ALGEBRA : JURNAL PENDIDIKAN, SOSIAL DAN SAINS

ISSN : 2807-663X e-ISSN : 2807-629X
Journal Homepage : https://algebra.yana.or.id/index.php/ejournal/index
Volume 5 Number 4 (2025)

EFFECTIVENESS OF LAW ENFORCEMENT AGAINST CYBER CRIME IN THE JURISDICTION OF BALI REGIONAL POLICE

Anak Agung Gede Mahendra[1*], I Made Wirya Dharma[2], Ni Putu Sawitri Nandari[3], Dewa Ayu Putri Sukadana[4]
[1234]Fakultas Hukum, Universitas Pendidikan Nasional, Denpasar, Indonesia
*Correspondence email: agungmahendraa@icloud.com

ABSTRACT

Law enforcement against cybercrime within the jurisdiction of the Bali Regional Police is specifically carried out by the Bali Regional Police Cyber Investigation Directorate. From 2023 to 2025, cybercrime cases increased at varying rates each year. In 2023, there were 54 cases, 47 in 2024, and 35 in 2025. The purpose of this research is to examine and analyze the effectiveness of cybercrime law enforcement within the jurisdiction of the Bali Regional Police and the obstacles faced by the Bali Regional Police in investigating and prosecuting cybercrime cases. This research uses an empirical method, utilizing a statutory regulatory approach, legal concept analysis, and factual analysis. The results of the study indicate that cybercrime law enforcement within the jurisdiction of the Bali Regional Police has not achieved the desired level of effectiveness. This despite various efforts, both preventive and repressive. Meanwhile, obstacles faced by the Bali Regional Police in investigating and prosecuting cybercrime cases include: legal substance factors due to jurisdictional limitations; legal structure factors including minimal human resources within the police investigators and limited investigative budgets; and legal culture factors due to a lack of legal awareness and low public participation

Keywords : Effectiveness; Law Enforcement; Cybercrime.

INTRODUCTION

One of the phenomena of the Industrial Revolution 4.0 that is currently demonstrating a significant influence is the internet. At the very least, the journey of space and time via the internet has forced science and technology to move at an unstoppable pace. Businesses, governments, officials, and individuals around the world use the internet as a means of managing their businesses, policies, and daily lives. However, the rapid development of the internet as an information medium can sometimes be a double-edged sword. While it contributes to human welfare, progress, and civilization, it can also be an effective means of committing crimes (Appludnopsanji, 2021).

The crime referred to in this study is cybercrime, or more commonly known as cybercrime. Cybercrime is a type of crime that has developed in the modern era as a negative impact of the development of information technology. The primary mode of this crime involves using computers or other communication devices connected to a computer network (Hadi, 2022).

The term cybercrime originated in a background paper for the 10th UN Congress workshop in 2000 in Vienna, Austria, as quoted by Barda Nawawi Arief, which divided it into two categories. First, cybercrime, in a narrow sense, is called computer crime, and second, cybercrime, in a broader sense, is called computer-related crime. In its context, cybercrime is defined as criminal activity committed using computers, computer networks, or the internet (Arsawati, I Nyoman Juwita, Darma, I Made Wirya and Antari, 2021).

Husamuddin et al. explain that cybercrime refers to a category of crimes committed using information and communication technology. These crimes take the form of crimes related to cyberspace or the digital world, exploiting vulnerabilities in computer systems and networks. According to them, this definition involves a series of actions that can harm individuals, companies, or governments, and encompasses various types of crimes committed via the internet or digital technology devices (Butarbutar, 2023).

Furthermore, another definition defines cybercrime as a term referring to criminal activity using computer networks as a tool, target, or venue for the crime. Cybercrime includes online auction fraud, check forgery, credit card fraud, confidence fraud, identity fraud, child pornography, etc. Cybercrime is also very difficult to identify because the criminal landscape is vast and constantly adopts new motives. Each perpetrator of this crime targets victims or exploits vulnerabilities in digital systems (Tabrani, 2025). This crime is also often a means of furthering real-world crimes, such as drug trafficking and prostitution (human trafficking). Considering the transnational nature of cybercrime, several obstacles are encountered in law enforcement. Furthermore, the spread of this cybercrime has tended to increase significantly in recent years along with the development of information technology and the internet (Fahmi, 2022).

