International Journal of Law, Crime and Justice
Volume.2, Number.1 March 2025
e-ISSN: 3047-1362; p-ISSN: 3047-1370, Pages 282-295
DOI: https://doi.org/10.62951/ijlcj.v2i1.540
Available online at: https://international.appihi.or.id/index.php/IJLCJ

Obstacles and Challenge of Law Enforcement in the Face of Mayantara Crime in Indonesia

Maulana Arif Fadli[1], Muhammad Hatta[2], Isvani[3], Angga Dhipinto[4], Devia Anjelia[5], Rafita Sari[6]

[1-6] Magister Hukum, Fakultas Hukum, Universitas Malikussaleh, Indonesia
Jl. Unimal Bukit Indah Campus, Blang Pulo, Muara Satu District, Lhokseumawe City, Aceh, 24355
Maulana.247410101011@mhs.unimal.ac.id

Abstract. *The rapid development of information and communication technology (ICT) has increased the risk of cybercrime in Indonesia. Law enforcement against this crime faces various obstacles and challenges, both in terms of regulations, the capacity of law enforcement officials, and public awareness. This study aims to analyze the obstacles and challenges in law enforcement against violent crime in Indonesia and provide recommendations to improve its effectiveness. Through a qualitative approach with a case study method, this study uses primary data from interviews with law enforcement officials, academics, and cybersecurity practitioners, as well as secondary data from laws and regulations and related reports. The results of the study show that existing regulations, such as the Electronic Information and Transaction Law (ITE Law), still have weaknesses in accommodating the development of cybercrime. In addition, limited human and technological resources in law enforcement institutions, as well as low public awareness of cybersecurity, also hinder the effectiveness of law enforcement. To address these challenges, the study recommends more adaptive regulatory revisions, capacity building of law enforcement officials through more advanced training and technology, and public education campaigns to increase public awareness of cybersecurity. In addition, international cooperation needs to be strengthened to deal with transboundary crimes.*

Keywords : *Mayantara Crime, Law Enforcement, ITE Law, Cybersecurity, Cybercrime*

1. INTRODUCTION

The rapid development of information and communication technology (ICT) has had a significant impact on people's lives, including in Indonesia. These advances bring many benefits, such as easier access to information, improving business efficiency, and expanding communication networks. However, behind the benefits, this progress also poses new challenges, especially in the form of cybercrime. Crimes include various illegal activities such as hacking, online fraud, dissemination of illegal content, data theft, and cyberattacks that threaten national security. This phenomenon is even more worrying considering that Indonesia is one of the countries with the most internet users in the world, reaching more than 200 million people in 2023 (APJII, 2023).

In recent years, rapid technological advancements and widespread use of the internet have brought many benefits to society. However, along with these advancements, the threat of cybercrime has become increasingly prevalent, posing significant challenges for individuals, businesses, and governments around the world. Cybercriminals exploit vulnerabilities in digital

Received: February 14, 2025; Revised: February 28, 2025; Accepted: March 22, 2025; Published: March 25, 2025

systems, targeting sensitive data, financial resources, and even critical infrastructure (Mokokambang et al, 2023).

Crimes of terrorism threaten not only individuals, but also institutions, companies, and even national security. Cyberattacks on critical infrastructure, such as banking, energy, and government systems, can cause significant material and non-material losses. For example, in 2021, a ransomware attack on one of the hospitals in Indonesia resulted in the disruption of health services and the leakage of patient data (BSSN, 2021). In addition, the rise of online fraud and the spread of hoaxes through digital platforms also cause unrest in the community.

Law enforcement against violent crime in Indonesia faces various obstacles and complex challenges. First, from the regulatory aspect, even though Indonesia already has the Electronic Information and Transaction Law (ITE Law) Number 11 of 2008 which was amended into Law Number 19 of 2016, its implementation is still considered less effective. Several articles in the ITE Law are considered multi-interpreted and vulnerable to abuse, causing controversy in their enforcement (Prasetyo, 2021). Second, the capacity of law enforcement officials in handling criminal cases is still limited, both in terms of human resources, technology, and infrastructure. Crimes of terrorism require special expertise in the field of information technology, while many law enforcement officials do not have this competence. In addition, the lack of supporting tools and technologies, such as digital forensic software, also hampered the investigation process.

