The Easta Journal Law and Human Rights
Vol. 5, No. 01, October 2026, pp. 73 – 82
ISSN: 2985-7112, DOI: 10.58812/eslhr.v5i01

The Limits of State Intelligence Authority Over Private Spaces from a Criminal Law Perspective

Nurmutia Sjafar
Fakultas Hukum, Universitas Negeri Gorontalo

Article Info

Article history:

Received May 25, 2026
Revised June 9, 2026
Accepted July 10, 2026

Keywords:

Criminal Law;
Legality;
Privacy;
State Intelligence;
Surveillance

ABSTRACT

The development of information technology has expanded the operational mechanisms of state intelligence through *surveillance* activities targeting citizens' private spaces. This situation raises legal issues when surveillance is conducted without clear limits on authority and has the potential to conflict with criminal law. This study aims to analyze the limits of state intelligence authority over private spaces and to examine the legality of *surveillance* actions from a criminal law perspective. This study employs a normative legal research method using a statutory approach and a conceptual approach. Legal materials were obtained through a literature review of relevant legislation, books, journals, and legal doctrines. The results of the study indicate that the authority of state intelligence is not absolute, as it remains constrained by the principles of legality, proportionality, and the protection of citizens' private rights. *Surveillance* activities are only justified if conducted based on lawful authority, have a clear national security objective, and are carried out proportionally. Surveillance activities conducted without a clear legal basis have the potential to constitute an unlawful act from a criminal law perspective.

This is an open-access article under a CC BY-SA license.

Corresponding author:

Name: Nurmutia Sjafar
Institution: Fakultas Hukum, Universitas Negeri Gorontalo
Email: nurmutiasjafar40@gmail.com

1. INTRODUCTION

Advances in information technology have transformed the operations of state intelligence agencies, making them increasingly complex, secretive, and difficult to oversee legally. Intelligence activities are no longer limited to conventional information gathering but have expanded to include monitoring digital communications, tracking electronic activities, collecting personal data, and even surveillance of citizens' private spaces[1]. This situation places the intelligence function in a problematic position because, on the one hand, it is necessary for the sake of national security, while on the other hand, it has the potential to conflict with criminal law norms that protect the private rights of every individual.

The state, through the National Intelligence Agency, is granted the authority to conduct investigations, security operations, and intelligence gathering to maintain national stability, as stipulated in Law No. 17 of 2011 on State Intelligence. In practice, this authority is often exercised through

surveillance mechanisms conducted covertly and in secret. The nature of intelligence work raises legal issues when. private sphere without the consent of the subject being monitored [2]. This situation raises questions regarding the legal limits of intelligence actions from a criminal law perspective.

The right to privacy is part of the fundamental rights that receive legal protection under the Indonesian legal system. Article 28G of the 1945 Constitution of the Republic of Indonesia guarantees protection of the sense of security, honor, dignity, and personal safety of every citizen. Similar protections are also found in Law No. 27 of 2022 on Personal Data Protection and several provisions in the Criminal Code that prohibit unauthorized access to an individual's personal information [3]. These norms indicate that private spaces are objects of legal protection that cannot be entered arbitrarily, including by state officials.

In reality, intelligence *surveillance* practices do not always operate within clear boundaries. Allegations of illegal wiretapping targeting human rights activists, journalists, and opposition groups have repeatedly surfaced in the Indonesian public sphere. The 2019 case involving alleged hacking and surveillance of digital accounts belonging to democracy activists is one example that has drawn criticism regarding the weakness of oversight mechanisms for state intelligence activities. A similar situation also arose in a case of personal data leaks allegedly involving institutional access to specific electronic systems without the data owners' consent [4].

These phenomena reveal a very fine line between intelligence actions deemed lawful in the interest of national security and actions that potentially constitute criminal offenses. Covert information gathering, by its very nature, shares characteristics with several forms of modern criminal acts, such as illegal access, unauthorized wiretapping, personal data breaches, and violations of communication secrecy. The difference between the two lies solely in the basis of legitimacy granted by the state.