Law enforcement itself is defined as an effort aimed at maintaining and improving order and ensuring legal certainty in society. Broadly speaking, law enforcement is defined as a form of implementing values derived from analyzing rules and attitudes to maintain order within the community. Therefore, law enforcement is not merely the implementation of laws and regulations, but rather the process of harmonizing values and actual behavioral patterns aimed at achieving peace (Huda, 2022).

The laws and regulations governing cybercrime in Indonesia are set out in the Republic of Indonesia Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE) as regulated in articles 27 to 37 (Orlando, 2022). The construction of these articles regulates in more detail the development of traditional crime modes as stated in the Criminal Code (KUHP). Basically, the presence of the policy of the Republic of Indonesia Law Number 9 of 2016 amendments to the Republic of Indonesia Law Number 11 of 2008 concerning Electronic Information and Transactions (abbreviated as the ITE Law) cannot be separated from the development of the use of technology (Undang-undang Republik Indonesia Nomor 19 Tahun 2016, 2016).

This debate will examine Indonesian cybercrime by researching at the Bali Regional Police. Cybercriminals target Bali Province, under the Bali Regional Police (POLDA), a popular tourist destination. These perpetrators are Indonesians and foreigners linked with foreign perpetrators (Indradewi, 2021). The Bali Regional Police's Cyber Investigation Directorate enforces cybercrime laws within its area. Bali Regional Police handled different numbers of cases from 2023 to 2025. There were 54 cases in 2023, 47 in 2024, and 35 in 2025. Bali Regional Police have reduced Indonesian crime by handling cybercrime crimes. Upon closer inspection, global and cybercrime-based offences provide substantial obstacles for authorities in promptly identifying and apprehending

culprits. This is because many Indonesian cybercriminals are linked to foreigners. Bali Regional Police arrested 12 members of a network that unlawfully registered SIM cards and sold one-time passwords (Fauzi, Ahmad, 2020).

Cybercrime law enforcement, especially its efficacy, is intriguing. Many cybercrime studies have focused on normative legal issues. Law enforcement officials, especially police, who enforce the law, rarely explain law enforcement (Wicaksono, 2025). Based on the description above, the researcher wants to study and discuss the Bali Regional Police's enforcement of cyber crime law to create a thesis with the research title. Effectiveness Of Law Enforcement Against Cyber Crime In The Jurisdiction Of Bali Regional Police

RESEARCH METHODS

Research is the process of collecting and analyzing data to discover legal facts within society. In this study, the researcher used an empirical legal research method. In empirical legal research, the subject of study is law conceptualized as actual behavior, an unwritten social phenomenon experienced by everyone in social relationships. Muhaimin, in his book, defines empirical legal research as a legal research method that functions to examine law in its concrete meaning and examine how it operates in society. Because this research examines people in social relationships, the empirical legal research method is considered sociological legal research. The research approach is a plan for how the research will be conducted. Meanwhile, Tabrani, in his research, explains the research approach as the entire method or activity in a study, starting from problem formulation to drawing conclusions (Galenso, Vidi, 2024).

Generally, research data consists of two types: primary data and secondary data. Primary data sources are data derived from field data obtained from respondents and informants. Primary data sources are data obtained from primary sources. These primary data sources can be obtained from respondents, informants, and sources. Meanwhile, secondary data sources were obtained through literature review and document study. Literature review can include books, journals, seminar proceedings, papers, legal encyclopedias, legal literature dictionaries, or other written legal materials (Jainah, Zainab Ompu, 2024).

The data collection techniques used in this study include primary and secondary data. There are three primary data collection techniques in empirical legal research that can be used individually, separately, or combined (Muhaimin, 2020). Data analysis is a crucial step in obtaining research results. This is because data will lead to scientific findings when analyzed using appropriate techniques. To process the data obtained from literature or document study, this study utilized qualitative analysis. Qualitative analysis is a research method that produces descriptive data, namely what is stated in writing and actual behavior. The research location is where the researcher obtains the necessary data. The location selection is based on considerations and suitability for the chosen topic. The research location is the Bali Regional Police, specifically the Cyber Crime Directorate, which is located at Jalan Kamboja No. 1, Denpasar, Bali.