Third, crimes of interfaith are often transnational, requiring intensive international cooperation. Mayantara crimes often involve perpetrators from abroad, so they require international cooperation that is not yet fully effective (Suryani, 2020). However, coordination between countries in handling this crime is still not optimal, considering the differences in regulations and national interests of each country (Suryani, 2020). Fourth, public awareness of cybersecurity is also still low, so many victims are unaware that they have become targets of violent crimes (Kominfo, 2022). Many people do not understand the importance of protecting personal data and using technology wisely. This makes them vulnerable to falling victim to online fraud, phishing, or other cyberattacks.

Indonesia has long been recognized as a country based on legal principles. Law can be interpreted as a rule that can control human life in a country with legal principles like Indonesia. This is because the law regulates the order of human life within its scope, so that society becomes the main implementer needed to be able to implement and enforce the law as the foundation of the state. In enforcing the law in a country, according to Soerjono Soekanto (2004), it must be supported by one of the factors that can affect the success or not of law

enforcement in a country, namely the existence of law enforcement (Cristiana et al., 2019). If the country is based on legal principles, then the country needs law enforcement, in Indonesia itself the most basic law enforcement is the police, because the police are the entrance to law enforcement in Indonesia (Latukau, 2019).

The law serves to create order, justice, and legal certainty. In addition, law also plays a role as a tool to regulate social and economic relations in society (Mahfud, 2019). Law enforcement in Indonesia often faces challenges, inconsistencies in the application of the law, and low legal awareness of the public (Wahyudi, 2022). Judicial institutions, such as the Supreme Court and the Constitutional Court, play an important role in interpreting and enforcing the law in Indonesia. However, these institutions also often face criticism related to independence and transparency (Butt, 2020).

Based on the description above, this study aims to analyze the obstacles and challenges in law enforcement against capital crimes in Indonesia. By understanding these issues, it is hoped that effective solutions can be found to increase the effectiveness of law enforcement and protect the public from the threat of cybercrime.

2. LITERATURE REVIEW

Legal Framework for Crimes in Indonesia

Law in Indonesia can be interpreted as a set of rules, norms, and principles that govern human behavior in society, which are binding and enforced by a legitimate authority, such as the government or judicial institutions. Law in Indonesia functions to create order, justice, and legal certainty in the life of society, nation, and state. Law in Indonesia is sourced from various foundations, including Pancasila as the basis of the state, the 1945 Constitution (1945 Constitution) as the supreme constitution, and other applicable laws and regulations (Asshiddiqie, 2020).

In general, laws in Indonesia can be divided into two main categories, namely public law and private law. Public law regulates the relationship between the state and individuals or society, such as criminal law, constitutional law, and state administrative law. Meanwhile, private law regulates relationships between individuals or legal entities, such as civil law, commercial law, and family law. In addition, Indonesia also knows the customary law system that applies in various regions, which is the cultural heritage and traditions of the local community (Hadjon, 2021).

Law in Indonesia has unique characteristics because it is influenced by various legal systems, such as customary law, Islamic law, and Western (European) law. This makes

Indonesia a country with a pluralistic legal system. However, this legal pluralism also poses challenges, especially in terms of harmonization and consistent law enforcement throughout Indonesia.

Cybercrime is one of the major challenges in the digital era that requires a comprehensive and effective legal framework. In Indonesia, the legal framework for dealing with crimes has been built through various laws and regulations, with the Electronic Information and Transaction Law (UU ITE) Number 11 of 2008 which was amended to Law Number 19 of 2016 as the main foundation. In addition to the ITE Law, there are several derivative regulations and other legal instruments that support the handling of cybercrimes, such as the Criminal Code (KUHP), the Personal Data Protection Law (PDP Law), as well as regulations from related institutions such as the State Cyber and Cryptography Agency (BSSN).