The absence of clear parameters regarding the boundaries of private space that state intelligence may enter leads to ambiguity in legal norms during law enforcement practices. The State Intelligence Act provides only general provisions regarding the functions and authority of intelligence agencies without detailing the limits of *surveillance* activities that are criminally justifiable [5]. Such conditions create opportunities for abuse of authority that is difficult to control, as intelligence activities are inherently secretive and shielded from public oversight.

This issue has become increasingly relevant with the development of digital technology, which enables massive and systematic surveillance. The use of digital *surveillance* devices, electronic location tracking, and social media monitoring makes private spaces increasingly vulnerable to intrusion without the data owner's consent. These developments present new challenges for criminal law because existing mechanisms for protecting privacy rights have not yet fully kept pace with the operational patterns of modern intelligence, which operate covertly and are technology-driven.

Studies on state intelligence have been extensively conducted by previous scholars. A study conducted by Mutia Jawaz Muslim and Aulia Fikrina in 2024, entitled The Supervisory Mechanism of the State Intelligence Agency of the Republic of Indonesia within a Democratic Legal Framework, examined the oversight mechanisms of the State Intelligence Agency in a democratic system, including internal supervision, presidential oversight, and parliamentary control exercised by the House of Representatives [6]. The study found that oversight serves as an essential instrument for maintaining the accountability of intelligence institutions without diminishing the effectiveness of their operational functions. Nevertheless, the research primarily focused on institutional aspects and the governance of intelligence oversight, and therefore did not address the legality of intelligence activities from a criminal law perspective, particularly

concerning the protection of citizens' private sphere

Another study was conducted by Silvi Habsari Duria Sumariyastuti in 2019 under the title Wiretapping from a Human Rights Perspective. The research focused on the position of wiretapping as a limitation on citizens' right to privacy and its relevance to fundamental human rights principles. The findings indicated that wiretapping may only be justified when carried out on a legal basis, for a legitimate purpose, and through adequate oversight mechanisms[7]. However, the study was primarily oriented toward constitutional law and human rights approaches, and therefore did not explore the possibility of intelligence activities being classified as criminal acts when conducted beyond the scope of authority granted by statutory regulations.

A subsequent study was conducted by Clifford Deannova Saputra et al. in 2024 through research entitled Legal Perspectives on Privacy and Personal Data Protection in the Digital Era. The study examined the protection of privacy rights and personal data amid the rapid development of digital technologies, as well as various legal challenges arising from the increasing collection and processing of electronic data. Its primary focus was directed toward personal data protection, information security, and legal accountability within the digital environment [7]. Consequently, the study did not specifically analyze surveillance activities carried out by state intelligence agencies nor the potential criminal liability arising from intelligence actions that intrude upon citizens' private sphere without a lawful basis of authority

The fundamental difference between this study and previous research lies in the study's focus, which is specifically directed at the limits of state intelligence authority from a criminal law perspective. This study does not treat intelligence activities solely as a matter of administrative authority or human rights violations, but rather as a matter of criminal legality related to the potential for unlawful acts against citizens' private spheres. This position gives the study a distinct orientation by directly positioning *surveillance* activities as the subject of criminal law analysis.

A criminal law approach is essential given that the nature of intelligence activities fundamentally resembles various forms of modern criminal offenses regulated under Indonesian legislation. Unauthorized access to electronic systems, the covert collection of personal data, and the monitoring of private communications are acts that, under certain conditions, may constitute criminal offenses if carried out without a valid legal basis. Such circumstances highlight the need for clear normative boundaries to ensure that intelligence authority does not evolve into an instrument of power that exceeds the principles of criminal legality.

Based on the above discussion, this study aims to examine the limits of state intelligence authority over private spaces from a criminal law perspective and to analyze the legality of intelligence *surveillance* activities when linked to the elements of criminal acts within the Indonesian legal system.

