
The Principle of Legality in Cyber Crimes Comparative Study between Indonesian ITE Law and International Cyber Law

Robert Napitupulu *1, Riza Zarzani *2

¹²Panca Budi Development University

E-mail: robertnapitupulu25@gmail.com rizarzarzani@gmail.com

Abstract

The principle of legality is a fundamental principle in modern criminal law, which demands that no act can be punished without pre-existing legal provisions. In the context of cybercrime, the application of the principle of legality faces significant challenges due to the transnational, complex, and rapidly evolving nature of cyber. This study aims to analyze the extent to which the provisions of cyber crimes in the Indonesian Electronic Information and Transactions Law (UU ITE) fulfill the principle of legality, especially the elements of *lex scripta*, *lex certa*, and *lex stricta*, and to compare them with the provisions of the Budapest Convention on Cybercrime and its implementation in countries such as Germany and Japan.

Through a normative legal approach and comparative legal method, this study found that although the ITE Law has formally fulfilled *lex scripta*, many of its provisions are still vague and open to multiple interpretations, thus failing to fulfill the elements of *lex certa* and *lex stricta*. Articles such as Article 27 paragraph (3) and Article 28 paragraph (2) of the ITE Law are often used excessively and repressively, without adequate legal certainty. In contrast, the Budapest Convention emphasizes the formulation of detailed, proportional criminal norms that uphold human rights. The results of this study indicate that cyber criminal law reform in Indonesia is urgently needed to be in line with the principles of a democratic state of law. Harmonization with international standards such as the Budapest Convention is an important step to ensure legal certainty, justice, and protection of digital rights in the information era.

Keywords: *Principle of Legality, Ite Law, Cybercrime, Budapest Convention, Lex Certa, Lex Stricta.*

INTRODUCTION

In the development of modern law, the principle of legality (*nullum crimen sine lege, nulla poena sine lege*) is a fundamental foundation in every criminal law system, including cyber criminal law. This principle ensures that no act can be qualified as a crime and no punishment can be imposed without a preceding legal provision. In Indonesia, this principle has gained constitutional legitimacy as stated in Article 1 paragraph (1) of the Criminal Code (KUHP) which reads: "No act can be punished except by virtue of criminal provisions in existing laws and regulations." Even at a higher level, Article 28I paragraph (1) of the 1945 Constitution emphasizes that the right not to be prosecuted on the basis of retroactive law is part of human rights that cannot be reduced under any circumstances (non-derogable rights). (Rank 2019)

However, the emergence of crimes in cyberspace has brought serious challenges to the application of this legality principle. Cyberspace is a new domain that transcends geographical boundaries, state jurisdiction, and traditional characteristics of criminal law. The development of information and communication technology has created forms of crime that were previously unknown in conventional criminal law. (Iskandar 2019) For example, digital identity theft, ransomware attacks, phishing, doxing, spreading hoaxes, and manipulating algorithms in digital political campaigns. All of these crimes require rapid legal adaptation, while criminal law, which is subject to the principle of legality, requires criminal provisions to be formulated in writing, clearly, and definitely before the act is committed.

In the Indonesian context, the regulation of cyber crimes is specifically stated in Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) as amended by Law Number 19 of 2016, as well as in several articles of the Criminal Code. This law was born as a response to the legal need for the increasingly widespread misuse of information technology. However, in its implementation, the ITE Law often draws criticism because it is considered vague, multi-interpretable, and opens up space for criminalization of socially and politically legitimate digital expressions or activities. Several articles such as Article 27 paragraph (3) (insults and defamation), Article 28 paragraph (2) (dissemination of hate information), and Article 45 (criminal threats) are examples of legal norms that are often debated in the context of the principle of legality. The main criticism is the failure to fulfill the elements of *lex certa* and *lex stricta*, namely the demand that criminal norms be formulated firmly, definitely, and not open to multiple interpretations.(Dhadha et al. 2021)

