetic radiation or radio frequency.

While in Minister of Communication and Information Regulation Number 11 /PER/M. KOMINFO/02/2006 concerning Technical Wiretapping of Information which contains guidelines for conducting wiretapping legally, it defines that Information Wiretapping is listening, recording, or recording a conversation conducted by Law Enforcement Officials by installing additional tools or devices on telecommunications networks without the knowledge of the people conducting the conversation or communication.

While the definition of wiretapping in the KUHAP Draft Law in Article 83 paragraph (1) states that: "Wiretapping of conversations through telephones or other telecommunications devices is prohibited, except carried out against conversations related to serious crimes or strongly suspected that such serious crimes will occur, which cannot be revealed if wiretapping is not carried out."

In Indonesia, protection of privacy rights was only widely recognized after the amendment of the 1945 Constitution, but the provisions that can be referred to as one form of privacy protection in Indonesia is Article 551 of the Criminal Code. Article 551 of the Criminal Code states that "Whoever without authority walks or rides on land that is clearly prohibited from entering by the owner, is threatened with a fine of at most two hundred twenty-five rupiah.

After the reform, the Right to Privacy in Indonesia is guaranteed protection explicitly in various laws and regulations as well as the Constitution. Article 28 G paragraph (1) of the 1945 Constitution states, "Everyone has the right to protection of personal self, family, honor, dignity, and property under their control, as well as the right to a sense of security and protection from the threat of fear to do or not do something which is a human right." Article 32 of Law No. 39 of 1999 concerning Human Rights states: "Independence and secrecy in relations through communication tools shall not be disturbed, except by order of a judge or other legal authority in accordance with the provisions of laws and regulations."nFrom various regulations and laws mentioned above, it can be concluded that there are at least 17 laws and regulations related to wiretapping or interception in Indonesia. The following are 17 laws and regulations related to wiretapping that apply in Indonesia:

3.3.1. Law Number 30 of 2002 concerning the Corruption Eradication Commission

This law regulates the authority to wiretap, based on sufficient preliminary evidence. Recording of information from wiretapping is carried out for a maximum period of 1 (one) year and can be extended only 1 (one) time for the same period, after obtaining written permission from the Panel of Judges at the suggestion of the Leadership of the Corruption Eradication Commission

3.3.2. Law Number 31 of 1999 concerning Eradication of Corruption Crimes

This law regulates the authority granted to the Attorney General or Police to conduct wiretapping in corruption cases with sufficient preliminary evidence and in special circumstances.

3.3.3. Law Number 15 of 2002 concerning Money Laundering Crimes as amended by Law Number 8 of 2010 concerning Prevention and Eradication of Money Laundering Crimes

This law regulates the authority to wiretap using special techniques with sufficient preliminary evidence. With regard to special techniques, wiretapping procedures are carried out in accordance with the provisions of laws and regulations.

3.3.4. Law Number 36 of 1999 concerning Telecommunications

This law regulates the provision by telecommunication service providers of recording information for the benefit of criminal judicial processes upon written request from the Attorney General or Chief of Police of the Republic of Indonesia. The request must be accompanied by sufficient preliminary evidence. Recordings of information from telecommunications must be submitted confidentially to the requesting party. This law does not regulate wiretapping authority.

3.3.5. Law Number 26 of 2000 concerning Human Rights Courts

This law regulates the authority of the Attorney General's investigators to wiretap with written permission from the Chief of the District Court for a maximum period of 1 (one) year.

3.3.6. Law Number 21 of 2007 concerning Eradication of Trafficking in Persons Crimes

This law regulates the authority of investigators to conduct wiretapping related to trafficking in persons crimes based on sufficient preliminary evidence with written permission from the Chief of the Court for a maximum period of 1 (one) year.