2. LITERATURE REVIEW

2.1 The Concept of State Intelligence Authority

State intelligence authority is a special form of authority granted by the state to intelligence agencies to carry out investigative, security, and intelligence-gathering functions in order to maintain national stability. These functions are carried out through covert information-gathering mechanisms to detect threats to national security and sovereignty. According to Loch K. Johnson, intelligence activities are essentially state instruments that operate through *surveillance*, information analysis, and covert operations to support national security policy-making [8]. The secretive nature of intelligence work often places these activities in a legal gray area that is difficult to oversee.

Law No. 17 of 2011 on State Intelligence provides legal legitimacy for the exercise of intelligence functions in

Indonesia. These authorities include investigation, security measures, and countermeasures against all forms of threats that could potentially disrupt national interests. Legal issues arise when the exercise of these authorities encroaches upon citizens' private spheres through *surveillance*, communication monitoring, or the collection of personal data. According to Frederic H. Gareau, the expansion of intelligence authority without clear legal restrictions has the potential to lead to *abuse of power* because intelligence activities essentially operate through intervention in the private sphere of individuals [10].

2.2 *Protection of the Private Sphere in Criminal Law*

The private sphere is part of the fundamental rights that are protected under modern legal systems. This protection encompasses private communications, electronic data, personal life, and individual information that cannot be accessed arbitrarily by others. Samuel Warren and Louis Brandeis stated that the right to privacy is a person's right to enjoy their private life without interference from others, including the state [11]. This concept later evolved into the foundation for privacy protection in various modern criminal legal systems.

From a criminal law perspective, violations of private space are considered unlawful acts if committed without a valid legal basis. Eddy O.S. Hiariej explains that entering private space through wiretapping, accessing electronic data, or monitoring communications without authorization may constitute a criminal offense because it violates the principles of legality and the protection of individual rights [12]. This protection is further strengthened by Law No. 27 of 2022 on Personal Data Protection, which prohibits the use of personal data without the data subject's consent. This regulation demonstrates that private space is a subject of legal protection with criminal law dimensions.

2.3 *The Legality of Surveillance from a Criminal Law Perspective*

Surveillance is a monitoring method used to obtain specific information through direct or electronic monitoring of specific individuals or groups. The development of digital technology has shifted *surveillance* away from conventional methods toward electronic data tracking, social media monitoring, and the systematic collection of digital information. David Lyon explains that modern *surveillance* has evolved into a mechanism of social control capable of penetrating nearly every aspect of society's private life through information technology [13]. This situation raises legal questions regarding the boundaries of the state's surveillance authority.

Criminal law establishes the principle of legality as the foundation for limiting any actions that may infringe upon individual rights. Barda Nawawi Arief states that state authority must remain subject to the principle of legality to prevent it from evolving into repressive actions that violate citizens' rights [14]. *Surveillance* activities by state intelligence agencies are permissible provided they are conducted within lawful authority, are proportionate, and have a clear legal basis. Conversely, *surveillance* actions conducted beyond the bounds of authority have the potential to be classified as criminal acts, particularly if they involve unauthorized access to communications, personal data, or an individual's private sphere.

3. METHOD

This study employs a normative legal research method with an approach focused on analyzing positive legal norms, legal principles, and criminal law doctrines related to state intelligence authorities' powers regarding private spaces. The normative legal research is conducted through an examination of laws and regulations governing state intelligence functions, the protection of privacy rights, and criminal provisions

regarding unauthorized access and *surveillance* activities [15]. This approach is used to analyze the legal boundaries of intelligence activities from a criminal law perspective and to assess the potential for unlawful acts in the execution of state intelligence functions.

