Cybercrime and Its Countermeasures in the Indonesian Legal System

Zakiul Fuad [*1] Mhd. Azhali Siregar [*2] T Riza Zarzani N [*3]
[123]Panca Budi Development University
E-mail: hudarizka12@gmail.com mhdazhali@dosen.pancabudi.ac.id
trizazarzani@dosen.pancabudi.ac.id

Article Info
Article History
Received: 2025-08-05
Revised: 2025-08-06
Published: 2025-09-10

Keywords:
Phishing, ITE Law, Law Enforcement

Abstract
The rapid development of information technology has provided many conveniences in people's lives, but has also opened up opportunities for cybercrime, one of which is phishing. Phishing is a form of digital fraud by impersonating a trusted party to obtain sensitive information such as personal data and financial credentials. In Indonesia, the rise in phishing cases poses a serious threat to national digital security, especially with the low level of digital literacy in the community. This study aims to evaluate the effectiveness of the Electronic Information and Transactions Law (UU ITE) in dealing with phishing crimes and identify the main obstacles in its enforcement. The method used is normative legal research with a statutory and conceptual approach. The results of the study indicate that normatively, the ITE Law contains several relevant articles to ensnare phishing perpetrators, such as Article 28 paragraph (1), Article 30, and Article 35. However, its effectiveness in practice is still limited due to the lack of an explicit definition of phishing, the difficulty of digital evidence, the weak capacity of law enforcement officers, and the lack of integration of handling mechanisms between agencies. Furthermore, the cross-border nature of phishing adds jurisdictional complexity and demands more intensive international cooperation. Therefore, legal reform is needed through the formulation of specific articles on phishing, strengthening the technical capacity of law enforcement agencies, and developing implementing regulations that support a swift and adaptive legal response to the dynamics of digital crime.

I. INTRODUCTION

The development of information and communication technology has brought significant changes to various aspects of life, including the economic, social, and government sectors. However, this progress has also opened up opportunities for various forms of cybercrime, one of which is phishing. Phishing is a fraudulent act carried out by impersonating a trusted entity to obtain sensitive information such as personal data, financial information, and login credentials.(Dewantoro and Dian Alan Setiawan SH 2023)In Indonesia, phishing cases are increasing due to high internet penetration and low digital literacy. The diverse and evolving modus operandi of phishing makes it difficult to detect and effectively combat. This crime not only harms individuals but can also threaten national security and economic stability.

To address the challenges of cybercrime, the Indonesian government passed Law No. 11 of 2008 concerning Electronic Information and Transactions (UU ITE) as the legal basis for regulating and combating various forms of cybercrime. The ITE Law was subsequently amended through Law No. 19 of 2016 and Law No. 1 of 2024 to adapt to technological developments and societal dynamics.(Setiawan 2021)

Several provisions in the ITE Law that are relevant to phishing crimes include:

- Article 28 paragraph (1): Prohibits the spread of false and misleading news that results in consumer losses in electronic transactions.
- Article 30: Regulates illegal access to other people's electronic systems.
- Article 35: Prohibits the manipulation of electronic information and/or electronic documents with the aim of making it appear as if it were authentic data.
- Article 45A paragraph (1): Regulates criminal sanctions for perpetrators who

spread false and misleading news that results in consumer losses in electronic transactions.

Amendments to Law Number 1 of 2024 also add new provisions such as Article 27B which regulates extortion and/or threats through electronic information and/or electronic documents.(Yudistira and Ramadani 2023)Despite the existence of a legal framework governing cybercrime, law enforcement against phishing cases still faces various challenges. Some of these include:

- Identification of Perpetrators: Phishing perpetrators often use fake identities and operate anonymously, making identification and capture difficult.
- Limited Capacity of Law Enforcement Officials: Lack of resources and technical expertise in cyberspace among law enforcement officials can hamper the process of investigating and prosecuting phishing cases.
- International Cooperation: Due to the cross-border nature of cybercrime, effective international cooperation is needed to handle phishing cases involving perpetrators from abroad.
- Public Digital Literacy: Low public awareness and understanding of phishing threats makes them vulnerable to becoming victims and reluctant to report such incidents to the authorities.