On the other hand, the development of international law and global cybercriminal law policy shows a tendency to increasingly prioritize the soft law approach, harmonization of norms, and the principle of subsidiarity in cybercriminalization. One of the important reference documents in international cybercriminal law is the Budapest Convention on Cybercrime (2001), also known as the European Convention on Cybercrime adopted by the Council of Europe. This convention has become a global benchmark because it offers a legislative model that can be adopted by various countries, including non-European countries. Although Indonesia has not yet ratified the convention, many of its norms have become references in the process of updating national law, including in the RKUHP and the formation of sectoral regulations such as Government Regulations and Regulations of the Minister of Communication and Information.(Rianto, Zarzani, and Saragih 2024)

The main challenge that emerged in this comparative study is the imbalance between the speed of technological development and the speed of legal adaptation. The principle of legality, which was originally designed to provide protection against state arbitrariness in punishing, is now being tested in a different situation. In cyberspace, many actions can result in major losses in a very short time, but there are not necessarily legal norms that specifically prohibit such actions. This creates a legal vacuum, and in some cases encourages law enforcement officers to use rubber articles or expand the meaning of crimes, which is contrary to the spirit of the principle of legality itself.

For example, in cases of insults via social media, law enforcers often use Article 27 paragraph (3) of the ITE Law, which does not define concretely what is meant by "insult". This is different from criminal law in many European countries which require a detailed description of the crime, and can only be applied after going through a court test with strict evidence. In the Budapest Convention itself, it is emphasized that criminalization must be carried out proportionally and must not threaten basic rights such as freedom of expression and privacy. This means that the principle of caution in forming criminal norms is very important so that there is no over-criminalization of digital citizens.(Setiawan 2021)

Furthermore, if we compare it with the practices in countries that have ratified the Budapest Convention, such as Germany, France, or Japan, their approach tends to prioritize the principles of the rule of law, due process, and predictability of the law. In Germany, for example, cyber crimes are strictly codified and placed in the general criminal law structure (*Strafgesetzbuch*), accompanied by clear interpretative guidelines. This shows that the principle of legality in the context of cyber law can no longer be understood rigidly, but must be developed within the framework of human rights protection and digital legal certainty.

Taking this context into account, this research will raise two main focuses, namely:

1. Analyzing the extent to which the provisions on cyber crimes in the Indonesian ITE Law fulfill the principles of legality, including *lex scripta*, *lex certa*, and *lex stricta*. This focus

- will look at the normative wording of certain articles in the ITE Law and assess whether the formulation is sufficient to fulfill the legal clarity required by the principle of legality.
2. Comparing the application of the principle of legality in the regulation of cyber crimes according to the Indonesian ITE Law with the provisions of the Budapest Convention and its legal implementation in countries that have ratified the convention. This focus will explore the global approach to cybercriminal law to see if there are any best practices that can be used as inspiration for legal reform in Indonesia.

This comparative study is important not only for academic purposes, but also to provide practical contributions to national criminal law reform. The Indonesian government is currently promoting the improvement of digital legal regulations, including through the Personal Data Protection Bill and the implementation of the latest National Criminal Code (Law Number 1 of 2023) which has come into effect and will gradually replace the old Criminal Code. Therefore, the study of the principle of legality in the context of cyber crimes is very strategic, especially to ensure that the criminalization process does not harm citizens, but rather strengthens legal protection for the digital community.

Moreover, the principle of legality is a guarantee of procedural and material justice. In the digital era, violations of this principle not only impact individuals, but also the democratic order and human rights protection in general. Therefore, harmonization of national criminal law with international standards is non-negotiable, considering the cross-border nature of cybercrime and the need for transnational legal cooperation. Indonesia needs to ensure that every provision of cybercrime is drafted with the principles of caution, accountability, and high legal certainty. (2013 Investigation)

Ultimately, the urgency of this research lies in the effort to build cybercriminal law that is not only responsive to technological developments, but also consistent with the basic principles of the rule of law. Through a comparative approach, this research is expected to identify the weaknesses and strengths of the national legal system in accommodating the principle of legality, as well as provide concrete recommendations for strengthening the digital criminal justice system in Indonesia.