The research approaches used consist of *the statutory approach* and *the conceptual approach*. The statutory approach was conducted by examining various regulations related to the research, including Law No. 17 of 2011 on State Intelligence, the Criminal Code, Law No. 27 of 2022 on Personal Data Protection, and the Law on Information and Electronic Transactions. The conceptual approach is used to examine the concepts of legality, protection of privacy rights, *surveillance*, and the limits of state authority in criminal law based on expert opinions and evolving legal doctrines [16].

The legal materials in this study consist of primary, secondary, and tertiary sources. Primary legal materials include legislation and official legal documents related to intelligence authority and the protection of privacy rights. Secondary legal materials were obtained from books, scientific journals, and previous research relevant to the study's theme. Tertiary legal materials include legal dictionaries, language dictionaries, and electronic sources that support the explanation of legal terms. The collection of legal materials was conducted through a literature review, followed by qualitative analysis using a descriptive-analytical method to derive legal arguments regarding the limits of state intelligence authority over private spaces from a criminal law perspective [17].

4. RESULTS AND DISCUSSION

4.1. The Limits of State Intelligence Authority Over Private Spaces from a Criminal Law Perspective

State intelligence authority is, in principle, a special authority granted by the state to maintain national security stability through investigative, security, and intelligence-gathering activities. The covert nature of intelligence work means that the exercise of this authority often directly encroaches upon the private sphere of citizens. Legal issues arise when *surveillance* is conducted without clear limiting parameters, thereby potentially violating criminal law norms [18]. Such a situation places intelligence functions in a dilemma because the state is required to maintain national security, yet at the same time is obligated to respect the right to privacy as part of every individual's legal rights.

Law No. 17 of 2011 on State Intelligence does indeed provide legitimacy for the exercise of state intelligence functions. However, the law does not provide detailed operational boundaries regarding which private spaces may be accessed through *surveillance* activities. This regulatory gap creates legal ambiguity because covert information-gathering activities, by their very nature, share characteristics with certain forms of modern criminal offenses, such as unauthorized access to electronic systems, illegal wiretapping, or the collection of personal data without the data subject's consent.

From a criminal law perspective, the principle of legality serves as the primary foundation for determining the legality of an act. This principle asserts that no act can be justified without a clear legal basis. Consequently, intelligence activities that intrude into citizens' private spheres cannot be justified solely in the name of national security if their implementation lacks clear legal parameters. State authority must remain subject to the bounds of legality to prevent it from becoming a repressive instrument of power that violates individual rights [19].

In practice, intelligence *surveillance* activities are carried out through various methods, ranging from monitoring electronic communications, collecting digital data, tracking social media activity, to monitoring the movements of specific individuals. These mechanisms constitute a substantial

form of intervention into private spaces because they are carried out without the consent of the subjects being monitored. The issue becomes increasingly complex when surveillance is conducted covertly and without adequate external oversight mechanisms [20]. Such conditions create opportunities for abuse of authority that is difficult to control through ordinary legal mechanisms.

Indonesian criminal law has, in fact, provided protection for private spaces through various statutory provisions. The Criminal Code prohibits the unlawful entry into private premises, while the Law on Information and Electronic Transactions prohibits unauthorized electronic access to another person's electronic systems. Similar protections are further reinforced by the Personal Data Protection Act, which designates personal data as part of private rights that the state is obligated to protect. The existence of these regulations demonstrates that criminal law views private spaces as objects of legal protection that cannot be entered arbitrarily [21].

The main issue lies in the absence of clear parameters regarding the limits of criminal justification for state intelligence actions. The state does indeed have the authority to conduct surveillance for the sake of national security, but this authority is not absolute. *Surveillance* actions must still adhere to the principles *of necessity, proportionality,* and *legality* to avoid becoming unlawful acts. When surveillance is conducted excessively and exceeds the needs of national security, such actions risk losing their legal legitimacy [22].