Given the high number of phishing cases and their negative impacts, as well as the challenges to effective law enforcement, in-depth research is needed to evaluate the effectiveness of the ITE Law in addressing phishing crimes in Indonesia. This research aims to:

- Analyzing the extent to which provisions in the ITE Law can be used to ensnare phishing perpetrators.
- Identifying obstacles faced in law enforcement against phishing cases.

Provide recommendations to improve the effectiveness of the ITE Law in dealing with phishing crimes, including proposed policy changes and increasing the capacity of law enforcement officers.

II. RESEARCH METHODS

This research uses a normative legal research method with a statute approach and a conceptual approach.(Indra Utama Tanjung 2024)A legislative approach was used to analyze the positive legal norms contained in Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 19 of 2016 and most recently by Law Number 1 of 2024, particularly provisions relating to phishing crimes. A conceptual approach was used to understand the concept of phishing crimes in the context of cyber law and how their regulation should operate effectively. The data used were secondary data in the form of primary legal materials (statutory regulations), secondary legal materials (legal literature, scientific journals, and academic studies), and tertiary legal materials (legal dictionaries and legal encyclopedias). The data analysis technique was carried out qualitatively, by outlining the relationship between legal norms and empirical facts occurring in society, in order to assess the effectiveness of the ITE Law in dealing with phishing crimes in Indonesia.

III. RESULTS AND DISCUSSION

A. Characteristics and Trends of Phishing Crimes in Indonesia

Phishing is one of the most common and damaging forms of cybercrime in today's digital age. Phishing involves fraudulent attempts to impersonate a trusted entity to obtain sensitive information such as personal data, financial information, and login credentials. Phishing perpetrators utilize social engineering and psychological manipulation techniques to trick victims into providing the desired information.

In Indonesia, phishing cases have shown a significant upward trend in recent years. According to a report from the Indonesia Anti-Phishing Data Exchange (IDADX), the number of phishing reports received in the first quarter of 2023 reached 26,675, a dramatic increase from 6,106 cases in the previous quarter. This increase indicates that phishing is a serious threat to cybersecurity in Indonesia.

Phishing in Indonesia encompasses a variety of evolving methods. Some common types of phishing include:

1. Deceptive Phishing: Perpetrators impersonate trusted entities through fake emails or websites to steal victims' personal information.
2. Spear Phishing: Targeted attacks on specific individuals or organizations with

tailored messages to increase the success of the scam.

3. Whaling: An attack that targets individuals in high positions within an organization, such as executives or senior officials, to gain access to sensitive company information.
4. Smishing: Phishing via text messages or SMS containing links or requests for personal information.
5. Vishing: Phishing via voice or VoIP calls to trick victims into providing personal or financial information.

Phishing modus operandi in Indonesia often exploits current issues or emergencies to increase the effectiveness of attacks. For example, during the COVID-19 pandemic, many phishers impersonated health authorities or aid providers to deceive victims. Furthermore, perpetrators also exploited social media platforms and instant messaging apps to spread phishing links, given the high usage of these platforms in Indonesia.(Majid, Othman, and Onzer 2022)

Phishing trends in Indonesia also indicate that certain sectors are prime targets for attacks. According to the IDADX report, the social media sector was the most frequently targeted sector, accounting for 64.34% of attacks in the fourth quarter of 2023, followed by the financial sector at 20.58%. This suggests that phishing perpetrators are targeting platforms widely used by the public to increase the chances of successful attacks.(Dewantoro and Dian Alan Setiawan SH 2023)

The impact of phishing attacks is devastating, both for individuals and organizations. Victims of phishing can experience financial loss, identity theft, and privacy violations. For organizations, phishing attacks can lead to sensitive data leaks, reputational damage, and significant financial losses. Furthermore, phishing attacks can also be used as a gateway for more complex cyberattacks, such as ransomware or cyberespionage.(Sutarli and Kurniawan 2023)

Addressing the threat of phishing requires a comprehensive approach that includes increasing public awareness and education about cybersecurity, implementing advanced security technologies, and effective law enforcement against phishing perpetrators. The government, the private sector, and the public need to work together to create a safe and trusted digital ecosystem.