METHOD

The research method used in this study is a normative legal approach with a comparative legal method. This research is based on an analysis of the laws and regulations in force in Indonesia, especially Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) and its amendments, as well as the Criminal Code (KUHP), in relation to the principle of legality. (Indra Utama Tanjung 2024) Analysis was also conducted on international legal documents such as the Budapest Convention on Cybercrime and its implementation in several countries that have ratified the convention, such as Germany and Japan. The data used were in the form of primary legal materials (statutes, international conventions) and secondary legal materials (literature, journals, and relevant court decisions), which were analyzed qualitatively to identify the conformity of cybercrime norms with the principle of legality and to compare the effectiveness and legal certainty between the Indonesian legal system and international standards.

RESULTS AND DISCUSSION

Cyber Crime Provisions in the Indonesian ITE Law Fulfil the Basic Principles of Legality, Including Lex Scripta, Lex Certa, and Lex Stricta.

The principle of legality in criminal law is a non-negotiable principle. The existence of this principle guarantees that a person cannot be punished for an act that at the time it was committed was not yet determined as a criminal act in written law. In this context, the three main elements of the principle of legality, namely *lex scripta* (must be written), *lex certa* (must be clear), and *lex stricta* (must not be analogous), are parameters for measuring the extent to which a criminal provision meets the principles of a state of law that upholds certainty and justice. In the digital era, where cybercrime is developing very rapidly, the principle of legality is even more important as a control and corrective tool against the possibility of over-criminalization that often occurs due to the law lagging behind the reality of technology. (Sitepu and Piadi 2019)

Law No. 11 of 2008 concerning Information and Electronic Transactions (UU ITE), as amended by Law No. 19 of 2016, is the initial milestone in the formation of a cyber criminal law regime in Indonesia. This law was designed to answer the legal needs in dealing with new phenomena in the form of misuse of information technology. However, to date, the ITE Law has been one of the most criticized laws because it is considered to contain criminal provisions that are not in line with the principle of legality. Therefore, it is important to examine the extent to which the ITE Law can be considered to meet the provisions of *lex scripta*, *lex certa*, and *lex stricta* in practice.

First, from the *lex scripta* side, formally the ITE Law has fulfilled the element that criminal provisions must be derived from written law. The articles in the ITE Law that regulate cyber crimes are clearly stated in the state gazette and are legitimate legislative products. The criminal articles start from Article 27 to Article 37, followed by the criminal threat in Article 45 and so on. For example, Article 30 regulates illegal access to another person's electronic system without permission. Article 31 regulates wiretapping, and Article 32 concerns the manipulation of electronic data. In this case, formally, the fulfillment of the *lex scripta* element is not a problem because criminal norms have been determined in the form of legitimate laws. This shows that Indonesia continues to uphold the formal legal principle in its criminal law system. (Huda and Ruslie 2023)

However, the fulfillment of the principle of legality does not stop at the existence of written norms. Much more important is how the contents of the norms are formulated. This is where the second element, namely *lex certa*, comes under sharp scrutiny. *Lex certa* demands that criminal norms must be formulated with clear sentences, not open to multiple interpretations, and provide objective limitations on an act that is qualified as a crime. In practice, many articles in the ITE Law have actually caused debate because they are considered vague and susceptible to subjective interpretation.

One of the most controversial articles is Article 27 paragraph (3) of the ITE Law, which states:

"Any person who intentionally and without authority distributes and/or transmits and/or makes accessible electronic information and/or electronic documents that contain insults and/or defamation."