The alleged wiretapping of democracy activists and journalists in Indonesia demonstrates how state *surveillance* activities can raise serious concerns regarding the protection of private space. The alleged hacking of activists' digital accounts in 2019 indicates that surveillance technology can be directed at specific civilian groups without a transparent legal basis. This situation raises concerns that intelligence powers may be used excessively beyond the primary objective of safeguarding national security. The secrecy surrounding intelligence mechanisms makes it difficult for the public to ascertain the legality of such actions [23].

A similar phenomenon has occurred at the international level through the mass *surveillance* practices carried out by *the National Security Agency* (NSA) in the United States and exposed by Edward Snowden in 2013. Surveillance of the public's digital communications was conducted on a massive scale under the pretext of safeguarding national security in the wake of the global terrorism threat. These practices subsequently drew international criticism as they were deemed to violate citizens' privacy rights and contradict the principles of human rights protection [24]. This case demonstrates that intelligence activities without strict legal constraints have the potential to evolve into systematic violations of citizens' private spheres.

The absence of effective oversight mechanisms is a primary factor amplifying the potential for abuse of intelligence authority. The secretive nature of intelligence work makes *surveillance* activities difficult to challenge through standard criminal evidentiary procedures. Such conditions create a legal imbalance because the subjects who are victims of surveillance often do not know that their private sphere has been secretly intruded upon. Consequently, legal protection of the right to privacy becomes weak because violations are difficult to prove and difficult to hold criminally accountable.

A criminal law perspective emphasizes that the legitimacy of state authority cannot negate the unlawful nature of an act if that act is carried out beyond the limits of authority granted by law. This principle is crucial to ensure

that intelligence authority does not evolve into unchecked power. A rule-of-law state ensures that all actions by state officials remain subject to the supremacy of the law, including those carried out in the name of national security [25]. Therefore, intelligence *surveillance* activities must be strictly limited to avoid conflicting with the principle of criminal legality.

The vagueness of norms in the regulation of state intelligence indicates an urgent need to establish clearer boundaries of authority within the Indonesian legal system. Regulations that are too general regarding intelligence functions create broad room for interpretation and the potential for abuse in practice. This lack of clarity ultimately leads to legal uncertainty regarding when intelligence actions are justified and when they become acts that violate criminal law. Such a situation is dangerous because it can gradually erode legal protections for the public's private sphere.

4.2. *The Legality of State Intelligence Surveillance Actions from a Criminal Law Perspective*

The legality of *surveillance* actions by state intelligence is a fundamental issue in criminal law because it is directly related to the limits of justification for an act that, under certain conditions, possesses the characteristics of a criminal offense. *Surveillance* activities are essentially carried out through covert monitoring, surveillance, wiretapping, and the collection of information regarding specific individuals. Problems arise when such actions intrude into citizens' private spheres without consent and are carried out through non-transparent mechanisms [26]. Such conditions raise questions regarding whether intelligence actions can be fully justified in the name of national security or whether they are, in fact, potentially unlawful acts from a criminal law perspective.

Indonesian criminal law establishes the principle of legality as a fundamental tenet in determining the validity of an action. This principle asserts that any action restricting individual rights must have a clear and explicit legal basis. Consequently, *surveillance* activities by state intelligence agencies cannot be justified solely on the grounds of national security interests without normative parameters defining the limits of their implementation. The absence of detailed regulations regarding the methods and limits *of surveillance* creates an overly broad scope of interpretation for intelligence officials in exercising their authority [27].

Law No. 17 of 2011 on State Intelligence does indeed provide legitimacy for the functions of state intelligence. However, this regulation focuses more on institutional functions rather than the operational limits of *surveillance* actions against citizens. Provisions regarding wiretapping and information collection remain general in nature and do not specifically outline mechanisms to protect citizens' privacy. This ambiguity in the norms has the potential to lead to *surveillance* practices that exceed the principles of criminal legality due to the absence of clear standards regarding permitted and prohibited actions.