3.3.7. Law Number 11 of 2008 concerning Information and Electronic Transactions

This law regulates the prohibition of wiretapping, except for wiretapping for the purpose of law enforcement at the request of the police, prosecutor's office, and/or other law enforcement institutions

3.3.8. Law Number 35 of 2009 concerning Narcotics

This law regulates the granting of authority to investigators (BNN (National Narcotics Agency) Investigators and Police Investigators) related to narcotics trafficking after there is sufficient initial evidence by several wiretapping methods. The wiretapping period is at most 3 (three) months and can be extended 1 (one) time for the same period. Wiretapping is only carried out with written permission from the Chief of the Court. This Law also regulates wiretapping in urgent situations, and within a maximum of 1 x 24 (one times twenty-four) hours, Investigators are obliged to request written permission from the Chief of the District Court

3.3.9. Law Number 17 of 2011 concerning State Intelligence

This law regulates the authority to conduct wiretapping by BIN (State Intelligence Agency), with the aim of gathering information on Targets related to activities that threaten national interests and security. Wiretapping is carried out on the orders of the Head of BIN and the determination of the Chief of the District Court, for a period of 6 (six) months and can be extended according to needs

3.3.10. Law Number 18 of 2011 concerning Amendment to Law Number 18 of 2004 concerning the Judicial Commission

This law regulates the provision that the Judicial Commission can request assistance from law enforcement officials to conduct wiretapping and record conversations in the event of alleged violations of the Code of Ethics and/or Guidelines for Judge Conduct by Judges

3.3.11. Government Regulation Number 19 of 2000 concerning Joint Teams for Eradication of Corruption Crimes

This regulation regulates the provisions related to the authority of investigators to conduct wiretapping. There are no other arrangements or explanations related to this authority

3.3.12. Law Number 15 of 2003 concerning the Establishment of Government Regulation in Lieu of Law Number 1 of 2002 concerning Eradication of Terrorism Crimes, into Law

This law regulates the authority of investigators, based on sufficient preliminary evidence, to conduct wiretapping related to terrorism crimes. Wiretapping is carried out on the orders of the Chief of the District Court for a maximum period of 1 (one) year, and must be reported or accounted for to the investigator's superior

3.3.13. Government Regulation Number 52 of 2000 concerning Implementation of Telecommunication Services

This regulation regulates the Request for information and recording results from telecommunication service providers by the Attorney General and/or the National Police for certain crimes with a copy to the Minister of Infokom. This Government Regulation also regulates written requests that must contain the object being recorded, recording period and period of recording results report. The results of information recording must be submitted confidentially to the Attorney General and/or Chief of Police and/or Investigators. Telecommunication service providers are obliged to fulfill information recording requests no later than 1 x 24 hours from the time the request is received. If not possible, notification must be made no later than 6 (six) hours after receipt of the request.

3.3.14. Minister of Information and Communication Regulation Number 11 of 2006 concerning Technical Wiretapping of Information

This regulation regulates Wiretapping conducted by law enforcement officials through information wiretapping tools and/or devices. Information wiretapping tools and/or devices and the target identification process are controlled by authorized law enforcement officials. Wiretapping can be carried out for the purpose of law enforcement, but the intended crimes are not specifically mentioned. Wiretapping results are confidential. Supervision of wiretapping is carried out by a Supervisory Team formed by the Director General to verify legal and technical aspects of the implementation of legal information wiretapping

3.3.15. Minister of Information and Communication Regulation Number 1 of 2008 concerning Information Recording for Defense and State Security

This regulation regulates Information Recording for the purposes of defense and state security, conducted upon request from State Intelligence to Telecommunications Providers with a copy to the Minister. Wiretapping procedures are regulated based on SOP (Standard Operating Procedures) established by BIN according to the characteristics of its interests. All information is confidential and is only used by BIN for the purposes of defense and state security

3.3.16. Regulation of the Chief of the National Police of the Republic of Indonesia Number 5 of 2010 concerning Wiretapping Procedures at the National Police Monitoring Center of the Republic of Indonesia

This regulation regulates wiretapping and supervision and control of the wiretapping process

3.3.17. Standard Operating Procedure of the Corruption Eradication Commission (KPK)

This SOP is Confidential, cannot be accessed.

The regulations as described above represent an overview of how wiretapping regulations are mapped in Indonesia, consisting of 12 Laws, 2 Government Regulations, 2 Ministerial Regulations, 1 National Police Regulation, and 1 Regulation in the form of SOP (Standard Operating Procedures). The majority of regulations are issued to grant wiretapping authority to each targeted state institution, and the rest are more regulatory in nature for the internal needs of each state institution. Rules regarding wiretapping permits depend on the authority of each institution, so the authority to grant wiretapping permits is through each existing regulation.