This article has been widely used in law enforcement practice, but has also been the source of much criticism. Normatively, this article uses the phrase "insults and/or defamation" without a detailed explanation of the parameters or benchmarks of the term. There is no explicit and measurable definition of insult, so this understanding is drawn from the Criminal Code (Articles 310 and 311), which is basically designed in the context of direct communication between

individuals, not in digital communication that is widespread and viral. (Iwan Rasiwan and SH 2025)

The lack of adequate explanation in the ITE Law causes the meaning of "insult" to depend on the subjectivity of law enforcers and the perception of victims. This is contrary to the principle of *lex certa*, which requires that a person can know for sure what actions are prohibited and how sanctions are imposed. In some cases, social media users who convey criticism of public officials can easily be charged with this article, even though theoretically criticism of state administrators is part of the rights of citizens protected by Article 28E of the 1945 Constitution.

The same conditions also apply in Article 28 paragraph (2) of the ITE Law, which states that:

"Any person who intentionally and without right disseminates information aimed at causing hatred or hostility towards individuals and/or certain community groups based on ethnicity, religion, race and inter-group (SARA)."

In substance, this article contains good intentions to protect vulnerable groups from hate speech. However, the wording of the article is ambiguous. What are the objective limits of "inciting hatred"? How do you measure the perpetrator's intention or *mens rea* in spreading the information? There are no objective criteria used to measure the element of hatred, so the phrases in this article are very susceptible to being misused to silence freedom of expression. The use of terms such as "information that incites hatred" without strict semantic limitations is contrary to the principle of *lex certa* which demands legal certainty and clarity.

The Constitutional Court in Decision Number 50/PUU-VI/2008 did state that the articles in the ITE Law are constitutional, but the Court also noted that the implementation of these articles must be carried out with the principle of caution and must not be used to criminalize legitimate expression. This means that the Court did not cancel the norm, but emphasized that law enforcers must not use the articles to limit the space for civil liberties. Unfortunately, this note is often not translated well in the field. (Mohamad 2019)

Furthermore, the element of *lex stricta* or the prohibition on interpreting criminal law analogously is also a problem in the application of the ITE Law. In criminal law, analogy is prohibited because it can cause someone to be punished for actions that are not actually formulated as crimes. In the practice of enforcing the ITE Law, many cases have been found where law enforcement officers have expanded the interpretation of certain articles to cover actions that are not explicitly regulated. For example, the use of Article 27 paragraph (1) concerning immoral content to ensnare perpetrators of distributing meme images that are considered "indecent", even though the images are satirical or even just parodies that do not explicitly violate moral norms.

This shows that law enforcement against cyber crimes in Indonesia often contradicts the principle of *lex stricta*. Law enforcement officers sometimes use broad, even analogical, interpretations in applying criminal provisions. This is a serious deviation from the principle of legality which should require strict and limited interpretation of a criminal law norm. Broad and uncontrolled interpretation of criminal law will open up space for abuse of authority and create legal uncertainty for digital citizens.

Furthermore, violations of the principle of legality in the ITE Law also have an impact on unequal legal treatment. Data collected from SAFEnet shows that most of the victims of the use of rubber articles in the ITE Law are civil society, activists, journalists, and ordinary social media users. Meanwhile, public reports of the spread of hate speech or hoaxes carried out by buzzers or certain groups are often not followed up seriously by law enforcement officers. This shows that violations of the principles of *lex certa* and *lex stricta* not only have an impact on legal uncertainty, but also lead to ongoing substantive injustice.

From all the descriptions above, it can be concluded that although formally the ITE Law has fulfilled the elements of *lex scripta* as a written law, it still has many problems in terms of

lex certa and lex stricta. The normative wording of the criminal articles in the ITE Law tends to be vague, open to multiple interpretations, and prone to misuse. In the context of a democratic state of law, this kind of criminal provision is unacceptable because it contradicts the basic principle that criminal law is the ultimum remedium which must be formulated strictly and limit-edly.

Therefore, it is appropriate that the ITE Law undergoes revision again, especially for arti-cles that contain unclear criminal elements. The approach that must be used is the rule of law approach that is oriented towards protecting human rights and legal certainty. Without it, cy-bercriminal law in Indonesia will not only fail to protect society from digital crimes, but will also become an instrument of repression that actually tarnishes the values of democracy and justice.