Surveillance activities share a close resemblance with certain forms of modern criminal offenses. Intercepting private communications without consent, accessing electronic systems without authorization, or secretly collecting personal data are acts that, under criminal law, can be classified as criminal offenses if carried out without legal justification. The main issue lies in the fact that intelligence activities are often carried out through methods that are substantially identical to the elements of such criminal acts. The distinction between the two depends solely on the existence of a legally valid basis of authority [28].

The Electronic Information and Transactions Law explicitly prohibits unauthorized access to another person's electronic system. A similar prohibition is also found in the Personal Data Protection Act, which provides protection against the use of personal data without the data subject's consent. The existence of these regulations demonstrates that Indonesian criminal law provides strong protection for citizens' private sphere. Therefore, state intelligence *surveillance* activities cannot be separated from the obligation to respect the principle of protection of private rights guaranteed by national criminal law.

The principles *of necessity* and *proportionality* are crucial elements in determining the legality of state intelligence *surveillance* actions. *Surveillance* is only justified if it is truly necessary for the sake of national security and is conducted in a manner proportional to the threat faced by the state. Surveillance actions carried out excessively, on a massive scale, and without a clear basis of threat risk losing their legal legitimacy. Such a situation causes intelligence actions to no longer fall within the scope of national security protection but instead transform into a form of intervention that violates citizens' privacy rights [29].

The case of mass *surveillance* by *the National Security Agency* (NSA) in the United States demonstrates how intelligence activities can escalate into serious violations of citizens' privacy. The revelations made by Edward Snowden in 2013 revealed the widespread collection of public communication data without the consent of the individuals being monitored. This practice drew international criticism as it was deemed to violate the principles of legality and the protection of privacy rights. This case demonstrates that national security is often used as a justification to excessively expand state surveillance.

A similar phenomenon is also beginning to emerge in digital surveillance practices in Indonesia. Allegations of hacking and monitoring of activists, journalists, and civil society groups indicate that *surveillance* technology can be used excessively without effective oversight mechanisms. The secrecy surrounding intelligence operations makes it difficult for the public to obtain certainty regarding the legal basis for such actions. Consequently, there is a potential for criminal violations of privacy that are difficult to prove because *surveillance* activities are conducted covertly.

The criminal law perspective emphasizes that the state cannot exercise authority absolutely without clear legal boundaries. The principle of the rule of law ensures that all actions by state officials remain subject to the law, including those carried out by intelligence agencies. Intelligence authority is fundamentally not a form of unchecked power, but rather an authority that must remain limited to prevent the abuse of power. Therefore, *surveillance* actions must have a specific legal basis, clear objectives, and accountability mechanisms that can be legally challenged.

The absence of strong control mechanisms over intelligence activities risks creating legal impunity. The secretive nature of intelligence work makes it difficult to prove violations of privacy through ordinary criminal mechanisms. This situation creates an imbalance because citizens who are victims *of surveillance* often do not realize that their right to privacy has been violated. Consequently, legal protection of privacy becomes ineffective due to the lack of adequate access to challenge the legality of intelligence actions.

Issues regarding the legality *of surveillance* are also closely tied to the development of modern digital technology. The use of surveillance software, electronic location tracking, and social media monitoring makes the public's private sphere increasingly vulnerable to covert intrusion. These developments indicate that criminal law

can no longer view violations of private space solely in conventional terms. Digital *surveillance* activities have given rise to new forms of intervention into private rights that require stricter and more specific legal restrictions [30].

The legality of state intelligence *surveillance* activities from a criminal law perspective can only be justified if they are carried out based on lawful authority, comply with the principle of legality, are proportionate, and are conducted in the interest of genuine national security. *Surveillance* activities conducted without clear limits, without oversight mechanisms, and exceeding the needs of national security have the potential to constitute an unlawful act and are contrary to the fundamental principles of modern criminal law.

