JOURNAL OF WORLD SCIENCE
https://jws.rivierapublishing.id/index.php/jws
Volume 5 No. 5 May 2026
P-ISSN: 2828-8726
E-ISSN: 2828-9307

The Misuse of Social Media as a Means of Electronic Transactions in the Ambon Class I Type a Navigation District

Rusly Karim*, D. J. A. Hehanussa, Elsa R. M. Toule
Universitas Pattimura, Indonesia
Email: leeruka82@gmail.com*

ABSTRACT

This study discusses the misuse of social media as a means of illegal electronic transactions in the Ambon Class I Type A Navigation District, particularly in relation to cyber fraud and identity abuse in the digital era. The research aims to analyze the forms of social media misuse, identify the modus operandi used by perpetrators, and evaluate the effectiveness of law enforcement against cybercrime involving government institutions. This research employed a normative juridical method using statutory, conceptual, and case approaches. Primary legal materials included the Indonesian Electronic Information and Transactions Law, the Criminal Code, and the Personal Data Protection Law, while secondary materials consisted of journals, books, and relevant legal documents. The findings reveal that the primary form of abuse involved fictitious PPPK recruitment fraud through fake social media accounts, falsified electronic documents, phishing practices, and manipulation of institutional identities, resulting in significant financial losses for victims. The study also found that law enforcement remains ineffective due to limitations in digital forensic infrastructure, difficulties in identifying anonymous perpetrators, weak coordination among institutions, and low public digital literacy. Furthermore, the absence of verified official social media accounts increased the vulnerability of institutional identity misuse. The study concludes that although Indonesia has adequate legal regulations to address cybercrime, effective law enforcement requires stronger digital infrastructure, improved investigative capacity, verified digital communication channels, and greater public awareness regarding cyber fraud prevention.

Keyword: Social Media Misuse; Illegal Electronic Transactions; Law Enforcement; Ambon Navigation District; Cybercrime.

INTRODUCTION

The rapid development of information and communication technology has fundamentally changed the order of life of modern society around the world, including in Indonesia. The digital era marked by massive internet penetration and widespread use of social media has created a new public space that is much more dynamic and complex than any physical space before (APJII, 2024). In Indonesia, Law No. 11 of 2008 concerning Electronic Information and Transactions (UU ITE) which was later revised through Law No. 19 of 2016 and finally amended by Law No. 1 of 2024, serves as a legal umbrella that regulates all activities and transactions that use electronic media, while protecting the public from potential cybercrime (Sitompul, 2012). The scope of the ITE Law is very broad, covering electronic transactions from online buying and selling to digital contracts, communication activities through social media and instant messaging applications, as well as various forms of cybercrime such as system break-ins, virus spread, and misuse of personal data. Behind the ease and speed of access to information offered by social media, new challenges have also emerged in the form of misuse of the platform for illegal purposes, including as a means of fake electronic transactions that are detrimental to the public (Barkatullah, 2019).

Social media has evolved from just a tool of communication and social interaction to a complex economic ecosystem, where buying and selling transactions, promoting goods and services, and recruiting labor are mostly done through platforms such as Facebook, Instagram, WhatsApp, and TikTok (Hananto, 2023). This phenomenon known as *social commerce*, although it provides convenience and efficiency, also carries the potential for multiplying

misuse of personal data, as a result of the risks in the use of social media and e-commerce at the same time. Excessive collection of user data by social media platforms has the potential for serious abuse, such as monopolistic practices such as *cross-sharing data*, *tying and bundling*, *self-preferencing tracking*, or *ranking manipulation* that leads to unfair business competition practices. In this context, the urgency of regulating and enforcing the law against the abuse of social media as a means of electronic transactions is becoming increasingly urgent to be carried out (Srnicek, 2017).

Cybercrime in Indonesia shows a significant increase trend from year to year, both in terms of the number of reports and the number of losses experienced by the community. The Directorate of Cyber Investigation of the Metro Jaya Police recorded a surge in cybercrime throughout 2025 with 4,271 police reports coming in, of which the most cases are online fraud or *scams* that continue to take victims (Wahid & Labib, 2021). Of the thousands of reports, online fraud occupies the highest position with 1,951 reports, followed by illegal access with 1,011 reports, threats and extortion with 424 reports, defamation with 333 reports, electronic document manipulation with 199 reports, and online pornography with 154 reports. These figures are just the tip of the iceberg considering that there are still many cases that are not reported by victims for various reasons, ranging from embarrassment, ignorance of reporting procedures, to the assumption that the legal process will not yield satisfactory results (Sahara & Kuswandi, 2025).

One of the most troubling and growing modes of cybercrime is fraud on behalf of government agencies or public officials through social media. The pattern of profiteering the names of government officials or agencies is the most dominant category of hoaxes in various findings in the field. The Bojonegoro District Attorney's Office, for example, appealed to the public to always be vigilant against fraudulent actions on behalf of agencies or Main Officials (PJU) of the Prosecutor's Office because of the rampant fake accounts on social media using the identity of prosecutor's officials in the mode of asking for money, donations, or assistance in any form through social media or telephone. The Head of the Bojonegoro District Attorney's Office officially sent a letter to the Regent to instruct all levels of government and the community to be extra vigilant against the maneuvers of the criminals, considering that the modus operandi used was very convincing and detrimental to many parties (Kejaksaan Negeri Bojonegoro, 2024).

Similar phenomena also occur at the national level in more dangerous modes, such as the fraud case on behalf of the Corruption Eradication Commission (KPK) that befell Deputy Chairman of Commission III of the House of Representatives of the Republic of Indonesia Ahmad Sahroni in early April 2026. In this case, the perpetrator with the initials TH (48) used a fake identity as part of the KPK team and asked for money of up to Rp300 million, with evidence confiscated in the form of money of around 17,400 US dollars or the equivalent of Rp300 million, as well as a number of fake attributes such as stamps and letters with KPK headplates (Kompas.com, 2026). Sahroni considers this mode to be very dangerous because it targets public trust in state institutions, and the actions of the perpetrators are more appropriately categorized as fraud on behalf of the institution, not just ordinary extortion. This case proves that fraud on behalf of government institutions is not only financially detrimental but also has the potential to damage public credibility and trust in state institutions that are supposed to be at the forefront of law enforcement and public services (Fukuyama, 2024).