The Principle of Legality in the Regulation of Cyber Crimes According to the Indonesian ITE Law with the Provisions in the Budapest Convention and its Legal Implementation

The principle of legality in criminal law is a universal principle that is a main pillar in a modern rule of law, not only in Indonesia, but also in international standards. In the context of cybercrime, the challenges to the application of the principle of legality are increasingly complex because the nature of this crime is cross-border, rapidly changing, and involves high technology that is often not fully understood by conventional legal systems. In this section, the discussion will focus on a comparative analysis between the regulation of the principle of legality in cyber crimes according to the Indonesian ITE Law and the provisions in the Budapest Convention on Cybercrime 2001, as well as how the principle is implemented in practice in several countries that have ratified the convention.(Sitompul 2015)

The Budapest Convention adopted by the Council of Europe in 2001 is the first international instrument to comprehensively regulate cybercrime and the legal procedures for dealing with it. This convention not only regulates the types of crimes that must be criminalized by member states, but also emphasizes the importance of the principle of legality as a basic principle in the formation and application of cybercriminal law. Articles 2 to 10 of this convention contain a list of crimes that are recommended to be criminalized nationally, such as illegal access, illegal interception, interference with data and systems, misuse of devices, and content-based crimes such as child pornography and digital copyright infringement.

One of the main advantages of the Budapest Convention is its formulation which tends to strictly fulfill the principles of lex certa and lex stricta. Each provision regarding the criminal act is formulated in detail, with a fairly clear description of the elements of the act and the perpetrator's intention. For example, Article 2 on "Illegal Access" is formulated as follows:

"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offenses under its domestic law... the intentional access, without right, to the whole or any part of a computer system."

The wording of this norm emphasizes the elements of "intentionality", the element of "unlawful", and the specific object, namely the computer system. This approach is consistent with the principle of nullum crimen sine lege certa, because it ensures that the public can clearly know which actions are classified as criminal acts, and how their boundaries are determined legally.(March 2019)

On the other hand, in the Indonesian ITE Law, the articles regulating cyber crimes, although formally fulfilling the elements of lex scripta, often do not describe the elements of the crime in detail as in the Budapest Convention. Take for example Article 30 paragraph (1) of the ITE Law, which states:

"Any person who intentionally and without authority or unlawfully accesses another person's computer and/or electronic system in any way."

In comparison, the structure of this article is not much different from Article 2 of the Budapest Convention. However, the fundamental difference lies in the absence of further elaboration or interpretative guidelines that provide meaning to the phrases “unlawful”, “without rights”, or “access by any means.” In a legal system that upholds the principle of legality, general phrases such as these need to be explained systematically, either through an explanation of the law, Supreme Court guidelines, or permanent jurisprudence, so that they are not used arbitrarily by law enforcers.

In addition, the Budapest Convention emphasizes the importance of proportionality and protection of human rights in any attempt to criminalize cybercrime. Article 15 of the Budapest Convention explicitly states that member states must ensure that legal measures taken to combat cybercrime must be carried out with due regard to human rights, including the protection of freedom of expression and privacy as set out in the European Convention on Human Rights. This approach provides a balance between the need to crack down on digital crime and the state's obligation to safeguard the fundamental rights of citizens.

Indonesia, to date, has not become a party to the Budapest Convention. The main reasons are the rule of law and differences in approaches in national legal systems. However, several principles contained in this convention have in fact become general principles of law that are internationally recognized, and therefore remain relevant to be used as benchmarks in evaluating national cybercriminal law. Furthermore, harmonization with international standards is important considering the transnational character of cybercrime, where international cooperation is a must in terms of investigation, extradition, and exchange of information.(Sangkilang 2023)

Countries such as Germany and Japan, which have ratified the Budapest Convention, demonstrate how the principle of legality is strictly implemented in their cybercriminal law. In Germany, for example, cybercrimes are codified in their Criminal Code (StGB) with very specific wording, and each provision is usually accompanied by in-depth legal commentary (jurisprudence and doctrine) as a guide to interpretation. In Japan, although its approach is based on a general penal code which was later supplemented by the Act on Prohibition of Unauthorized Computer Access (1999), this country maintains that each criminal article has clear elements and is not used to ensnare gray areas or legitimate expressions in the digital public space.