RESULTS AND DISCUSSION

Interviews were conducted with informants whom the researcher deemed to have a thorough understanding of and mastery of the research topic, specifically regarding cybercrime law enforcement within the Bali Regional Police jurisdiction. The researcher adhered to a pre-prepared interview guide during the interviews. The interviews took place in the informant's office. The informant in this research interview was First Inspector Robinson Bhayangkara, Head of Unit III, Sub-Directorate I, Ditressiber, Bali Regional Police.

The analysis of the interview results and questions posed to the informant relates to the first problem formulation, namely the effectiveness of cybercrime law enforcement within the Bali Regional Police jurisdiction from the perspective of regulations, institutional structure, and human resources. The findings indicate that the Ditressiber is still considered ineffective due to numerous shortcomings and obstacles faced by the Bali Regional Police. Meanwhile, the researcher's analysis of the interview results regarding questions submitted to sources or informants related to the formulation of the second problem or obstacles faced by the Bali Regional Police in conducting investigations and prosecutions of cybercrime cases includes legal substance factors caused by jurisdictional limitations, based on legal structure factors including the lack of human resources within the police

investigators and limited investigation budgets, while legal culture factors are caused by a lack of legal awareness and low public participation.

Researchers conducted research observations at the Bali Regional Police (Polda Bali), specifically the Cyber Investigation Directorate (abbreviated as Ditressiber), which is specifically tasked with conducting cybercrime investigations and inquiries within the Bali Police jurisdiction. Based on the researchers' observations, it is clear that cybercrime law enforcement within the Bali Police jurisdiction is carried out in accordance with the mechanisms stipulated in laws and regulations through several stages. These mechanisms are as follows:

a. Receiving public complaints
b. Conducting investigation administration
c. Examination of witnesses
d. Conducting case reviews to determine the elements of the crime based on the investigation results, witness statements, expert witness statements, and evidence
e. Escalating the handling to the investigation stage if a crime is found
f. Conducting investigation administration
g. Issuing a notification of the commencement of investigation (SPDP) and summoning witnesses
h. Conducting case reviews and suspect determination
i. Sending summonses and suspect determination
j. Examining suspects
k. Filing files
l. Submitting files to the Public Prosecutor

Researchers also observed cybercrime data handled by the Bali Regional Police Cyber Crime Directorate over the past three years, from 2023 to 2025, with varying numbers of cases each year. In 2023, there were 54 cases, 47 cases in 2024, and 35 cases in 2025. Based on the number of cases described, the researchers will present the data in a table with the following details:

Table 1. Data on cybercrime cases within the jurisdiction of the Bali Regional Police from 2023 to 2025

NO	CASE	YEAR			AMOUNT
		2023	2024	2025	
1	Online gambling	10	8	8	26
2	Illegal access	10	19	9	38
3	Fraud	12	6	4	22
4	Pornography	4	1	6	11
5	Skimming	-	-	-	-
6	Defamation	1	2	1	4
7	Threats/Extortion	2	3	5	10
8	Hate speech	2	7	-	9
9	Hoaxes	6	-	-	6
10	Personal data protection	7	1	2	9

Source: Bali Regional Police Cyber Investigation Directorate

Based on the data on cybercrime cases handled by the Bali Regional Police (POLDA) above, various types of cybercrime are identified, including online gambling, illegal access, fraud, pornography, defamation, skimming, threats/extortion, hoaxes, personal data protection, and hate speech.

In addition, the Bali Regional Police's Cyber Crime Directorate (Ditresbriber) also monitors online activities through cyber patrols to prevent cybercrime, as presented in the following graphic:

Figure 1. Cyber Patrol Activities at the Bali Regional Police Cyber Crime Directorate
Source: Bali Regional Police Cyber Crime Directorate

DISCUSSION

Effectiveness of Cybercrime Law Enforcement in the Bali Regional Police Jurisdiction

Crime types and dimensions necessitate mitigation activities, including law enforcement, both criminal and non-penal. Law enforcement seeks social justice and order. Law enforcement involves developing concepts to uphold or successfully function legal norms so they can guide traffic and legal relations in society and the state. Cybercrime is newer than street crime, as mentioned. In parallel with the IT revolution, cybercrime evolved. Cybercrime includes a wide spectrum of dangers, including huge and coordinated attacks on essential communication and information infrastructure globally, including Indonesia.