Londok in the journal *Lex Crimen* revealed that although regulations related to *cyber crime* have been regulated in legislation, the reality on the ground shows that the application of criminal sanctions against cybercrime perpetrators still faces various obstacles. Some of them are the lack of understanding of law enforcement officials on the technical aspects of cybercrime, weaknesses in law enforcement, and challenges in identifying and arresting perpetrators who often operate across countries (Londok, 2014). One of the biggest challenges in law enforcement against *cyber crime* is the gap between existing regulations and implementation on the ground, where the law often cannot be applied optimally, either due to limited digital evidence or due to a lack of coordination between law enforcement agencies and related agencies (Marzuki, 2021).

The challenges of cybercrime law enforcement in the digital era are increasingly complex with the nature of crimes that are cross-jurisdictional and the rapid development of technology. Nurjanah (2026) in her research at the Proceedings of the National Seminar of SENPISHUM, State University of Jakarta, emphasized that law enforcement against cybercrime in the digital era faces complex challenges due to the rapid development of information technology and the nature of crime that crosses jurisdictional boundaries. The results of his research show that although the latest ITE Law provides a more comprehensive and adaptive legal foundation, there are still obstacles to implementation such as limited technical capacity of the apparatus, difficulties in coordination across institutions and internationals, and regulations that are not fully harmonized (Nurjanah, 2026).

Hartanto, Mutiara, Wahyuningtyas, and Kusumawiranti in the Lontar Merah journal, which analyzed significant regulatory changes based on Law No. 1 of 2024 as the second amendment to the ITE Law, revealed that the changes did clarify several material provisions including regulations on Electronic System Operators (PSE), child protection, and certain criminal limits (Hartanto et al., 2024). Nevertheless, the main challenges remain in the technical capacity of law enforcement, cross-border jurisdictions, and personal data protection mechanisms. This study recommends strengthening digital forensic units and continuous training, harmonizing work procedures between PSEs and law enforcement officials for adequate access to electronic evidence, and drafting national operational guidelines that combine legal certainty and human rights protection.

The Type A Navigation District Class I Ambon, as a Technical Implementation Unit within the Directorate General of Sea Transportation of the Ministry of Transportation, has a very vital task and function in ensuring shipping safety in the waters of Maluku and its surroundings. Based on data from various news sources, the Ambon Navigation District is not only tasked with taking care of shipping safety in the form of infrastructure such as beacon signs, *beacons*, and other navigational aids, but is also seconded in the context of saving humanity (Ministry of Transportation of the Republic of Indonesia, 2023). The Head of the Ambon Class I Navigation District, Andi Fiardi, emphasized that the function of shipping navigation is not only related to the safety of shipping through infrastructure, but also includes the rescue of humanity, as evidenced when the Ambon Navigation District deployed KN Bacan to evacuate the Terajana Motor Sailing Ship and its 17 passengers who experienced engine failure and floated in the waters of Seram Island.

In addition to these operational tasks, the Type A Class I Navigation District of Ambon is also active in educational and socialization activities to the community. The Ambon

Navigation District held the Navigation *Goes to School Program* in collaboration with Prosperous Early Childhood Education (PAUD) to introduce the duties and functions of shipping navigation from an early age, with the hope of encouraging children to understand and love the duties and functions of navigation and shipping. The Navigation District also held socialization on the implementation *of the Automatic Identification System* (AIS) on Shipping Channels in the waters of Maluku and North Maluku as well as conducting social service activities at the Ambon Women's Correctional Institution. These various activities show that the Navigation District has a fairly high public visibility in the eyes of the people of Maluku, which unfortunately can be used by irresponsible parties to commit fraudulent acts on behalf of the institution.

In the midst of various positive activities carried out by the Type A Class I Navigation District of Ambon, this institution has actually been the target of misuse of names by irresponsible individuals who commit employee recruitment fraud through social media. Based on a report compiled by October 2024, there was a case of alleged fraudulent recruitment of Government Employees with Employment Agreements (PPPK) in the Ambon Class I Type A Navigation District in a very structured and convincing mode. The reported party, known as Amalia Rumida alias Amel, in carrying out her action of selling her in-laws' name as the Head of Personnel Subdivision in the Type A Navigation District Class I Ambon, and even sent a circular announcing the results of the PPPK selection with the number PG.33 of 2024 to convince the victim (Terasmaluku.com, 2024).

Even more astonishing, after the victim, named Jarnawi Sondi, deposited money gradually every time asked in the hope of becoming an employee of the Ambon Type A Class I Navigation District, the reported person again asked for a sum of money under the pretext of making an official uniform. The total amount of deposits that have been deposited by the victim reaches IDR 14,950,000, and this case has been reported to the Maluku Police Integrated Police Service Center (SPKT) on October 9, 2024. What is more worrying, the victim's brother, Bambang Sondi, expressed suspicion of insider involvement considering that the letter number used by the perpetrator was recorded in the administrative data of the Ambon Navigation District even though it was different (Sitompul, 2024).

This incident is not an isolated case, but part of a broader pattern of fraud on behalf of government agencies in Maluku. Almost at the same time, at the same city level, PPPK recruitment fraud is also rampant which profitees from the name of the Mayor of Ambon, Bodewin Wattimena. The Mayor of Ambon even went so far as to declare an open war against pungli and PPPK recruitment fraud, with a firm statement that there is no one close to the mayor, no back lane, and anyone who asks for money with the name of the mayor is a fraud that must be processed by law. This situation shows that the problem of misuse of the name of government agencies through social media in the Maluku region has reached an alarming level and requires serious attention from all stakeholders (Pemerintah Kota Ambon, 2024).

Based on the above background, the problem that will be studied in this study is how the form of misuse of social media as a means of electronic transactions that occurs on behalf of the Type A Class I Navigation District of Ambon, as well as how to enforce the law against the abuse of social media. This study aims to analyze and find the right legal conception in overcoming the abuse of social media on behalf of the Type A Navigation District Class I Ambon, by contributing to the development of cyber law in Indonesia, especially in the

protection of government institutions from digital identity crimes. In addition, this study aims to identify, describe, and analyze various forms of social media abuse, including modus operandi, perpetrator characteristics, victim profiles, and factors that cause these crimes. This research also aims to analyze and evaluate the effectiveness of law enforcement that has been carried out by law enforcement officials and related agencies, identify the obstacles faced, and formulate policy recommendations to improve the effectiveness of law enforcement in the future. In addition, this study aims to formulate an ideal law enforcement model and preventive policy recommendations to protect the good name of the institution and prevent misuse of names by irresponsible parties on social media.