In a legal context, the Electronic Information and Transactions Law (ITE Law) serves as the primary foundation for combating cybercrime, including phishing. However, the ITE Law's effectiveness in addressing phishing requires a thorough evaluation, given the ever-evolving complexity and dynamics of cybercrime. This evaluation is crucial to ensure that the existing legal framework provides adequate protection for the public and effectively prosecutes cybercriminals.

The following table shows data on phishing attack trends in Indonesia during the first quarter of 2023:

Month	Number of Phishing Reports
January	7,665 reports
February	15,050 reports
March	3,960 reports
Total	**26,675 reports**

This data shows that February 2023 saw the highest spike in phishing reports, reaching 15,050 cases. The total number of reports during the first quarter of 2023 reached 26,675 cases, a significant increase compared to the 6,106 reports in the fourth quarter of 2022.https://goodstats.id2023)

In addition, the industrial sectors most frequently targeted by phishing attacks during the January–March 2023 period were as follows:

Industrial Sector	Phishing Target Percentage
Social media	45%
Financial institutions	31%
Retail/E-commerce	20%
Spam	2%
ISP	1%
Cryptocurrency	1%

Social media is the primary target of phishing attacks, accounting for 45%. This indicates that phishing perpetrators exploit the popularity and user trust in social media platforms to carry out their attacks. This data underscores the importance of increasing public awareness and education about cybersecurity, as well as the need for effective law enforcement to combat phishing crimes in Indonesia.

B. Obstacles Faced in Law Enforcement Against Phishing Cases

Although Indonesia has a sufficient legal framework through Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) and its amendments in

Law Number 19 of 2016 and Law Number 1 of 2024, law enforcement against phishing crimes remains far from optimal. Phishing, as a form of cybercrime, has unique and highly complex characteristics, including its modus operandi, cross-border nature, and the challenges of digital evidence. This complexity creates various obstacles in the law enforcement process, from reporting and investigation to prosecution and even criminalization. This study aims to analyze in depth the obstacles that systematically weaken the effectiveness of law enforcement in dealing with phishing crimes in Indonesia.(Dhadha et al. 2021)

One of the most fundamental and fundamental obstacles is the aspect of perpetrator identification. Unlike conventional crimes that involve the physical presence of the perpetrator and victim in one location, phishing is carried out by exploiting the anonymity of digital space. Perpetrators can hide behind proxy networks, use dynamic IP addresses or VPNs from other countries, and register phishing site domains through international registrars that are difficult to reach within Indonesian jurisdiction. This identity-masking technology often results in perpetrator identification efforts ending in deadlock due to the lack of alignment between the perpetrator's digital identity and the perpetrator's true legal identity. Law enforcement officials also often encounter difficulties in tracing back the flow of digital data that could reveal the perpetrator's identity and where it originated.(Winarno 2011)

Furthermore, limited human resources within law enforcement agencies pose a serious structural obstacle. Not all police, prosecutors, or other law enforcement personnel possess adequate technical knowledge and skills in digital forensics. Proving a phishing crime requires expertise in analyzing server logs, file metadata, DNS structures, and even digital transaction reconstruction. Currently, this expertise is concentrated in specialized units such as the Cyber Crime Directorate of the National Police Criminal Investigation Agency (Bareskrim Polri) or institutions like the National Cyber and Crypto Agency (BSSN). Meanwhile, at the regional level, authorities still struggle to access sophisticated digital forensic tools or receive adequate technical training. This results in many phishing cases in the regions being unable to be optimally prosecuted and even ending without legal process due to a lack of strong evidence.(Setiawan 2021)

Furthermore, the lack of a specific legal framework also hinders the prosecution of phishing perpetrators. The ITE Law does not explicitly mention the term "phishing," requiring law enforcement officials to interpret and construct phishing acts within general articles, such as Article 28 paragraph (1), Article 30, or Article 35 of the ITE Law. This creates the risk of multiple interpretations and opens up room for differences of opinion among investigators, prosecutors, and judges during the evidentiary process. For example, Article 28 paragraph (1) requires proof that the false information disseminated by the perpetrator is truly misleading and causes concrete losses in electronic transactions. If the victim only experiences data theft without direct financial loss, this element of the offense is often deemed unfulfilled. Similarly, in Article 30 concerning illegal access to electronic systems, the element of "access" is often not technically proven if the perpetrator only reaches the stage of collecting data but has not yet directly accessed the victim's system.