Barda Nawawi Arief stressed the need to improve criminal law enforcement's cybercrime response and reconstruction. Apply ubiquity to cybercrime. Cybercrime is rising along with internet use. The principle of ubiquity argues that crimes committed within a country's borders or outside them (extraterritorial) must be brought under its jurisdiction. A Norton survey published on its website found that during the past year, more than 978 million adults in 20 countries, including Indonesia with 59.45 million, have committed worldwide cybercrime. Norton also noted that these perpetrators cause enormous losses. Cybercrime cost Indonesian consumers $3.2 billion worldwide. From January 1 to December 22, 2022, the National Police Headquarters' National Police Information Centre (Pusiknas) and the Criminal Investigation Agency (Bareskrim Polri)'s Operational Investigation Unit (Robinopsnal) reported 8,831 cybercrime cases across all regional police units in Indonesia, with 8,372 individuals reported. These cases include 3,723 authentic data manipulation, 2,131 electronic fraud, 1,098 cybercrime, 358 unauthorized system access, 164 online gambling, 145 electronic threats/persecution, 143 electronic pornography and prostitution, 59 insults, and 43 hate speech (Kirana, 2023).

Cybercrime requires laws outside the Criminal Code. Special regulations are needed due to the quickly changing technology that permits it. Rene David calls Indonesia a "hybrid legal system." Continental law appears to be more influential on public law, notably criminal law, practice and legal science. Thus, a Criminal Code amendment or overhaul should institute an integrated cybercrime regulation approach. Soerjono Soekanto says the law, law enforcement, facilities and infrastructure, society, and culture all affect cybercrime law enforcement. In this study, the researcher connects Soerjono Soekanto's opinion with informant interviews with Mr. Ipda Robinson Bhayangkara, PS. Panit I Unit III Sub-Directorate I Ditressiber Polda Bali, about Bali Regional Police cybercrime enforcement, as stated in the first problem formulation.

Regulations

The law relates to statutes. Better statutes mean better law enforcement. If restrictions are ineffective, enforcement will be harder. Police investigators in Bali Regional Police's cybercrime enforcement jurisdiction follow laws and regulations, including the Indonesian National Police Law, the Criminal Procedure Code, and the Amendments to Law No. 11 of 2008 on E. Law enforcement remains based on statutory provisions, but the ITE Law, a criminal policy regime for cybercriminals, is currently considered ineffective or inadequate to achieve legal certainty in the community.

Law Enforcement Institutional Structure

Police are role models and should have community-aligned skills. This aspect refers to criminal justice system law enforcers, such as police investigators. According to interviews with Ipda Robinson Bhayangkara, Head of Unit I, Unit III, Sub-Directorate I, Ditressiber, Bali Regional Police, cybercrime is enforced penally and non-penally. Penal activities stress rigorous criminal law enforcement to combat crime.

According to interviews with Ipda Robinson Bhayangkara, if penal efforts are implemented in accordance with the Criminal Code and ensnare each perpetrator based on the applicable laws, as explained in Republic of Indonesia Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions. This refers to prevention-focused non-penal measures. These non-penal activities will automatically aid criminal justice. To prevent cybercrime, the Bali Police Cyber Crime Directorate implements non-penal measures such as socialization to educate the community on effective communication tools and Law Number 19 of 2016 on Information Security. This starts with families and extends via Bali's forum talks with all levels of society.

Human resource factors

According to interviews with Ipda Robinson Bhayangkara, Head of Unit III, Sub-Directorate I, Bali Regional Police Cyber Crime Directorate, investigators evaluate cybercrime law enforcement from a human resources viewpoint. Despite limited IT-skilled investigators, the Cyber Crime Directorate effectively monitors internet activity that leads to crimes. Overall, National Police detectives lack computer operational abilities, hacking knowledge, and cybercrime investigation skills. The cyber police force has few members compared to the number of cybercrime cases registered in police records. The limited number of specialists in investigating cybercrime cases hinders the police's ability to eliminate them quickly, allowing perpetrators to act more freely (Utarie, 2020).