This research is expected to provide benefits both theoretically and practically. Theoretically, this research is expected to contribute to the development of legal science, especially in the field of criminal law and cyber law, related to the concept of social media abuse on behalf of government institutions. More specifically, this research can enrich the study of the application of Law Enforcement Theory and Legal System Theory in the context of cybercrime involving government institutions. Practically, this research is expected to provide constructive input for law enforcement officials in increasing their capacity in handling cases of social media abuse, including in digital investigation techniques, electronic evidence management, and coordination between institutions and jurisdictions. In addition, this study is expected to provide guidance for the Type A Navigation District Class I Ambon in making preventive efforts to protect the good name of the institution, strengthen cybersecurity, and develop reporting protocols and quick responses to indications of name misuse. This research is also expected to increase public awareness and digital literacy, especially in the Maluku region, regarding fraudulent modes on behalf of government agencies through social media. The results of this research are expected to be public education materials that are disseminated through various communication channels and provide input for improving regulations related to cybercrime and personal data protection in Indonesia.

METHOD

Types of Research

The type of research used in this study is normative legal research (normative juridical). Normative legal research is research that examines law as a system of norms, legal principles, laws and regulations, and relevant legal doctrines (Soekanto & Mamudji, 2015). This approach was chosen because this study focuses on analyzing the suitability between the practice of using social media as a means of electronic transactions in the Type A Navigation District Class I Ambon with the applicable positive legal provisions, especially those that regulate Information and Electronic Transactions (ITE), the misuse of social media, and the legal responsibility of the parties.

This normative research is carried out by examining primary legal materials, namely:

1. Laws and regulations such as Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions,
2. Government regulations, as well as other implementing regulations related to electronic transactions and misuse of social media.

This research also uses secondary legal materials in the form of literature, legal journals, previous research results, and relevant legal documents, as well as tertiary legal materials such

as legal dictionaries and encyclopedias. The approaches used in this normative legal research are the statute *approach* and the conceptual approach. The legislative approach is used to systematically examine all the rules governing electronic transactions and social media. A conceptual approach is used to analyze legal concepts such as abuse of rights, the validity of electronic transactions, proof, and legal responsibility in cyberspace (Marzuki, 2017).

Problem Approach

The approach in legal research is a method or perspective used by researchers to approach and analyze the legal problems being researched, thereby determining the direction and depth of the analysis to be carried out. In legal research, there are three main categories of approaches, namely normative approaches that examine legal issues from a positive legal perspective, empirical approaches that examine legal issues as cultural realities, and philosophical approaches that examine legal issues from an ideal perspective (Ali, 2021). This research, which uses the type of normative-empirical legal research, will apply three main approaches, namely:

a. Statute approach

It is the most fundamental approach in normative law research, because positive law is basically a set of rules contained in applicable laws and regulations. This approach is carried out by examining all laws and regulations related to the legal issues being researched. In the context of this research, a legislative approach will be used to analyze in depth various legal provisions that regulate the misuse of social media as a means of electronic transactions, including (Ibrahim, 2012):

1. Law No. 11 of 2008 concerning Information and Electronic Transactions (ITE Law) and its amendments (Law No. 19 of 2016 and Law No. 1 of 2024);
2. the Criminal Code (KUHP), Article 378 concerning fraud, Article 263 concerning forgery of letters, and Article 417 concerning forgery of letters from government agencies;
3. Law Number 27 of 2022 concerning Personal Data Protection (PDP Law);
4. Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions.

b. Conceptual Approach

It is an approach that moves from the views and doctrines that have developed in the legal sciences, which are used to identify, clarify, and analyze legal concepts that are relevant to the problem under study.

Furthermore, a conceptual approach will also be used to analyze various legal theories that are the framework of this study, namely (Mertokusumo, 2007):

1. Law Enforcement Theory (Lawrence M. Friedman);
2. Legal System Theory.

c. Case Approach

It is an approach that is carried out by examining court decisions related to the legal issues being studied, to understand how judges interpret and apply legal provisions in concrete cases. In the context of this study, a case approach will be used to analyze court decisions relevant to the misuse of social media as a means of electronic transactions, especially fraud cases on behalf of government institutions or public officials (Mertokusumo, 2007).

Legal Material Collection Techniques

The technique of collecting legal materials is a very important operational step in legal research, because the quality of the data collected will greatly determine the quality of the analysis and conclusions produced. In normative-empirical legal research like this, the technique of collecting legal materials is carried out through two main paths, namely (Waluyo, 2016):

a. Primary legal material

It is a binding and authoritative legal material, consisting of laws and regulations and other official legal documents issued by the competent institution. In this study, the primary legal materials that will be collected and analyzed include:

1. Law No. 11 of 2008 concerning Information and Electronic Transactions (Statute Book No. 58 of 2008);
2. Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions;
3. Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions;
4. the Criminal Code (KUHP);
5. Law Number 27 of 2022 concerning Personal Data Protection;
6. Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions.

b. Secondary legal material

It is a legal material that provides explanation, interpretation, or analysis of primary legal materials, which consists of various legal literature such as textbooks, scientific journals, legal articles, seminar papers, and the doctrine of legal experts. In this study, secondary legal materials to be collected include:

1. Textbooks on cyber *law*, criminal law, and legal research methodologies;
2. National and international scientific journals; and
3. Seminar papers and proceedings.

c. Tertiary legal materials

It is a legal material that provides instructions or explanations of primary and secondary legal materials, which are usually in the form of legal dictionaries, legal encyclopedias, journal indexes, and bibliographies. In this study, the tertiary legal materials that will be used include:
(1) Indonesian legal dictionary and English-Indonesian legal dictionary;
(2) Legal encyclopedia; and
(3) Catalogs and indexes from legal libraries and journal databases (Amiruddin & Asikin, 2018) :

Legal Material Collection Techniques

Legal Materials Collection Techniques are carried out by searching, identifying, inventorying, and systematically studying various legal materials that are relevant to research problems. In addition to literature studies, this study will also use field *research* techniques to collect primary data that cannot be obtained from literature materials. The primary data to be collected includes (Soekanto, 2014):

(1) Data on the law enforcement process of PPPK recruitment fraud cases on behalf of the Ambon Class I Type A Navigation District, which will be obtained through interviews with law enforcement officials at the Ambon Police and/or the Maluku Police;
(2) Data on the perspective and experience of the victim of fraud, which will be obtained through interviews with victims or victims' families who are willing to be interviewed;
(3) Data on social media management policies and practices and information security in the Ambon Type A Class I Navigation District, which will be obtained through interviews with Navigation District employees, especially those responsible for public relations, personnel, and information technology; and
(4) Data on the general public's perception of fraud modes on behalf of government agencies, which will be obtained through interviews with several community members in the Ambon region who are selected purposively.