The legal norms of interception or wiretapping actions according to the Constitutional Court's decision mandate that in forming rules regarding wiretapping mechanisms, wiretapping requirements need to be considered, namely:

1. The existence of official authority designated in Law to grant wiretapping permits,
2. The existence of a definite time guarantee in conducting wiretapping,
3. Limitation on handling wiretapping result material
4. Limitation regarding people who can access wiretapping.
5. While the elements that must exist in wiretapping regulations are:
6. Authority to conduct, order or request wiretapping,
7. Specific purpose of wiretapping,
8. Category of legal subjects authorized to conduct wiretapping,
9. Existence of permission from superiors or judge's permission before conducting wiretapping,
10. Wiretapping procedures,
11. Supervision of wiretapping,
12. Use of wiretapping results, and other important matters, namely
13. Complaint mechanism if there are losses arising from third parties due to the wiretapping action being carried out, as well as other regulations in the form of violation sanctions, and internal mechanisms to guarantee Human Rights

At least the formulation of legal norms regarding interception or wiretapping acts that have been outlined by the Constitutional Court is the basis for the revision and improvement of various regulations or laws and regulations concerning the practice of interception or wiretapping that some time ago underwent judicial review.

In the normative context in Indonesia, wiretapping or interception is generally prohibited, unless the law allows it. From a criminal law perspective, wiretapping to uncover a crime can be justified and does not violate Human Rights ("HAM"), as long as the law regulates it accordingly. This is explicitly contained in Article 28J paragraph (2) of the 1945 Constitution ("UUD 45"), particularly in Article 28 J paragraph (2) of the 1945 Constitution which states that:

> "In exercising his rights and freedoms, every person shall be subject to the limitations established by law solely for the purpose of guaranteeing the 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."

The prohibition on wiretapping or interception itself in Indonesia is specifically regulated in Article 40 of the Telecommunications Law and Article 31 paragraphs (1) and (2) of the ITE Law, particularly in Article 40 of the Telecommunications Law which states that everyone is prohibited from conducting wiretapping activities on information transmitted through telecommunications networks in any form. The sanction for such action is imprisonment of at most 15 years. The exception to Article 40 of the

Telecommunications Law can be seen in Article 43 of the Telecommunications Law, namely the provision of information recording by telecommunications service providers to telecommunications service users and for the benefit of criminal judicial processes, is not a violation of Article 40 of the Telecommunications Law.

While another wiretapping prohibition regulated in Article 31 paragraphs (1) and (2) of the ITE Law is as follows:

Article 31 paragraphs (1) and (2) of the ITE Law are as follows:

1. Every Person who intentionally and without right or unlawfully conducts interception or wiretapping of Electronic Information and/or Electronic Documents in a particular Computer and/or Electronic System belonging to another Person.
2. Every Person who intentionally and without right or unlawfully conducts interception of transmission of Electronic Information and/or Electronic Documents that are not public in nature from, to, and within a particular Computer and/or Electronic System belonging to another Person, whether it does not cause any changes or causes changes, deletion, and/or cessation of Electronic Information and/or Electronic Documents being transmitted.

The sanction for violation of Article 31 paragraphs (1) and (2) of the ITE Law is imprisonment of at most 10 years and/or a fine of at most Rp 800 million (eight hundred million rupiah), as regulated in Article 47 of the ITE Law. However, it should be noted that regarding this interception prohibition, there is also an exception in Article 31 paragraph (3) of the ITE Law. Except for interception as referred to in paragraphs (1) and (2), interception carried out in the context of law enforcement at the request of the police, prosecutor's office, and/or other law enforcement institutions established based on law."

Both laws have never regulated what happens if wiretapping is carried out by someone on the orders of a certain state. The weight of criminalization burden is only directed at "people" who de facto conduct wiretapping. There are no other derivative provisions, such as if that "person" conducts wiretapping on the orders of another state or institutional orders.