Obstacles faced by the Bali Regional Police in investigating and prosecuting cybercrime cases

Cybercrime is not new in Indonesia, but law enforcement has failed to handle it, especially during police investigations. Cybercrime prosecution via criminal means is difficult. Because these cybercrimes involve numerous countries and different methods, perpetrators commit crimes in Indonesia and elsewhere. Extradition and mutual legal help are needed by law enforcement. This crime uses virtual accounts and perpetrators from many nations outside Indonesia's jurisdiction. Police have many challenges in prevention and enforcement. The police's law enforcement duties must match individuals' and institutions' traits. Understand that the police are a state government agency that maintains public order (Kamtibmas), law enforcement, protection, and community service. Law enforcement and investigators, who are protected by the law, may not always meet their goals. The preventative and law enforcement challenges they encounter are elements of crime prevention (Malaka, 2025).

Indonesia has many regulatory tools to catch cybercriminals, however they are not fully implemented. Law enforcement faces challenges in investigating and prosecuting cybercrime. To enforce criminal legislation, including cybercrime, one can evaluate each legal system component that directly affects law enforcement. An arrangement or unity of interdependent pieces is a system. Synchronization (integration) is essential. Lack of synchronization (integration) contributes to legal ineffectiveness and law enforcement failure. Lawrence M. Friedman says law is a system of components. Friedman believes the judicial system has structure, substance, and culture. He believes law enforcement's success depends on legal framework, substance, and culture. Legal structure encompasses law enforcement, legal substance comprises legal tools, and legal culture is a society's living law. Friedman characterizes the legal structure as comprising the number and size of courts and their jurisdiction. Structure include legislative organization, police department protocols, and more. Structure serves as a cross-section of the legal system. an action-freezing still photo."

The number and size of courts, their jurisdiction (including the types of issues they can hear), and the procedures for court appeals make up a judicial system. Structure also includes how the legislative is formed, what the president can and cannot do, police processes, etc. The legal institutions that implement legal instruments make up structure (legal structure). Structure illustrates how the law is applied formally. This framework depicts how courts, legislatures, and legal systems work. The researcher connects Lawrence M. Friedman's theory with police investigators'

opinions on cybercrime enforcement challenges in Bali Regional Police jurisdiction, as shown by interviews with First Inspector Robinson Bhayangkara, Head of Unit I, Sub-Directorate I, Cyber-Crime Directorate, Bali Regional Police, in the aforementioned room.

Significant Legal Factors

The researcher found that the Criminal Procedure Code (KUHAP) (formal) and Law Number 1 of 2024, the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions, govern cybercrime, both material and formal. At the policy formulation level, the approved legislation nevertheless have deficiencies that affect implementation by implementing actors, such as poor cybercrime law enforcement. In an interview with researcher and IPDA Robinson Bhayangkara, PS. Head of Unit III, Sub-Directorate I, Directorate of Cyber Crimes, Bali Regional Police, investigators faced challenges in apprehending cybercriminals due to jurisdictional limitations in Article 2 of the ITE Law, which is closely related to policing. Article 2 is territorial and protective. Only Indonesian criminals are subject to the territorial concept. Police investigators find it difficult to arrest and prosecute criminals outside Indonesian jurisdiction. Due to a lack of extradition accords, not all nations can extradite cybercriminals to Indonesia for trial. Article 2 of the ITE Law applies the protection principle to offences that undermine Indonesian vital interests. The researcher connects Lawrence M. Friedman's theory with police investigators' opinions on the challenges of enforcing cybercrime law in Bali, as shown by an interview with First Inspector Robinson Bhayangkara, Head of Unit I, Sub-Directorate I, Ditressiber, Bali Regional Police, in the Ditressiber room. 1. Significant Legal Factors The researcher found that the Criminal Procedure Code (KUHAP) (formal) and Law Number 1 of 2024, the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions, govern cybercrime, both material and formal. At the policy formulation level, the approved regulations still have deficiencies that affect law enforcement against cybercrime criminals. This is from the researcher's interview with First Inspector Robinson Bhayangkara, Head of Unit I, Sub-Directorate I, Ditressiber, Bali Regional Police. According to the head of Unit III Sub-Directorate I of the Bali Regional Police Cyber Directorate, arresting cybercriminals is challenging due to jurisdictional limitations in Article 2 of the ITE Law, which impacts police law enforcement efforts. Article 2 follows the territorial and protection principles. In this context, the territorial principle only applies to perpetrators who commit crimes in Indonesia, but it is difficult for police investigators to arrest and prosecute perpetrators outside Indonesia. This is because not all nations have extradition arrangements with Indonesia to extradite cybercriminals to Indonesia. Article 2 of the ITE Law applies the protection principle to offences that undermine Indonesian vital interests.