Legal Material Analysis

Legal material analysis is a central stage in the legal research process, where data that has been collected through literature studies and field studies is processed, interpreted, and evaluated to produce research findings and conclusions. In normative juridical law research like this, the analysis of legal materials is carried out using methods, namely:

a. Descriptive analysis methods

It is used to describe systematically, factually, and accurately the facts, characteristics, and relationships between the phenomena being studied, without manipulating or making judgments in advance. In the context of this study, descriptive analysis will be used to:

(1) Describe in detail various forms of misuse of social media as a means of electronic transactions that occur on behalf of the Type A Class I Navigation District of Ambon, including modus operandi, characteristics of the perpetrators, profile of the victim, and chronology of the incident;
(2) Systematically describe the legal framework that regulates the misuse of social media in electronic transactions, both in the ITE Law, the Criminal Code, and other laws and regulations;
(3) Describe the law enforcement process that has been carried out by law enforcement officials in handling cases of social media abuse on behalf of the Navigation District, including the stages of investigation, investigation, prosecution, and court decisions (if any); and
(4) Describe the factors that affect the effectiveness of law enforcement, both internal (structure, substance, legal culture) and external (technological, social, economic). This systematic and factual description forms the foundation for further analysis, because without a clear understanding of "what happened", it is impossible to make an evaluation of "whether what happened was as it should be".

b. Prescriptive analysis methods

Used to provide an assessment and recommendation of what should be done under applicable law, or to evaluate whether an action, policy, or decision is in accordance with the relevant legal provisions. In normative legal research, prescriptive analysis is a distinctive feature that distinguishes it from pure social research, which usually only stops at the descriptive or explanatory level. In the context of this study, prescriptive analysis will be used to:

(1) Evaluate whether the law enforcement that has been carried out by law enforcement officials against cases of social media abuse on behalf of the Navigation District has been in accordance with the provisions of the ITE Law, the Criminal Code, and other laws and regulations;
(2) Identify whether there are deficiencies or weaknesses in existing law enforcement, whether they come from the substance of the law, law enforcement structure, or legal culture; and
(3) Formulate normative policy recommendations on what law enforcement officials, Navigation Districts, and other stakeholders should do to improve law enforcement effectiveness and prevent similar abuses in the future (Soekanto & Mamudji, 2015).

RESULTS AND DISCUSSION

Forms of Abuse of Social Media as a Means of Electronic Transactions that Occur on Behalf of the Type A Class I Navigation District of Ambon

The most significant and documented form of social media abuse in the context of Ambon's Class I Type A Navigation District is the practice of fictitious employee recruitment fraud using a structured operational mode. Based on media investigation reports, this case emerged in October 2024 through allegations of fraudulent selection of Government Employees with Employment Agreements (PPPK) targeting people in the Ambon area (Pelu, 2024). The perpetrator, identified as Amalia Rumida, carried out psychological manipulation by profiteering the identity of an internal official (Head of Personnel Sub-Division) in order to build false credibility in front of the victim (Maluku News Editor, 2024).

To convince the victim administratively, the perpetrator distributed an electronic document in the form of a circular letter announcing the results of the PPPK selection with a fictitious number PG.33 of 2024 through an instant messaging platform (Kantor Distrik Navigasi Kelas I Ambon, 2024). The practice of illegal electronic transactions occurred when the victim, Jarnawi Sondi, deposited funds in stages with a total loss of IDR 14,950,000, which included the pretext of administrative costs to the procurement of official uniforms (Pelu, 2024). This phenomenon shows that the absence of official digital information channels from institutions has been used by criminal actors to create disinformation spaces that facilitate criminal acts of fraud and violations of the Electronic Information and Transactions (ITE) Act (Nasution, 2023).

This operational mode shows the use of social engineering tactics through profiteering the names and positions of structural officials to manipulate the trust of victims. Pseudo-credibility is built by profiteering from the position of the Head of Personnel Sub-Division, which psychologically gives the impression that the perpetrator has authority in the recruitment process (Pelu, 2024). However, a more crucial aspect is the alleged insider involvement or leakage of administrative data. As reported, the letter number PG.33 of 2024 used by the perpetrator was recorded in the administrative system of the Ambon Navigation District, although with different matters (Maluku Terkini Editor, 2024). This indicates a vulnerability in the internal document security system that allows outsiders to access the format or numbering of official letters for criminal purposes (Kurniawan, 2022).

This phenomenon is in line with the national cybercrime pattern where fraud syndicates tend to choose institutions that have high public legitimacy but are weak in digital presence

(Nasution, 2023). Research released in the Supreme Court's Marinews notes that profiteering of official names (such as from the Prosecutor's Office, the Police, or Kodam) is often used to legitimize fraudulent schemes, either through lures or threats (Humas Mahkamah Agung RI, 2023). The strategy of the perpetrators targeting the Ambon Navigation District shows that they are taking advantage of the gap between the great authority of institutions in the real world and the lack of information supervision in the digital world (Pratama, 2025a). This gap provides space for perpetrators to build false narratives that are difficult to verify instantly by the general public (BSSN, 2024).

In addition to recruitment fraud, Ambon's Class I Type A Navigation District faces real risks from fraudulent schemes for fictitious procurement of goods and services. This mode involves using official attributes such as the name and logo of the institution on fake social media accounts to ensnare vendors with offers of fake navigation projects (Editor Tribrata News Polri, 2025). Perpetrators generally ask for an initial payment as an auction guarantee or administrative fee through unofficial communication channels (Dinas Sosial Provinsi Jawa Tengah, 2025). This pattern is identical to the incidents experienced by the Bojonegoro District Attorney's Office, where fake WhatsApp and Facebook accounts profited from the identity of the Chief Officials to request certain funds or assistance (Humas Kejari Bojonegoro, 2025). This vulnerability is particularly relevant for Navigation Districts considering that the cycle of procurement of navigation facilities of strategic value is often an easy target for criminals who monitor the agency's public information (Setiawan, 2022).