1. **Electronic Information and Transaction Law (ITE Law)**

   The ITE Law is the main legal basis in regulating crimes in Indonesia. The law covers a wide range of aspects, including the prohibition of illegal access, wiretapping, the dissemination of illegal content, and fraud through electronic systems. Some of the key articles in the ITE Law are:

1) Article 27: Regulates the dissemination of content that violates morality, gambling, insults, or defamation.
2) Article 28: Regulates the spread of fake news (hoaxes) and hate speech.
3) Article 30: Regulates hacking and illegal access to electronic systems.
4) Article 32: Regulates the illegal wiretapping or interception of electronic information.

Although the ITE Law has become an important foundation, its implementation has often drawn criticism because some articles are considered multi-interpreted and vulnerable to abuse, especially articles on defamation and hate speech (Prasetyo, 2021).

2. **Criminal Code (KUHP)**

   The Criminal Code is also used as a legal instrument to deal with crimes of terrorism, especially for criminal acts that are not specifically regulated in the ITE Law. For example, online fraud can be charged with articles on fraud in the Criminal Code. However, the Criminal Code is considered less relevant in dealing with complex and technology-based crimes (Wibowo, 2022).

3. **Personal Data Protection Law (PDP Law)**

   In 2022, Indonesia passed the Personal Data Protection Law (PDP Law) as an effort to protect citizens' personal data from misuse, including in the context of capital crimes.

The PDP Law regulates the obligations of data controllers to protect personal data, sanctions for violators, and the rights of data owners. This law is expected to be an important instrument in preventing crimes involving theft or data leakage (Kominfo, 2022).

4. **The Role of the State Cyber and Cryptography Agency (BSSN)**

   BSSN is a government agency responsible for overseeing cybersecurity in Indonesia. BSSN has an important role in responding to cyberattacks, conducting investigations, and providing policy recommendations related to cybersecurity. This institution also collaborates with law enforcement officials to handle criminal cases (BSSN, 2021).

5. **Challenges in the Legal Framework**

   Although the legal framework for capital crimes in Indonesia already exists, several challenges still hinder its effectiveness, including:

   a. Not Comprehensive Regulations: Some forms of cybercrime, such as ransomware attacks and deepfakes, have not been specifically regulated in the ITE Law or other regulations.
   b. Capacity of Law Enforcement Officers: Law enforcement officers often lack the technical expertise to handle complex criminal cases.
   c. Inter-Agency Coordination: Coordination between law enforcement agencies, BSSN, and the private sector still needs to be improved to deal with violent crime effectively.

Mayantara Crime Law Enforcement Mechanism in Indonesia

Law enforcement against cybercrime in Indonesia involves a series of processes that include reporting, investigation, prosecution, and imposition of sanctions. This mechanism involves various parties, including law enforcement officials (such as the police and prosecutor's office), specialized institutions such as the State Cyber and Cryptography Agency (BSSN), as well as the active role of the community and the private sector. The following is a complete explanation of the law enforcement mechanism against crimes in Indonesia:

1. **Mayantara Crime Reporting**

   Reporting is the first step in the law enforcement process. Victims of violent crime can report the incident to the authorities, such as the Indonesian National Police (Polri) through a special unit that handles cybercrime, namely the Directorate of Cyber Crimes (Dittipidsiber). In addition, the public can also report crimes through online platforms

such as Kominfo Content Complaints or Report! provided by the Ministry of Communication and Information Technology (Kominfo, 2022).

2. **Investigation and Evidence Gathering**

   After receiving the report, law enforcement officials will conduct an investigation to collect digital evidence. This process involves digital forensic analysis, such as IP address tracking, system log checks, and data retrieval from electronic devices. Law enforcement officials work closely with BSSN and information technology experts to ensure that the evidence collected is valid and can be accounted for in court (Wibowo, 2022).