On the other hand, in Indonesia, many provisions in the ITE Law actually open up grey areas. For example, in Article 27 paragraph (3) and Article 28 paragraph (2) of the ITE Law, criminal provisions not only do not fulfill the elements of *lex certa*, but have also been used to ensnare political expression, public criticism, and even journalistic reports. This is contrary to the principle of *lex stricta*, which prohibits the expansion of interpretation or the use of analogies in criminal law. In the context of the Budapest Convention, cyber crimes must be limited only to actions that actually cause harm or danger to the integrity of a digital system or violation of digital rights, not to opinions or discourses that develop in society.

Even more ironic, many democratic countries have removed the provisions on insult or defamation from their criminal laws, precisely to maintain the balance between freedom of expression and personal honor. Indonesia, on the other hand, still uses the article as a legal “weapon” in the ITE Law. This shows that Indonesia is still trapped in a repressive criminal law paradigm, rather than preventive and educative as emphasized in international legal standards.

In terms of implementation, the Budapest Convention also regulates procedural law, such as the collection of digital evidence, seizure of electronic systems, interception of data traffic, and cooperation between countries. Although the ITE Law has been followed by technical regulations such as PP No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PSTE), Indonesia does not yet have a comparable procedural framework to deal with cross-border cybercrime investigations. As a result, in many cases, law enforcement

officers have difficulty prosecuting perpetrators who use foreign servers, anonymous accounts, or hidden technological infrastructure. (Ersya 2017)

In relation to the principle of legality, non-standardized legal procedures also have the potential to violate the principle of due process of law, especially when the process of arrest, confiscation of devices, or blocking of content is carried out without adequate supervision by judicial institutions. This is where it is important to make the practices of the Budapest Convention an inspiration for Indonesia, not only in terms of the substance of criminal norms, but also in the framework of digital criminal procedure based on human rights.

Taking into account all of the above aspects, it can be concluded that although the Indonesian ITE Law has regulated a number of cyber crimes in written law (*lex scripta*), it still does not fully meet the standards of the principle of legality as outlined in the Budapest Convention, especially in terms of *lex certa* and *lex stricta*. Multi-interpretive normative wording, excessive criminal practices, and the absence of strict interpretative guidelines make Indonesian cybercriminal law vulnerable to misuse and far from the principle of substantive justice.

Therefore, the most relevant recommendation is that Indonesia, even though it has not ratified the Budapest Convention, continue to harmonize its laws with international standards through:

1. Re-arranging articles in the ITE Law that are open to multiple interpretations to fulfill the elements of *lex certa* and *lex stricta*.
2. Preparation of binding judicial guidelines or interpretations as a reference in the application of cyber criminal law.
3. Enhancing international cooperation in combating cybercrime through bilateral and regional platforms.
4. Prioritize a human rights-based criminal law approach as the main foundation of national digital regulation.

With these steps, the principle of legality as a basic principle in a state of law can truly be upheld in the cyber realm, making the law not a tool of repression, but a guarantee of protection for the dignity and rights of citizens in the digital era.

CONCLUSION

Based on the results of the analysis, it can be concluded that although the Indonesian ITE Law has formally fulfilled the elements of *lex scripta* because it is formulated in the form of statutory regulations, there are still serious weaknesses in fulfilling the principle of legality substantially, especially in terms of *lex certa* and *lex stricta*. Many articles in the ITE Law are vague, open to multiple interpretations, and susceptible to misuse, so they do not provide adequate legal certainty for citizens. Compared to the Budapest Convention and practices in its member countries, the ITE Law tends to be repressive and not proportional in balancing the interests of combating digital crime and protecting human rights. Therefore, reform of the ITE Law by referring to the principles of legality and international standards is very urgent to realize a fair, certain, and democratic cybercriminal law system.