This risk is exacerbated by the phenomenon of online impersonation or online impersonation. The research entitled "Online Identity and Cybercrime: Unmasking Threats in the Digital Age" (2025) reveals that identity abuse is one of the most massive threats in Indonesia along with rapid digitalization (Sitorus, 2025). Based on the latest data, there will be more than 229.4 million internet users in Indonesia by 2025, with a penetration rate of 80.66% (APJII, 2025). Of these, around 143 million people are active users of social media (We Are Social, 2025). In the absence of verified official accounts (blue ticks), the public loses the key validation instruments to distinguish authoritative information from impersonator accounts, thus increasing vulnerability to catfishing practices and institutional identity-based fraud (Pratama, 2026a).

Other methods of misuse of information that threaten the credibility of the Type A Class I Navigation District of Ambon are *phishing* and *social engineering attacks*. Perpetrators can distribute fake electronic form links that resemble the official interface of agencies to steal sensitive data such as banking credentials or OTP codes belonging to partners and prospective employees (Editor Tribrata News Polri, 2025). This trend is confirmed by data from the Ministry of Communication and Digital (Komdigi) which recorded a significant spike in the handling of fraudulent content; from 19,137 cases in the period from October 2024 to August 2025, the figure increased sharply to 26,634 content by the end of October 2025 (Kementerian Komunikasi dan Digital RI, 2025). This improvement confirms that psychological manipulation techniques through fake links are becoming a key instrument in today's cybercrime ecosystem (Nasution, 2026a).

In addition, the threat of sending fake invoices or bills to third parties is a very serious financial risk. The perpetrator can intercept communication lines and send fictitious bills to logistics vendors or port service providers with payment instructions to personal accounts

(Setiawan, 2024). A similar mode has been identified in the case of *Online Single Submission* (OSS) service fraud in Bontang, where the perpetrator sent a payment request letter accompanied by valid data of the victim's company to create a legal impression (Humas DPMPTSP Kota Bontang, 2025). For the Navigation District, which has an extensive ecosystem of cooperation with various vendors, this mode not only has the potential to cause massive material losses but can also damage strategic partnership relationships and institutional reputations in the eyes of the public (Pratama, 2026b).

The urgency of handling social media abuse is supported by the findings of cross-border research in the journal Frontiers in Sociology (2025) entitled "Social Media Impact on Societal Security". The study revealed that 81.80% of respondents acknowledged the negative impact of social media on public safety, which indicates that digital threats have become a mass security phenomenon (Smith et al., 2025). In the local context, the recruitment fraud case in the Ambon Navigation District is not an isolated incident, but part of a pattern of systematic cybercrime in Maluku, similar to the case of profiteering the name of the Mayor of Ambon, Bodewin Wattimena, in the PPPK recruitment scam (Maluku Terkini Editor, 2023).

From the perspective of criminal law, this act fulfills the elements of the criminal Code Article 378 regarding fraud through the use of false identities and false dignity for self-gain (Nasution, 2024a). More specifically, because it involves a digital medium, the perpetrator can be charged with Article 28 paragraph (1) of Law No. 1 of 2024 (Second Amendment to the ITE Law) related to the spread of fake news that harms consumers in electronic transactions, with a criminal threat of 6 years in prison.

The most serious violations occurred in the manipulation of electronic documents (such as the fictitious circular PG.33 of 2024), which is classified as data forgery based on Article 35 of the ITE Law. Considering that the forged documents are related to government institutions and public services, the criminal threat can be aggravated up to 15 years in prison and a fine of IDR 15 billion as stipulated in the provisions of Article 51 paragraph (1) jo Article 35 of the ITE Law. Strict law enforcement is essential to mitigate public security risks in the increasingly vulnerable digital space (Pratama, 2026c).

Although the regulatory framework regarding cybercrime has been comprehensively regulated in Indonesian legislation, the implementation of criminal sanctions against the perpetrators still faces serious obstacles on the ground. Research by Londok (2025) in the journal *Lex Crimen* highlights the gap between the available legal norms and the reality of law enforcement (Londok, 2025). The main obstacles identified include the limited understanding of law enforcement officials on cyber technical aspects, difficulties in identifying perpetrators who often operate across borders (borderless crime), and difficulties in collecting legitimate digital evidence (Londok, 2025).

This gap causes the law to often not be optimally applied, especially since the evidentiary process in cybercrime requires in-depth digital forensic expertise (Nasution, 2024b). This challenge is exacerbated by the lack of integrative coordination between law enforcement agencies and related technical agencies, so that the effectiveness of cracking down on cybercrime actors is hampered (Pratama, 2024). In general, this emphasizes that the success of cyber law enforcement does not only depend on the strength of regulation, but also on the readiness of human resource infrastructure and inter-institutional synergy (Hartanto, 2023).

Law Enforcement against the Abuse of Social Media as a Means of Illegal Electronic Transactions in the Type A Navigation District Class I Ambon

The law enforcement process against the PPPK recruitment fraud case that profited from the name of the Type A Class I Navigation District of Ambon officially began through the victim's report to the Maluku Regional Police Integrated Police Service Center (SPKT) on October 9, 2024. In the report, it was revealed that the operational mode involved the manipulation of electronic documents in the form of a circular letter announcing the results of the selection number PG.33 of 2024 and the exploitation of family relations with internal officials of the institution (Maluku News Editor, 2024b). Although the total material losses reached tens of millions of rupiah, the follow-up investigation into the perpetrator's digital identity still requires intensive coordination between the police cyber unit and telecommunication service providers (Nasution, 2024b).

On the other hand, the Ambon Police and the Maluku Police have initiated broader preventive and repressive measures to reduce the number of cybercrimes in the Maluku region. In January 2026, the Ambon Police reported strengthening cooperation with the central financial authority to monitor digital transaction anomalies indicated as the result of fraudulent crimes (Humas Polres Ambon, 2026). In addition to routine cyber patrols to mitigate phishing sites, the Maluku Regional Police has established strategic synergy with PT Bank Negara Indonesia (Persero) Tbk Ambon Branch to strengthen the resilience of the digital banking system from cyber attacks (Soplanit, 2026a). The Maluku Police Chief emphasized that increasing digital literacy and supervision of illegal online loans is a top priority to protect the public from more massive economic losses in the era of digital transformation (Pratama, 2026d).

The Maluku Police has proven its operational capacity in dealing with cross-regional cybercrime, despite facing complex jurisdictional challenges. In June 2022, the Maluku Police through the cyber team of the Directorate of Criminal Investigations succeeded in tracking and securing a 16-year-old student with the initials RP in Ambon City for the case of online game account fraud against the victim in Samarinda, East Kalimantan (Pelu, 2022). This success was achieved thanks to the use of the **Salawaku Emarina** application which allows for rapid response coordination between cross-provincial whistleblowers and investigators in Maluku (Humas Polda Maluku, 2022). Although the case ended in mediation, this incident underscores that cybercrime is no longer limited by administrative boundaries, thus requiring strengthening the competence of investigators in handling digital evidence that is *borderless* (Londok, 2025).