In the ITE Law, what is meant by "person" is Indonesian citizens, foreign citizens, and legal entities. So, if the perpetrator of illegal wiretapping is a foreign citizen, the ITE Law can be applied (Koto, 2021). The ITE Law can be applied to every person who commits legal acts regulated in the ITE Law (whether located in Indonesian legal jurisdiction or outside Indonesian legal jurisdiction) as long as the legal act has legal consequences in Indonesian legal jurisdiction and/or outside Indonesian legal jurisdiction and harms Indonesian interests.

While in the Telecommunications Law, it is not explained who is meant by "person", however in general criminal law terminology, the "person" referred to is an individual/person who commits a criminal act. Thus, sanctions regarding wiretapping in normative provisions only apply to individuals or legal entities, and certainly do not apply to other states institutionally.

4. CONCLUSION

Interception or wiretapping in the context of Islamic criminal law is equated with the term Tajassus which means to investigate or to spy. From this definition, we can draw the conclusion that tajassus is seeking the faults of others by investigating them or spying on them, and this attitude of tajassus is an attitude that is prohibited in the Qur'an and

hadith. Furthermore, it is explained in narrations that Umar bin Khaththab radhiyallahu 'anhu emphasized

حممَلًا ولا تظنَّنَّ بكلمة خرجت من أخيك المؤمن إلَّا خيراً، وأنت تجد لها في الخير

> "Do not have ill thoughts about words that come out from your believing brother except with good thoughts. And you should always carry his words to good assumptions."

Based on this narration, it can be understood that Islam prohibits actions of having bad suspicions or spying on others with the purpose of seeking faults committed. Based on this narration as well, the scholars provide explanations about the prohibition of interception or *tajassus* as stated by Abu Bakar bin Jabir al-Jazairi who said that it is forbidden to seek faults and investigate the defects of Muslims and spread them and examine them. He also emphasized do not investigate the aurat (defects) of Muslims and do not investigate them. Al-Jazairi's statement is clarified by al-Usaimin who said that tajassus is seeking the defects of others or investigating the wrongdoings of one's brother, and this is a despicable act and must be punished for whoever commits it.

A more specific opinion is expressed by Nabhani who said that the prohibition of tajassus against Muslims in the Qur'an is general in meaning that it applies to individuals, groups, and states whether carried out for personal, group, or state interests. While according to Ali Ash-Shobuni, the act of wiretapping, spying, or seeking the faults of others secretly, as well as monitoring the defects of others is an action that can be categorized as tajassus which is haram in law and its perpetrator must be severely punished according to the level of harm caused, except if there is already clear evidence that can endanger the ummah in general.

ACKNOWLEDGEMENTS

I express my gratitude to all parties who have contributed to the preparation of this article. Specifically, I would like to convey my appreciation to researchers for their valuable suggestions and input that assisted in the preparation of this article. I am also grateful to State Islamic University Sunan Ampel Surabaya which has provided support, whether in the form of facilities, data, or other resources. Not to forget, I extend my appreciation to colleagues and fellow academics who have provided insights, discussions, and moral encouragement during the writing process. Finally, I express my gratitude to my family and all parties who have provided support, both directly and indirectly, in completing this article. May this work provide benefits to readers and the academic world.

REFERENCES

Aldi, M., & Kawakib, A. N. (2025). Reconstruction of Islamic Education Philosophy in Minangkabau Customary Values: Actualizing the Principles of Adat Basandi Syarak, Syarak Basandi Kitabullah. *JIIP-Jurnal Ilmiah Ilmu Pendidikan*, *8*(2), 1548–1557.

Amiri, S. M. H. (2025). *Privacy in Islam: What Muslims Should Know About Data Protection*. Dhaka College.

An-Na'im, A. A. (2017). Islam and human rights: Beyond the universality debate. In *International Law and Islamic Law* (pp. 399–407). Routledge.

An-Nabhani, T. (2003). *Asy-Syakhshiyyah al-Islamiyyah* (6th ed.). Dar al-Ummah.

Appelstrand, M. (2002). Participation and societal values: the challenge for lawmakers and policy practitioners. *Forest Policy and Economics*, *4*(4), 281–290.

Aspinall, E., Mietzner, M., & Tomsa, D. (Eds.). (2015). *The Yudhoyono Presidency: Indonesia's Decade of Stability and Stagnation*. Institute of Southeast Asian Studies.