3. **Prosecution and Legal Process**

   Once the investigation is completed and the evidence is deemed sufficient, the case will be transferred to the Prosecutor's Office for further processing. The prosecution is carried out based on relevant articles in the Electronic Information and Transaction Law (ITE Law), the Criminal Code (KUHP), or other regulations. This legal process involves a court hearing, where the judge will decide whether the defendant is guilty and impose appropriate sanctions (Prasetyo, 2021).

4. **Imposition of Sanctions**

   Penalties for crimes vary depending on the type and severity of the crime. For example, violations of Article 27 of the ITE Law (dissemination of illegal content) can be punished by a maximum prison sentence of 6 years and/or a fine of up to IDR 1 billion. Meanwhile, violations of the Personal Data Protection Law (PDP Law) can be subject to criminal sanctions and heavier fines (Suryani, 2020).

5. **The Role of Special Institutions and Inter-Agency Collaboration**

   BSSN plays an important role in supporting the enforcement of international criminal laws, especially in terms of prevention, early detection, and response to cyberattacks. In addition, collaboration between the National Police, the Prosecutor's Office, Communication and Informatics, and the private sector (such as internet service providers and technology companies) is also needed to increase the effectiveness of law enforcement (BSSN, 2021).

Mayantara's Crime

Cybercrime is defined as any form of illegal activity carried out through or against computer systems and internet networks (Smith, 2020). Some of the main categories of mayland crime include:

1. Cyber Fraud

   Online fraud which includes phishing, social engineering, and financial fraud (Jones & Xu, 2021).
2. Cyber Terrorism

   Attacks carried out by individuals or groups with the aim of disrupting the political and economic stability of a country (Ali & Hassan, 2022).
3. Data Breach

   Theft or dissemination of sensitive information that can harm individuals or organizations (Nguyen et al., 2023).

The Impact of Mayantara Crime

The impact of cybercrime is vast, covering economic, social, and political aspects. According to recent research, economic losses due to cybercrime are estimated to reach billions of dollars every year (Kaspersky, 2023). In addition, this threat also increases public distrust of digital services (Brown & Taylor, 2020).

Various strategies have been developed to reduce the risk of cybercrime, including:

1. Regulations and Policies

   Strengthening cybersecurity regulations through international laws and policies (UNODC, 2021).
2. Security Technology

   The use of encryption, two-factor authentication, and advanced firewalls to protect data (Chen et al., 2022).
3. Education and Public Awareness

   Cyber awareness campaigns to increase public understanding of cyber threats (Martinez, 2024).

3. METHODS

Type of Research

This research is a qualitative research with a **case study** approach. The case study was chosen because it allows researchers to explore in depth the barriers and challenges of law enforcement against violent crime in Indonesia, focusing on specific contexts and dynamics.

Data Source

The data in this study was collected from two types of sources, namely:

1) Data Primer

It was obtained through in-depth interviews with relevant sources, such as law enforcement officials (Polri, Prosecutor's Office), legal experts, academics, and cybersecurity practitioners.

2) Data Seconds

It is obtained from official documents, such as BSSN's annual report, court decisions, laws and regulations, as well as articles and scientific journals related to crimes and law enforcement.

Data Collection Techniques

1) In-Depth Interviews

Interviews are conducted using interview guides that have been prepared in advance. The resource persons were selected purposively based on their expertise and experience in handling crimes of the dead.

2) Document Study

Analysis of official documents, such as the ITE Law, PDP Law, BSSN reports, and court decisions related to the crime of mayantara.

3) Observation

Observation of law enforcement processes, such as court hearings or investigative activities by law enforcement officials (if possible)

Data Analysis Techniques

The data that has been collected is analyzed using thematic analysis techniques. The steps are as follows:

1) Data Transcription

Interview data and documents are transcribed and organized systematically.

1) Coding

Data is grouped based on relevant themes or categories, such as regulatory barriers, apparatus capacity, and public awareness.

2) Theme Identification

Themes that emerged from the data were identified and associated with the focus of the research.