Legal Structural Factors

This factor refers to the institutions that enforce laws, particularly in the area of cybercrime law enforcement. Based on interviews conducted by researchers with IPDA Robinson Bhayangkara, Head of Unit I, Unit III, Sub-Directorate I, Directorate of Cybercrime, Bali Regional Police, police investigators encountered obstacles in handling cybercrimes, which can be seen in human resources and institutional support systems related to fulfilling investigation budgets. From a human resources perspective, these obstacles are closely related to the high volume of investigations. The large number of cases handled by the Bali Regional Police Cyber Investigation Directorate, coupled with a limited number of human resources (investigators), can lead to suboptimal cybercrime law enforcement. This is because investigators must prioritize cases, whether they are public demands (related to cybercrime issues circulating in the community or public complaints). Furthermore, many police investigators still lack computer operational skills, particularly understanding of computer hacking. Meanwhile, seen from the budget aspect, the amount of budget for carrying out investigative activities (pre-prosecution) is quite limited, because it does not match the budget requirements provided for each case in each investigation process, both for easy and very difficult cases, so it is felt to be very insufficient and will have implications for the investigation process which is less than optimal.

Legal culture factors

Cultural barriers to cybercrime law enforcement include limited legal understanding and public participation. According to discussions with researchers, inadequate legal awareness and public participation hinder police enforcement, particularly in cybercrime cases within Bali Regional Police jurisdiction. First, the public is not properly educated about the wise use of electronic media, resulting in frequent disturbances on internet-based social media services that might lead to crimes.

Second, many people still don't disclose cybercrime to law enforcement, resulting in many victims before preventive steps are taken. The following summary suggests that legal substance, structure, and culture hinder cybercrime law enforcement. Friedman's legal system theory states that law enforcement's success or failure depends on three components of the legal system: substance, structure, and culture, which are organisms that interact. These three obstacles greatly impact cybercrime enforcement. According to this theory, these obstacles show an empirical reality that must be considered to achieve the law's goals, in this case law enforcement against cybercrime. The empirical relationship between law enforcement, legislation, and human behaviour in empirical life affects the application of law and the alignment between das sein and das sollen.

CONCLUSION

Based on the researcher's research on the effectiveness of cybercrime law enforcement within the Bali Regional Police jurisdiction, it can be concluded that: The effectiveness of cybercrime law enforcement within the Bali Regional Police jurisdiction, from the perspective of regulatory aspects, institutional structure, and human resources, has not yet achieved the desired level of effectiveness. Despite various efforts, both preventive and repressive, the Bali Regional Police Cyber Crime Directorate still faces numerous shortcomings and obstacles, significantly impacting the success of law enforcement. Obstacles encountered in the investigation and prosecution of cybercrime cases include: legal substance factors due to jurisdictional limitations; legal structure factors include limited human resources within the police force and limited investigative budgets; and legal culture factors are due to a lack of legal awareness and low public participation. Based on the researcher's research on the effectiveness of cybercrime law enforcement within the Bali Regional Police jurisdiction, it can be concluded that The effectiveness of cybercrime law enforcement within the Bali Regional Police jurisdiction, from the perspective of regulatory aspects, institutional structure, and human resources, has not yet achieved the desired level of effectiveness. Despite various efforts, both preventive and repressive, the Bali Regional Police Cyber Crime Directorate still faces numerous shortcomings and obstacles, significantly impacting the success of law enforcement. Obstacles encountered in the investigation and prosecution of cybercrime cases include: legal substance factors due to jurisdictional limitations; legal structure factors include limited human resources within the police force and limited investigative budgets; and legal culture factors are due to a lack of legal awareness and low public participation.