At the national level, protection for victims of digital transaction fraud has been strengthened through the establishment of the **Indonesia Anti-Scam Center (IASC)** by the Financial Services Authority (OJK) together with the PASTI Task Force on November 22, 2024 (Soplanit, 2024). IASC serves as an integrated coordination center to accelerate the blocking of bank accounts that are indicated to be used as a reservoir for criminal proceeds. Based on the latest report as of April 2026, IASC has succeeded in freezing funds of financial fraud victims reaching IDR 585.4 billion and paralyzing around 460,000 accounts of perpetrators nationwide (Suara Merdeka Editor, 2026). The synergy between criminal reporting in the police and account reporting on the IASC's official website is a crucial strategy for institutions such as the Ambon Navigation District to mitigate the financial impact of fraudulent practices that profit from the institution's name (Pratama, 2026).

The implementation of cyber law enforcement in the case of the Ambon Navigation District is now based on the latest regulatory framework, namely Law Number 1 of 2024 as the second amendment to the ITE Law. Research by Hartanto et al. (2025) in the *journal Lontar Merah* explains that this regulation has clarified material provisions regarding the responsibilities of Electronic System Operators (PSE) and the limits of cyber crimes (Hartanto et al., 2025). However, the effectiveness of this law still depends on the balance between regulatory innovation and investment in the technical capacity of law enforcement officials, especially in archipelagic areas such as Maluku that require a cross-sectoral range of cooperation (Hartanto et al., 2025).

A major technical challenge in the case of a scam that profitees the name of the Navigation District is the process of identifying the perpetrators who often use digital anonymity or VPN networks to obscure the trail (Kurniawan, 2024a). Verification of the identity of "Amalia Rumida alias Amel" requires synchronizing data between Maluku Police investigators and internal personnel data of the Navigation District to ensure the correctness of the claim of family relationships (Maluku Terkini Editor, 2024b). In addition, the management of digital evidence such as *WhatsApp* conversations and electronic transfer evidence must follow strict *chain of custody* procedures in order to have legal legality at trial (Nasution, 2025a). Without the fulfillment of these digital forensic standards, such evidence is vulnerable to being rejected in legal proceedings.

Cyber law enforcement in Indonesia still faces significant structural challenges, as revealed in the study *"Juridical Review of Cybercrimes"* published by the Journal of the National Police Research and Development Institute (2025). The findings of the study highlight the disparity in investigative capabilities between regions and the limitations of qualified digital forensic equipment (Puslitbang Polri, 2025). Although the ITE Law provides broad authority, regulatory barriers in accessing data from banking institutions and digital platform providers often slow down the investigation process (Pratama, 2025b). In the jurisdiction of the Maluku Police, the limitation of forensic infrastructure can be a serious obstacle in processing electronic evidence which is crucial to fully uncover the recruitment fraud case (Nasution, 2025a).

This challenge has become increasingly complex with suspicions of *insider involvement* related to the leak of the Ambon Navigation District internal administration letter number (Maluku Terkini Editor, 2024a). If it is proven that there is employee involvement, either through intentional or negligence in maintaining the confidentiality of documents, then the subject can be charged with Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) Article 67 Disclosure of Personal Data That Does Not Belong to Him or failure to protect data. In addition, the perpetrator can be subject to the article of abuse of authority as stipulated in the Criminal Code article 421 concerning Abuse of Power by Officials. The integrity of the electronic document management system is a determining factor in preventing the misuse of internal information by irresponsible parties (Kurniawan, 2024b).

As an urgent preventive measure, the Type A Class I Navigation District of Ambon needs to immediately build a professional digital presence through the creation of verified official social media accounts (blue checkmarks) on major platforms such as Facebook, Instagram, and WhatsApp Business (Kementerian Kominfo RI, 2024). The management of this account must be supported by a special team that is proactive in disseminating educational content, counter-

narrative to hoaxes, and providing a complaint hotline for real-time information verification (Kurniawan, 2024c). This strategy is essential to mitigate the risk of profiteering on the name of an institution while building public trust through information transparency (Pratama, 2026f).

Overall, law enforcement against illegal electronic transactions that profit from the name of the Navigation District faces complex challenges that are multidimensional. Although regulations such as the ITE Law and the Criminal Code have provided a strong legal foundation with severe criminal sanctions, their implementation is still hampered by disparities in technical capabilities, limitations in digital forensic equipment in the regions, and potential insider involvement (Puslitbang Polri, 2025). In the future, a holistic approach is needed that integrates strengthening digital infrastructure, cross-sector synergy (police, OJK, Komdigi), and improving the digital literacy of the Maluku people to create a maritime ecosystem that is safe from cybercrime (Nasution, 2026b).

CONCLUSION

The abuse that occurred was in the form of fictitious PPPK recruitment fraud by Amalia Rumida (Amel) in the mode of profiteering the names of Navigation District officials and fake letters (Number: PG.33 of 2024), which resulted in losses of IDR 14.9 million. In addition, there is the potential for project fraud, fake accounts, phishing, and invoice fraud. Law enforcement on this case is relatively weak, where the report that came to the Maluku Police on October 9, 2024 has not shown clear developments. Some of the obstacles faced include difficulties in identifying perpetrators who use VPNs and fake identities, lack of digital forensic equipment, disparity in the capabilities of the apparatus in various regions, and obstacles in accessing banking data and platforms. The root of the problem is (i) the Navigation District that does not have an official social media account and TTIS (Electronic Signature), (ii) the limited capacity of the apparatus in Maluku, and (iii) the low digital literacy of the community, which nationally is only recorded at 65.4%. Coupled with the alleged involvement of internal parties, considering that the fake letter number was found in internal data. Although existing regulations are adequate, such as the ITE Law No. 1/2024 and the Criminal Code which provide a severe criminal threat (up to 15 years), technical and structural obstacles in the implementation of the law are still a major obstacle.

REFERENCES

Ali, Z. (2021). *Metode penelitian hukum*. Sinar Grafika.

Amiruddin, & Asikin, Z. (2018). *Pengantar metode penelitian hukum*. RajaGrafindo Persada.

APJII. (2025). *Laporan survei penetrasi internet Indonesia 2025*. Cloud Computing Indonesia. https://cloudcomputing.id

Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). (2024). *Laporan survei penetrasi internet Indonesia 2024*. APJII.