3) Data Interpretation

The themes that have been identified are interpreted to answer the research questions and provide recommendations.

Data Validity

To ensure the validity of the data, this study uses triangulation techniques, namely:

1) Triangulation Source

   This stage compares data from various sources, such as interviews with law enforcement officials, legal experts, and official documents.

2) Triangulation Method

   This stage uses more than one data collection method, such as interviews, document studies, and observations.

Research Ethics

This research adheres to the principles of research ethics, namely:

1) Informed Consent

   Resource persons were given an explanation of the purpose of the research and gave approval before being interviewed.

2) Concealment

   The identity of the source and sensitive information are kept confidential.

3) Non-Maleficence

   The research must not be detrimental to the source or related parties.

4. RESULTS

This qualitative research aims to identify obstacles and challenges in law enforcement against violent crime in Indonesia. Based on data obtained through in-depth interviews, document studies, and observations, this study found several key findings that can be grouped into four main themes : regulation, capacity of law enforcement officials, public awareness, and characteristics of violent crime.

1. Regulations That Are Not Comprehensive

Based on interviews with legal experts and law enforcement officials, it was found that existing regulations, such as the Electronic Information and Transaction Law (ITE Law), are considered not to be able to accommodate all forms of violent crime that continue to develop. Several articles in the ITE Law, such as Article 27 and Article 28, are considered multi-interpreted and vulnerable to abuse. In addition, there are no specific regulations governing violent crimes such as ransomware attacks, deepfakes, or systematic data theft. Regulations that are not comprehensive are the main obstacles in law enforcement. The ITE Law, although it has become an important foundation, still has weaknesses in terms of the scope and clarity

of its articles. This has led to difficulties in handling new and complex criminal cases. There is a need for revisions to the ITE Law and the development of special regulations that are more adaptive to technological developments.

2. **Limited Capacity of Law Enforcement Officers**

Law enforcement officials, such as the National Police and the Prosecutor's Office, face limitations in terms of human resources, technology, and budget. The resource person stated that many officials do not have adequate technical expertise to handle criminal cases. In addition, the available digital forensic tools are also limited, thus hampering the investigation process. The limited capacity of law enforcement officials is a serious challenge in law enforcement of crimes in the country. Training and competency improvement in the field of information technology is an urgent need. In addition, the government needs to allocate a larger budget for the procurement of supporting tools and technologies, such as digital forensic software.

3. **Low Public Awareness**

Based on interviews with cybersecurity practitioners and academics, it was found that public awareness of cybersecurity is still low. Many victims of violent crime do not realize that they have been targeted, so they do not report the incident to the authorities. In addition, the public also lacks understanding of the importance of protecting personal data and using technology wisely. Low public awareness of cybersecurity is an obstacle in law enforcement. Education and socialization about cybersecurity need to be improved, both through public campaigns, educational curricula, and special training. Raising public awareness will help reduce vulnerability to violent crime and increase participation in case reporting.

4. **Characteristics of Cross-Border Crimes**

Crimes of interracial nature are often transnational, requiring intensive international cooperation. However, coordination between countries in handling this crime is still not optimal. The resource person stated that differences in regulations and national interests between countries often hinder the law enforcement process.

The characteristics of cross-border crimes demand more effective international cooperation. Indonesia needs to strengthen cooperation with other countries, both through bilateral and multilateral agreements, to facilitate the extradition process, information sharing, and handling of interstate crime cases involving perpetrators from abroad.

Based on the above findings, this study provides several recommendations to improve the effectiveness of law enforcement against violent crime in Indonesia:

1. Regulatory Revision

   This effort can be done by revising the ITE Law and developing special regulations that are more adaptive to technological developments.
2. Increasing the Capacity of the Apparatus

   This effort can be done by providing training and competency improvement for law enforcement officials, as well as allocating a budget for the procurement of supporting tools and technology.
3. Community Education

   This effort can be done by raising public awareness about cybersecurity through public campaigns, educational curricula, and specialized training.
4. International Cooperation

   This effort can be done by strengthening international cooperation in handling violent crime, including through bilateral and multilateral agreements

5. DISCUSSION

Based on the results of qualitative research on the obstacles and challenges of law enforcement against violent crime in Indonesia, there are several important points that need to be discussed further. This discussion will relate the research findings to a broader context, including policy implications, law enforcement practices, and efforts that can be made to address these challenges.