Azizi, F. (2020). *Penafsiran Al-Zamakhsyari terhadap Ayat-Ayat yang Menjadi Landasan Faham Jabariyyah dalam Tafsir Al-Kasysyaf*. UIN Sunan Gunung Djati Bandung.

Berween, M. (2017). Non-Muslims in the Islamic state: Majority rule and minority rights. In *International Law and Islamic Law* (pp. 599–610). Routledge.

Cownie, F., & Bradney, A. (2013). Socio-legal studies: a challenge to the doctrinal approach. In *Research methods in law* (pp. 42–62). Routledge. https://doi.org/10.4324/9780203489352-8

Craig, G., Burchardt, T., & Gordon, D. (Eds.). (2008). *Social Justice and Public Policy: Seeking Fairness in Diverse Societies*. Policy Press.

Dewi, S. (2018). Privacy: An overview of Indonesia statutes governing lawful interception. *Central European Journal of International and Security Studies*, *12*(4), 586–597.

Fadhil, M. (2020). The Harmonization of Wiretapping Regulations in Indonesia: Law Enforcement Perspective. *Jurnal Ilmiah Simantek*, *4*(3), 234–243.

Feener, R. M. (2013). *Shari'a and social engineering: The implementation of Islamic law in contemporary Aceh, Indonesia*. OUP Oxford.

Gul, S., Ahmad, R., & Rahman, S. U. (2025). Constitutional Dualities: Reconciling Islamic Normativity with Common Law Principles in Hybrid Legal Systems. *Indus Journal of Social Sciences*, *3*(2), 674–693. https://doi.org/10.59075/ijss.v3i2.1501

Hairong, M., & Ma, M. (2008). Research on lawful interception in information society from a comparative law perspective. *International Journal of Liability and Scientific Enquiry*, *1*(4), 392–401.

Hammar, R. K. R. (2018). The existence of customary rights of customary law community and its regulation in the era of special autonomy of Papua. *Journal of Social Studies Education Research*, *9*(1), 201–213.

Hochman, B. (2022). *The Listeners: A History of Wiretapping in the United States*. Harvard University Press.

Huda, M. C. (2022). *Metode Penelitian Hukum (Pendekatan Yuridis Sosiologis)*. IAIN Salatiga.

Jordan, M. E., Kleinsasser, R. C., & Roe, M. F. (2014). Wicked problems: Inescapable wickedity. *Journal of Education for Teaching*, *40*(4), 415–430.

Kamali, M. H. (2019). *Crime and punishment in Islamic law: A fresh interpretation*. Oxford University Press.

Koto, I. (2021). Cyber crime according to the ITE law. *International Journal Reglement \& Society (IJRS)*, *2*(2), 103–110.

Lestari, W. (2024). Ta'zir Crimes in Islamic Criminal Law: Definition Legal Basis Types and Punishments. *Al-Qanun: Jurnal Kajian Sosial Dan Hukum Islam*, *5*(1), 22–32.

Mukharrom, T., & Abdi, S. (2023). Harmonizing Islam and Human Rights Through the Reconstruction of Classical Islamic Tradition. *Samarah: Jurnal Hukum Keluarga Dan Hukum Islam*, *7*(1), 40–57.

Nour, M. M. A. (2024). From politics to social justice: A political analysis of social policy. *Politik Psikoloji Dergisi*, *4*(1).

Praditha, D. G. E. (2024). The Role of Balinese Customary Law as a Social Institution for Immigrants and Tourists: Sanctions in Awig-Awig Against Krama Adat, Krama Tamiyu, and Tamiyu. *Istinbath: Jurnal Hukum*, *21*(01), 176–187.

Raharjo, S. (1983). *Hukum dan Perubahan Social*. Alumni.

Soekanto, S. (1989). *Pokok-pokok sosiologi hukum*. Rajawali pers.

Soekanto, S., & Mamudji, S. (1994). *Penelitian Hukum Normatif*. PT. Raja Grafindo Persada.

Widiawan, M. A., & Junaidi, M. (2024). Corruption Arrest Hand Operation based on

Wiretapping Process Conducted by The Corruption Eradication Commission from The Perspective of Islamic Criminal Law. *Proceeding International Conference Restructuring and Transforming Law*, *3*(1).