Badan Siber dan Sandi Negara (BSSN). (2024). *Laporan analisis ancaman siber sektor pemerintahan 2023*. BSSN.

Barkatullah, A. H. (2019). *Hukum transaksi elektronik di Indonesia*. Nusa Media.

Dinas Sosial Provinsi Jawa Tengah. (2025, July 11). *[HOAX] Penipuan pengadaan barang dan jasa mengatasnamakan pejabat Dinas Sosial Provinsi Jawa Tengah*. https://dinsos.jatengprov.go.id

Editor Tribrata News Polri. (2025, October 21). *Waspada modus penipuan digital*

mengatasnamakan instansi pemerintah! Lindungi data dan aset Anda. *Tribrata News Polri*. https://tribratanews.polri.go.id
Fukuyama, F. (2024). *Trust: The social virtues and the creation of prosperity*. Free Press.
Hananto, A. (2023). The rise of social commerce: Analysing consumer behavior on TikTok Shop in Indonesia. *Journal of Digital Economy and Business, 1*(4), 215.
Hartanto, A. (2023). *The evolution of cyber crime and national law enforcement strategies*. PT Remaja Rosdakarya.
Hartanto, A., Mutiara, S., Wahyuningtyas, S., & Kusumawiranti, R. (2025). Analysis of the second amendment to the ITE Law: Challenges and expectations of cyber law enforcement in Indonesia. *Lontar Merah Journal, 6*(2), 128–135.
Hartanto, R., Mutiara, S., Wahyuningtyas, S., & Kusumawiranti, R. (2024). Juridical analysis of the second amendment to the Electronic Information and Transaction Law: Digital transformation and legal certainty. *Lontar Merah Journal, 7*(1), 42.
Humas DPMPTSP Kota Bontang. (2025). *Waspada penipuan mengatasnamakan layanan OSS dan permintaan pembayaran ilegal*. Situs Resmi Kota Bontang. https://bontangkota.go.id
Humas Kejari Bojonegoro. (2024, November 20). *Waspada penipuan mengatasnamakan pejabat Kejaksaan Negeri Bojonegoro*. https://kejaribojonegoro.kejaksaan.go.id
Humas Kejari Bojonegoro. (2025, December 24). *Kejari Bojonegoro imbau masyarakat waspada aksi penipuan mengatasnamakan kejaksaan*. https://bojonegorokab.go.id/berita/9169/kejari-bojonegoro-imbau-masyarakat-waspada-aksi-penipuan-mengatasnamakan-pju-kejaksaan
Humas Mahkamah Agung RI. (2023). *Waspada sindikat penipuan yang mengatasnamakan pejabat dan lembaga negara*. *Marinews Mahkamah Agung*. https://mahkamahagung.go.id
Humas Polda Maluku. (2022, June 3). *Polisi lacak pelaku penipuan game online melalui aplikasi Salawaku Emarina*. *Siwalima Online*. https://siwalima.co.id
Humas Polres Ambon. (2026). *Laporan analisis tren kejahatan siber dan transaksi elektronik ilegal di wilayah hukum Polres Ambon Semester I 2026*. Polres Ambon.
Ibrahim, J. (2012). *Teori dan metodologi penelitian hukum normatif*. Bayumedia Publishing.
Kantor Distrik Navigasi Kelas I Ambon. (2024). *Klarifikasi resmi mengenai surat edaran fiktif rekrutmen PPPK nomor PG.33 Tahun 2024*. Distrik Navigasi Ambon.
Kementerian Komunikasi dan Digital Republik Indonesia (Komdigi). (2025). *Laporan penanganan konten penipuan digital periode Oktober 2024–Oktober 2025 (Press Release No. 42/SP/KOMDIGI/10/2025).* Komdigi.
Kementerian Komunikasi dan Informatika Republik Indonesia (Kominfo). (2024). *Pedoman pengelolaan media sosial bagi instansi pemerintah: Strategi verifikasi dan keamanan informasi*. Kominfo RI.
Kementerian Perhubungan Republik Indonesia. (2023). *Profil keselamatan pelayaran Indonesia: Peran distrik navigasi dalam sistem transportasi laut*. Bakti Perpasa.
Kompas.com. (2026, April 28). *Polisi tangkap penipu yang mencatut nama KPK terhadap Ahmad Sahroni*. https://www.kompas.com
Kurniawan, B. (2022). *Manajemen keamanan informasi dan mitigasi insider threat pada instansi pemerintah*. PT Remaja Rosdakarya.
Kurniawan, B. (2024a). *Cybercrime investigation: Teknik pelacakan dan identifikasi pelaku di ruang digital*. PT Remaja Rosdakarya.
Kurniawan, B. (2024b). *Manajemen risiko keamanan informasi dan mitigasi insider threat pada instansi pemerintah*. PT Remaja Rosdakarya.
Kurniawan, B. (2024c). *Manajemen komunikasi krisis digital untuk lembaga pemerintah*. PT Remaja Rosdakarya.
Londok, J. R. (2014). The application of criminal sanctions for perpetrators of cyber crime in the legislation in Indonesia. *Lex Crimen, 3*(1), 165.