BIBLIOGRAPHY

- Dhadha, Tegar Pan, Laras Atika Rahayu, Dewi Sito Resmi, and Dora Kusumastuti. 2021. "The Effectiveness of the Role of the ITE Law in Protecting and Maintaining All Cyber Activities in Indonesia." *Legal Standing: Journal of Legal Studies* 6 (1): 40–48.
- Drajat, Harwita Sari. 2019. "The Role of the International Court of Justice in Settling

- International Disputes.” *Journal of Legal Research in Legal Science* Volume 13 (1).
- Ersya, Muhammad Prima. 2017. “Legal Issues in Tackling Cyber Crime in Indonesia.” *Journal of Moral and Civic Education* 1 (1): 50–62.
- Huda, Ulil Abshor Nurul, and Ahmad Sholikhin Ruslie. 2023. “Reverse Proof in Corruption Crimes in Indonesia in the Framework of Guaranteeing the Principle of Legal Certainty.” *Journal Evidence Of Law* 2 (2): 63–72.
- Indra Utama Tanjung. 2024. *BASICS OF LEGAL RESEARCH METHODS*. Karanganyar: CV Pustaka Dikara).
https://scholar.google.com/citations?view_op=view_citation&hl=id&user=rToGqjUAAAAJ&cstart=20&pagesize=80&citation_for_view=rToGqjUAAAAJ:Wp0glr-vW9MC.
- Iskandar, Anang. 2019. “Drug Abuse, Imprisoned or Rehabilitated.” *Criminal Law and Legal Development* 2 (1).
- Iwan Rasiwan, H, and MH SH. 2025. *The Principle of Balance of the New Criminal Code Reflects Pancasila Values in Law Enforcement*. Takaza Innovatix Labs.
- Marentek, Junio Imanuel. 2019. “Criminal Responsibility of Perpetrators of Premeditated Murder Reviewed from Article 340 of the Criminal Code.” *Lex Crimen* 8 (11).
- Mohamad, Irwansyah Reza. 2019. “Legal Protection of the Right to Obtain Health Services Reviewed from the Aspect of Human Rights.” *Akademika* 8 (2): 78–94.
- Rianto, Rianto, T Riza Zarzani, and Yasmirah Mandasari Saragih. 2024. “Legal Responsibility of Online Media Corporations and Social Media Users for Broadcasting News Shared to the Public Containing ITE Criminal Acts.” *JHIP-Journal of Scientific Education* 7 (1): 393–98.
- Sangkilang, Gabriella M. 2023. “LEGAL REVIEW OF MANAGEMENT OF CONFISCATED GOODS AND ASSET RECOVERY OF THE CRIMINAL ACT OF CORRUPTION 'PEMECAH OMBAK' IN LIKUPANG DUA SULUT (CASE STUDY OF DECISION NUMBER 15/PID. SUS-TPK/2021/PN. MND).” *LEX CRIMEN* 12 (2).
- Setiawan, M Nanda. 2021. “Criticizing the ITE Law Article 27 Paragraph (3) Viewed from the Socio-Politics of Indonesian Criminal Law.” *DATIN Law Journal* 2 (1): 1–21.
- Sidik, Suyanto. 2013. “The Impact of the Electronic Information and Transactions Law (UU ITE) on Legal and Social Changes in Society.” *Jurnal Ilmiah Widya* 1 (1): 1–7.
- Sitepu, Rida Ista, and Yusona Piadi. 2019. “Implementation of Restorative Justice in the Punishment of Corruption Offenders.” *Jurnal Rechten: Penelitian Hukum dan Hak Asasi Manusia* 1 (1): 67–75.
- Sitompul, Anastasia Hana. 2015. “Legal Study on Sexual Violence Against Children in Indonesia.” *Lex Crimen* 4 (1).