The findings of the study show that the ITE Law, as the main regulation in handling cybercrime, is considered to be unable to accommodate all forms of cybercrime that continue to develop. Articles such as Article 27 and Article 28 of the ITE Law are often multi-interpreted and vulnerable to abuse, thus causing controversy in their enforcement. This indicates the need for revisions to the ITE Law to clarify the scope and definition of the crime of interracial crime. In addition, the lack of specific regulations for crimes such as ransomware, deepfakes, or systematic data theft shows that Indonesia needs to develop a legal framework that is more adaptive to technological developments. Comprehensive regulations will make it easier for law enforcement officials to handle new and complex cases of violent crime.

The capacity of law enforcement officials, both in terms of human resources, technology, and budget, is a serious challenge in law enforcement of crimes against humanity. Many officers do not have adequate technical expertise to handle cybercrime cases, while the digital forensic tools available are also limited. This leads to a slow investigation process and case

handling. To overcome these limitations, efforts are needed to increase the capacity of law enforcement officials through training and certification in the field of information technology and cybersecurity. In addition, the government needs to allocate a larger budget for the procurement of supporting tools and technologies, such as digital forensic software and cyberattack early detection systems.

To increase public awareness, massive education and socialization efforts are needed through various channels, such as social media, public campaigns, and educational curriculum. Special training on cybersecurity can also be provided to vulnerable community groups, such as small and medium enterprises (SMEs) and the younger generation.

Indonesia needs to strengthen international cooperation in handling crimes between them, both through bilateral and multilateral agreements. For example, by expanding membership in international organizations such as INTERPOL or the ASEAN Cyber Capacity Program. In addition, it is necessary to establish a mechanism that facilitates the extradition process and information sharing between countries. Harmonization of regulations between countries is also needed to facilitate the handling of criminal cases involving perpetrators from abroad. For example, by adopting international standards in the handling of cybercrime, such as the Budapest Convention on Cybercrime.

6. CONCLUSION

Law enforcement against crimes in Indonesia still faces significant obstacles and challenges. Although there have been regulations such as the ITE Law and the PDP Law, their implementation is still ineffective because several articles are multi-interpreted and have not accommodated technological developments and increasingly complex types of digital crime. In addition, the capacity of law enforcement officials is still limited, both in terms of technical expertise, human resources, and available digital forensic technology. This causes the investigation of the crime of mayantara to be less than optimal. Public awareness of cybersecurity is also still low, which makes many individuals vulnerable to cyberattacks and other digital crimes. On the other hand, the cross-border nature of interstate crime is a challenge because it requires closer international cooperation. Differences in regulations and interests between countries often hinder the investigation and prosecution process of cybercriminals operating globally. To increase the effectiveness of law enforcement against cybercrime, several strategic steps are needed, such as revising and strengthening regulations, increasing the capacity of law enforcement officials through training and providing more sophisticated

technology, and increasing public education and awareness of cybersecurity. In addition, international cooperation must be strengthened to deal with transnational crimes.

7. LIMITATION

This research has several limitations that need to be considered:

1. Geographic Coverage

   This study focuses only on Indonesia, so the findings and recommendations may not be fully applicable to other countries with different legal and technological contexts.

2. Primary Data Limitations

   Although in-depth interviews are conducted with a wide range of stakeholders, the limited number of participants (15-20 people) may not be representative of all perspectives that exist in the cybersecurity industry.

3. Reliance on Secondary Data

   Some of the data used comes from industry reports and case studies that may not always reflect the current or specific situation in Indonesia.

4. Participant Bias

   Interviewed participants may have certain biases, especially if they come from the same background or have a particular interest in the cybersecurity industry.