Londok, J. R. (2025). Juridical analysis of law enforcement on cyber crime in the criminal justice system in Indonesia. *Lex Crimen, 14*(1), 42–48.
Maluku News Editor. (2024a, October 9). *Dugaan penipuan seleksi PPPK di Distrik Navigasi Ambon masuk ranah hukum*. *Maluku News Online*. https://malukupost.com
Maluku News Editor. (2024b, October 10). *Polda Maluku terima laporan dugaan penipuan rekrutmen instansi vertikal*. *Maluku News Online*. https://malukupost.com
Maluku Terkini Editor. (2023, November 15). *Waspada penipuan PPPK mengatasnamakan Pj Wali Kota Ambon Bodewin Wattimena*. *Maluku Terkini Online*. https://malukuterkini.com
Maluku Terkini Editor. (2024a, October 11). *Dugaan kebocoran administrasi internal di balik kasus penipuan rekrutmen navigasi*. *Maluku Terkini Online*. https://malukuterkini.com
Maluku Terkini Editor. (2024b, October 12). *Polda Maluku selidiki keterlibatan internal dalam kasus penipuan rekrutmen navigasi*. *Maluku Terkini Online*. https://malukuterkini.com
Marzuki, P. M. (2017). *Penelitian hukum: Edisi revisi*. Prenada Media Group.
Marzuki, P. M. (2021). *Kekuatan alat bukti informasi elektronik dalam persidangan pidana*. Kencana.
Mertokusumo, S. (2007). *Mengenal hukum: Suatu pengantar*. Cahaya Atma Pustaka.
Nasution, M. S. (2023a). *Cybercrime dan perlindungan konsumen di era digital*. Rajawali Pers.
Nasution, M. S. (2023b). *Cyber criminology: Analisis perilaku pelaku kejahatan di ruang digital*. Rajawali Press.
Nasution, M. S. (2024a). *Aspek hukum pidana dalam pemalsuan dokumen elektronik di Indonesia*. Rajawali Pers.
Nasution, M. S. (2024b). *Hukum pidana siber: Tantangan pembuktian dan penegakan hukum di era digital*. Rajawali Pers.
Nasution, M. S. (2025a). *Hukum pembuktian elektronik: Teori dan praktik di pengadilan Indonesia*. Rajawali Pers.
Nasution, M. S. (2026a). *The evolution of phishing: Cyberattack strategies in the public service sector*. Rajawali Pers.
Nasution, M. S. (2026b). *Digital transformation and cybersecurity in Indonesia: Towards a holistic ecosystem*. Rajawali Press.
Nurjanah, S. (2026). Challenges and strategies for cyber crime law enforcement in the digital era after the revision of the ITE Law. *Proceedings of the National Seminar on Education, Social, and Humanities (SENPISHUM) State University of Jakarta, 4*(1), 215.
Pelu, M. M. (2022, June 3). *Warga Kalimantan ditipu game online, pelaku ternyata remaja di Ambon*. *TribunAmbon.com*. https://ambon.tribunnews.com
Pelu, M. M. (2024, October 8). *Mengatasnamakan mertua di Distrik Navigasi Ambon, wanita ini tipu warga puluhan juta dengan loloskan PPPK*. *TribunAmbon.com*. https://ambon.tribunnews.com
Pemerintah Kota Ambon. (2024, October 10). *Pj Wali Kota Ambon tegaskan tidak ada "orang dalam" dalam seleksi PPPK*. https://ambon.go.id
Pratama, R. (2024). Technical and juridical obstacles in the arrest of transnational cybercrime perpetrators. *Journal of Digital Law and Justice, 9*(3), 201.
Pratama, R. (2025a). Analysis of the vulnerability of government institutions to identity profiteering crimes. *Journal of Cybersecurity and Law, 14*(2), 98.
Pratama, R. (2025b). Analysis of structural barriers in electronic data access in electronic system operators. *Journal of Cybersecurity and Law, 14*(2), 89.
Pratama, R. (2026a). Public vulnerability analysis in agencies without digital verification. *Indonesian Journal of Information Security, 16*(2), 82.
Pratama, R. (2026b). Analysis of the impact of reputation due to invoice fraud on government agencies. *Indonesian Journal of Information Security, 16*(2), 95.

Pratama, R. (2026c). The effectiveness of criminal sanctions of the ITE Law in handling fraud on behalf of government agencies. *Journal of Maritime and Cyber Law, 17*(2), 105.
Pratama, R. (2026d). Synergy of law enforcement and the banking sector in mitigating electronic fraud in Maluku. *Journal of Public and Digital Security, 11*(1), 78.
Pratama, R. (2026e). The effectiveness of the Indonesia Anti-Scam Center (IASC) in recovering the assets of fraud victims. *Indonesian Journal of Information Security, 16*(2), 102.
Pratama, R. (2026f). The effectiveness of verified social media accounts in reducing the impersonation crime rate. *Journal of Communication and Informatics, 16*(1), 48.
Puslitbang Polri [National Police Research and Development Center]. (2025). Juridical review of cybercrime: Challenges and constraints in the region. *Journal of National Police Research and Development, 28*(2), 112–115.
Republic of Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. *Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58*.
Republic of Indonesia. (2016). *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.
Republic of Indonesia. (2019). *Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik*.
Republic of Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*.
Republic of Indonesia. (2024). *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.
Sahara, A., & Kuswandi. (2025). Online fraud as a form of cybercrime in a criminological perspective. *Parliamentary Journal of Legal and Public Administration Studies, 2*(4), 95.
Setiawan, D. (2022). *Manajemen risiko penipuan dalam pengadaan barang dan jasa pemerintah*. Penerbit Erlangga.
Setiawan, D. (2024). *Audit investigatif penipuan transaksi elektronik di lingkungan pemerintah*. Penerbit Erlangga.
Sitompul, J. (2012). *Cyberspace, cybercrimes, cyberlaw: Tinjauan aspek hukum pidana*. Tatanusa.
Sitompul, J. (2024). *Penipuan manipulasi identitas dan informasi elektronik dalam UU No. 1 Tahun 2024*. Sinar Grafika.
Sitorus, R. (2025). Online identity and cybercrime: Unmasking threats in the digital age. *USU Journal of Talent, 10*(1), 4.
Smith, J., et al. (2025). Social media impact on societal security: A cross-national analysis. *Frontiers in Sociology, 10*(1), 142. https://doi.org/10.3389/fsoc.2025.0142
Soekanto, S. (2014). *Pengantar penelitian hukum*. UI Press.
Soekanto, S., & Mamudji, S. (2015). *Penelitian hukum normatif: Suatu tinjauan singkat*. Rajawali Pers.
Soplanit, J. (2024, November 24). *OJK dan Satgas PASTI luncurkan Indonesia Anti-Scam Centre*. *Antara News Ambon*. https://ambon.antaranews.com
Soplanit, J. (2026a, January 20). *Polda Maluku dan BNI Ambon perkuat sinergi keamanan digital*. *Antara News Ambon*. https://ambon.antaranews.com
Srnicek, N. (2017). *Platform capitalism*. Polity Press.
Suara Merdeka Editor. (2026, April 29). *IASC blokir dana korban penipuan transaksi keuangan capai Rp585,4 miliar*. *Suara Merdeka Purbalingga*. https://purbalingga.suaramerdeka.com
Terasmaluku.com. (2024, October 25). *Waspada penipuan rekrutmen PPPK di Distrik Navigasi Ambon, oknum catatkan nama pejabat*. https://terasmaluku.com

Wahid, A., & Labib, M. (2021). *Cyber crime*. Sinar Grafika.
Waluyo, B. (2016). *Penelitian hukum dalam praktek*. Sinar Grafika.
We Are Social. (2025, January). *Digital 2025: Indonesia social media trends*. https://wearesocial.com