5. CONCLUSION

State intelligence surveillance is an instrument that may be legally justified provided that it is carried out in accordance with the principles of legality, necessity, and proportionality. This study demonstrates that the legality of surveillance is determined not only by its objective of safeguarding national security, but also by the existence of a clear legal basis, well-defined limitations on authority, and effective oversight mechanisms. Surveillance measures conducted without an adequate legal foundation or beyond the scope of authority granted by law may violate citizens' privacy rights and, in certain circumstances, may exhibit characteristics comparable to acts that qualify as criminal offenses.

Therefore, it is necessary to strengthen the legal framework governing intelligence surveillance by establishing clear limitations on surveillance powers, including procedures for implementation, conditions for use, and mechanisms of legal accountability. In addition, the state should enhance independent oversight of intelligence activities through legislative, judicial, and institutional review mechanisms in order to prevent abuses of power. Strengthening the protection of personal data and privacy rights must also become a central component of surveillance policy development to ensure an appropriate balance between national security interests and the protection of human rights within a democratic state governed by the rule of law.

ACKNOWLEDGMENTS

The author would like to express gratitude to all parties who have provided support, assistance, and contributions to the process of compiling this research, both academically and morally, so that this research could be successfully completed.

REFERENCES

[1] A. Ariayuda, S. Hardjomuldjadi, S. Sami'an, and D. Edi Wibowo, "The Binding Force of Goods/Services Procurement Contracts from the Perspective of Article 1338 of the Indonesian Civil Code," *Interdiscip. Soc. Stud.*, vol. 5, no. 1, pp. 359–368, 2025, doi: 10.55324/iss.v5i1.988.

[2] S. Kaulika Katuuk, M. Sepang, and N. Nachrawy, "Functions, Duties, and Authorities of the State Intelligence Agency Based on Law Number 17 of 2011 on State Intelligence," *Lex Priv.*, vol. 11, no. 3, pp. 1–12, 2023.

[3] K. R. Anggen Suari and I. M. Sarjana, "Maintaining Privacy in the Digital Era: Personal Data Protection in Indonesia," *J. Anal. Huk.*, vol. 6, no. 1, pp. 132–142, 2023, doi: 10.38043/jah.v6i1.4484.

[4] O. K. Haris, S. A. Abdullah, A. Rizky, D. Yuningsih, and Z. P. Mustaka, "Criminal Law Policy on Personal Rights in Telephone Wiretapping and Digital Privacy Cases," *Halu Oleo Leg. Res.*, vol. 7, no. 2, pp. 405–419, 2025.

[5] Silvi Habsari Duria Sumariyastuti, "Wiretapping from a Human Rights Perspective," *Yurispruden*, Vol. 2, No. 2, Pp. 135–153, 2019.

[6] E. Mardeson And H. Mardesci, "The Oversight Mechanism of the State Intelligence Agency of the Republic of Indonesia within the Framework of a Democratic Rule of Law," *J. Ris. Indragiri*, Vol. 1, No. 3, Pp. 174–181, 2022, [Online]. Available: Http://Repository.Unisi.Ac.Id/Id/Eprint/329

[7] C. D. Saputra, G. S. Saputra, F. Aprilliani, And I. Martinelli, "Legal Perspectives on Privacy and Personal Data Protection in the Digital Era," *J. Ilmu Hukum, Hum. Dan Polit.*, Vol. 5, No. 1, Pp. 799–810, 2024, [Online]. Available: Https://Dinastirev.Org/DOI:Https://Doi.Org/10.38035/Jihhp.Https://Creativecommons.Org/Licenses/By/4.0/