REFERENCE

Appludnopsanji, E. a. (2021). Reformasi Sistem Peradilan Pidana Indonesia Berwawasan Pancasila. *KERTHA WICAKSANA*, *15*(1).

Arsawati, I Nyoman Juwita, Darma, I Made Wirya and Antari, P. E. D. (2021). A Criminological Outlook of Cyber Crimes in Sexual Violence Against Children in Indonesian Laws. *International Journal of Criminology and Sociology*, *2*(2).

Butarbutar, R. (2023). Kejahatan Siber Terhadap Individu : Jenis, Analisis, dan Perkembangannya. *Technology and Economics Law Journa*, *2*(2).

Fahmi, K. (2022). Efektivitas Pemberlakuan Sistem Satu Arah di Jalan Pesut Kota Samarinda Perspektif Maslahah Mursalah. *Qonun: Jurnal Hukum Islam Dan Perundang-Undangann*, *7*(2).

Fauzi, Ahmad. (2020). Tanggung Jawab Sosial dan Lingkungan Perusahaan Penanaman modal. *De Lega Lata Jurnal Ilmu Hukum*, *5*(2).

Galenso, Vidi, A. (2024). Pengaturan Keamanan Jaringan dan Kejahatan Siber dalam Hukum ITE. *Postulat Journal Of Law*, *2*(1).

Hadi, N. A. K. (2022). Penegakan Hukum Di Indonesia Dilihat Dari Perspektif Sosiologi Hukum. *Jurnal Hukum Dan Pembangunan Ekonomi*, *10*(2).

Huda, M. M. S. (2022). Implementasi Tanggung Jawab Negara Terhadap Pelanggaran Ham Berat Paniai Perspektif Teori Efektivitas Hukum Soerjono Soekanto. *Jurnal Agama Dan Hak Azasi Manusia*, *11*(1).

Indradewi, A. A. S. N. (2021). Efektifitas Penerapan Sanksi Administrasi Terhadap Warga Negara Asing Yang Melakukan Pelanggaran Visa Di Bali'. *Jurnal Komunikasi Hukum*, *7*(2).

Jainah, Zainab Ompu, S. (2024). Penerapan Sanksi Pidana Terhadap Pelaku Tindak Pidana Kejahatan Perjudian (Studi Putusan Nomor 315/Pid.B /2022/PN Gns). *MALEO LAW JOURNAL*, *8*(1).

Kirana, Y. (2023). Regulasi Yang Mengatur Secara Khusus Terkait Perlindungan Data Pribadi Di Indonesia Tentang Hoaks Dan Kerawanan Media Sosial (Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). *Jurnal Ilmiah Hukum Dan Keadilan*, *10*(1).

Malaka, Z. (2025). Tinjauan Sosiologi Hukum Tentang Penegakan Hukum di Indonesia. *TARUNA LAW: Journal of Law and Syariah*, *3*(1).

Muhaimin. (2020). *Metode Penelitian Hukum*. University Press.

Orlando, G. (2022). Efektivitas Hukum dan Fungsi Hukum di Indonesia' (2022) 6 (1) Tarbiyah Bil Qalam. *Jurnal Pendidikan Agama Dan Sains*, *6*(1).

Tabrani. (2025). Perbedaan Antara penelitian Kualitatif (Naturalistik) dan Penelitian Kuantitatif (Ilmiah) dalam barbagai Aspek'. *Jurnal Pendidikan Dan Konseling*, *5*(2).

Undang-undang Republik Indonesia Nomor 19 Tahun 2016. (2016). *Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Indonesia*. Negara Republik Indonesia Nomor 251 Tahun 2016.

Utarie, L. (2020). *Kewajiban Notaris Memberikan Penyuluhan Hukum Dalam Pembuatan Akta Otentik Di Kota Pekanbaru Berdasarkan Undang-Undang Nomor 2 Tahun 2014 Tentang Jabatan Notaris'*. Fakultas Hukum Universitas Lancang Kuning.

Wicaksono, I. (2025). Penerapan Asas Ultimum Remedium Dalam Penegakan Hukum Di Bidang Lingkungan Hidup. *Pagaruyuang Law Journal*, *5*(1).