5. Time Limitations

   This research was conducted in a limited time, so not all aspects of the crime can be explored in depth.

Considering these limitations, this study provides a good basis for understanding the challenges of law enforcement against violent crime in Indonesia, but further research is needed to overcome these limitations and expand the scope of the analysis.

8. REFERENCES

Ali, A., & Hassan, M. (2022). Cyber Terrorism and Its Global Impacts. *Journal of Cyber Security*, 15(2), 45-60.

APJII. (2023). *Internet Penetration Survey in Indonesia 2023*. Indonesian Internet Service Providers Association.

Asshiddiqie, J. (2020). *Introduction to Law: Legal Theory and Practice in Indonesia*. Jakarta: Rajawali Press.

Brown, L., & Taylor, K. (2020). The Socioeconomic Impacts of Cybercrime. *Cyber Security Review*, 18(3), 112-125.

BSSN. (2021). *Annual Report on Cybersecurity Threats in Indonesia*. National Cyber and Cryptography Agency.

Butt, S. (2020). *The Indonesian Legal System: Legal Reform and the Courts*. Australian Journal of Asian Law, 21(1), 1-15.

Chen, H., Smith, D., & Lee, R. (2022). Advances in Cybersecurity Technologies. *International Journal of Digital Security*, 27(4), 98-110.

Hadjon, P. M. (2021). *Legal Pluralism in Indonesia: Challenges and Opportunities*. Journal of Law and Development, 51(2), 123-140.

Jones, P., & Xu, L. (2021). Cyber Fraud and Online Scams: Trends and Countermeasures. *Global Journal of Internet Crime*, 9(1), 30-48.

Kaspersky. (2023). Annual Cybercrime Report 2023. *Kaspersky Lab Publications*.

Kominfo. (2022). *The Level of Public Awareness of Cyber Security in Indonesia*. Ministry of Communication and Information of the Republic of Indonesia.

Latukau, F. (2019). A Study Of The Progress Of The Role Of The Police In The Criminal Justice System. Law, Vol, XV, N, 1–15.

Mahfud, M. (2019). *Legal Politics in Indonesia*. Jakarta: Pustaka LP3ES.

Martinez, S. (2024). Public Awareness and Cybersecurity Education. *Journal of Cyber Awareness*, 10(1), 15-28.

Mokobombang, M., Darwis, Z., & Mokodenseho, S. (2023). Eradication of Cyber Crime in West Java Province: The Role of Law and Challenges in Law Enforcement Against Digital Crime. *Journal of Law and Human Rights Wara Ciencias*, *2*(6), 517-525.

Nguyen, T., Patel, R., & Singh, M. (2023). Data Breaches in the Digital Era. *Computing and Security Journal*, 14(2), 75-92

Prasetyo, A. (2021). *Challenges of Cyber Law Enforcement in Indonesia: An Analysis of the ITE Law.* Journal of Law and Justice, 10(2), 123-140.

Setiawan, R. (2020). *The Role of Society in Preventing Cybercrime*. Journal of Social and Humanities, 15(2), 78-92.

Smith, J. (2020). Defining Cybercrime in the 21st Century. *International Review of Cyber Law*, 11(4), 55-70.

Suryani, I. (2020). *International Cooperation in Handling Cybercrime: An Indonesian Case Study*. Journal of International Relations, 12(3), 89-104.

1945 Constitution (1945 Constitution) of the Republic of Indonesia.

Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law), amended by Law Number 19 of 2016.

UNODC. (2021). Global Cybercrime Regulations and Policy Frameworks. *United Nations Office on Drugs and Crime Reports*.

Wahyudi, I. (2022). *The Challenges of Law Enforcement in Indonesia: A Case Study of Corruption and Legal Reform*. Journal of Law and Justice, 10(1), 45-60.

Wibowo, D. (2022). *The Capacity of Law Enforcement Officers in Handling Mayantara Crimes in Indonesia*. Journal of National Security, 8(1), 45-60.