[8] P. Gill, "Intelligence, Threat, Risk And The Challenge Of Oversight," *Intell. Natl. Secur.*, Vol. 27, No. 2, Pp. 206–222, 2012.
[9] S. D. Warren And D. Louis, "Brandeis, The Right To Privacy, 4 Harv," *L. Rev*, Vol. 193, No. 10.2307, Pp. 193–195, 1890.
[10] E. O. S. Hiariej, *Principles of Criminal Law*. 2022.
[11] D. Lyon, "Surveillance Studies: An Overview," Pp. 13–18, 2007.
[12] E. A. Putri *Et Al.*, "Lawful Interception Actions by Investigators," Vol. 6, No. 1, Pp. 324–330, 2025.
[13] W. S. Widiarty, "*Textbook of Legal Research Methods.*" Publika Global Media, Pp. 55–60, 2024.
[14] E. A. Putri, S. Rahayu, And S. Lasmadi, "Lawful Interception by Investigators in Law Enforcement," PAMPAS: Journal Of Criminal Law, Vol. 6, No. 3, Pp. 325–341, 2025.
[15] M. M. Hutajulu, "Human Rights Protection," Vol. 8, No. 2, Pp. 363–370, 2026.
[16] C. Insights, "Democratizing Intelligence Oversight In Indonesia :," Pp. 802–815, 2024.
[17] D. Lyon, *Pandemic Surveillance*. John Wiley & Sons, 2021.
[18] S. D. Rosadi, *Discussion of the Personal Data Protection Law (Law of the Republic of Indonesia No. 27 of 2022)*. Sinar Grafika, 2023.
[19] N. Harisudin And M. H. T. Rahman, "Digital Constitutionalism, Privacy, and Human Rights: A Juridical Review of the Indonesian Legal Framework in the International Context," *Konf. Nas. Asos. Pengajar Huk. Tata Negara Dan Huk. Adm. Negara*, Vol. 3, No. 1, Pp. 467–469, 2025.
[20] Southeast Asia Freedom Of Expression Network (Safenet), "Indonesia Digital Rights Situation Report 2019: The Rise of Digital Authoritarianism," 2020. [Online]. Available: Https://Safenet.Or.Id/Id/2020/10/Laporan-Situasi-Hak-Hak-Digital-Indonesia-2019-Bangkitnya-Otoritarian-Digital/
[21] Ian Black, "NSA Spying Scandal: What We Have Learned," The Guardian. Accessed: Jun. 13, 2026. [Online]. Available: Https://Www.Theguardian.Com/World/2013/Jun/10/Nsa-Spying-Scandal-What-We-Have-Learned?CMP=Share_Btn_Url
[22] C. S. T. Kansil and N. A. Putri, "Implementation of the Rule of Law Principle in the National Legal System: A Case Study on Human Rights Protection," *J. Pendidik. Sej. dan Ris. Sos. Hum.*, vol. 4, no. 2, pp. 74–81, 2024.
[23] Sophie Duroy, *The Regulation of Intelligence Activities under International Law*. Cheltenham, UK: Edward Elgar Publishing, 2023. doi: 10.4337/9781803927084.
[24] A. Hafizah, M. Ablisar, and R. Lubis, "The Principle of Legality in Indonesian Criminal Law and Islamic Criminal Law," *Mahadi Indones. J. Law*, vol. 1, no. 1, pp. 1–10, 2022, doi: 10.32734/mah.v1i1.8311.
[25] A. R. T. Nainggolan, V. V. Sumilat, and V. A. Wongkar, "The Application of Criminal Provisions for the Offense of Interception or Wiretapping of Electronic Information or Electronic Documents," *Lex Crim.*, vol. X, no. 3, pp. 151–161, 2021.
[26] E. I. Maulidina, "The Urgency of Necessity and Proportionality Tests in the Exemption of Personal Data Subject Rights in Indonesia," *J. Anal. Huk.*, vol. 7, no. 2, pp. 143–159, 2024, doi: 10.38043/jah.v7i2.5464.
[27] N. A. Qurrotuaini, "The Right to Privacy as a Constitutional Right in the Digital Era: A Juridical Study from the Perspective of Cyber Law," *Staatsr. J. Huk. Kenegaraan dan Polit. Islam*, vol. 4, no. 2, pp. 235–254, 2025, doi: 10.14421/a9d95k61.