Furthermore, the issue of digital evidence also presents a unique challenge in the criminal justice process for phishing. In the context of proof, phishing requires electronic evidence that can demonstrate a direct link between the perpetrator and the phishing site, email, or domain used in the fraud. This evidence is often distributed across various international digital platforms such as Gmail, WhatsApp, Facebook, and foreign registrar domains. To access data from these platforms, a mutual legal assistance (MLA) mechanism is required between countries, a lengthy, bureaucratic process that often ends in failure due to differences in legal systems or because perpetrators meticulously conceal their digital footprints. As a result, many phishing cases cannot be legally and convincingly proven in court, preventing perpetrators from being convicted even though morally and logically they have clearly committed an unlawful act.

Furthermore, the low level of digital literacy in society also makes it difficult to enforce the law against phishing.(Sutarli and Kurniawan 2023)Most phishing victims are unaware that they have fallen victim to cybercrime, or even attribute the incident to personal negligence, making them reluctant to report it to law enforcement. In many cases, victims only realize they have been deceived after the losses they have suffered are already substantial and irrecoverable. This lack of legal awareness leads

to a high rate of unreported crimes, ultimately obscuring empirical data on the distribution and patterns of phishing crimes in Indonesia. Furthermore, when victims do report the incident, it is often not supported by adequate digital evidence because they lack knowledge of how to preserve digital traces such as email headers, transaction logs, or chat screenshots relevant to the crime they experienced.

Another obstacle arises from the lack of technical regulations to complement the ITE Law, such as provisions explicitly stipulating the obligation of electronic system operators to respond quickly and accurately to phishing reports. Currently, there are no standard operating procedures (SOPs) that govern the steps digital platforms or internet service providers must take when receiving phishing reports from the public. As a result, many phishing sites remain active for days or even weeks even after being reported to the relevant authorities. The lack of detailed technical regulations also means that platform operators are not required to disclose user data suspected of phishing, except through a lengthy legal process. This clearly slows down the case handling process and provides room for perpetrators to cover their tracks or escape legal responsibility.

From a jurisdictional perspective, the transnational nature of phishing crimes also poses significant challenges to law enforcement. Many phishing perpetrators operate from abroad, targeting Indonesian citizens. In such cases, national jurisdiction is limited, and Indonesian law enforcement cannot immediately arrest or investigate perpetrators abroad. This is where international cooperation in cyber law enforcement, whether through ASEAN forums, Interpol, or bilateral agreements such as the Mutual Legal Assistance Treaty (MLA), becomes crucial. Unfortunately, this cooperation remains sporadic and lacks a systematic and operational framework. Many cross-border phishing cases stall due to a lack of procedural understanding between Indonesia and the perpetrators' countries of origin.

Finally, institutional factors and fragmentation between sectors also act as obstacles in enforcing phishing laws.(2013 Investigation)In Indonesia, several institutions are involved in monitoring and handling cybercrime, such as the National Police Criminal Investigation Agency (Bareskrim Polri), the Ministry of Communication and Information Technology (Kominfo), the National Cyber and Cyber Security Agency (BSSN), and the banking sector. However, there is no integrated system linking information and coordination between these institutions. Each institution operates in its own sector, using separate data and different protocols. This lack of integration complicates phishing investigations, which often require rapid cross-agency coordination, particularly to stop attacks, secure phishing sites, and protect victims from further harm.

Given the various obstacles outlined, it is clear that law enforcement against phishing in Indonesia still faces serious challenges across regulatory, technical, operational, and institutional dimensions. Therefore, comprehensive reform is needed, encompassing legal regulations, strengthening the capacity of law enforcement officers, establishing regional cybercrime units, developing technical regulations for handling phishing, and enhancing international cooperation. Without these strategic measures, phishing will continue to develop into a major threat to Indonesia's digital ecosystem, potentially undermining public trust in electronic transactions and information technology in general.

C. The Effectiveness of the ITE Law in Combating Phishing Crimes

Phishing is a form of cyber threat that has evolved alongside advances in information technology. Phishing is not merely a technical violation, but also involves significant complexity in terms of evidence and the normative substance of cybercriminal law.(Dewantoro and Dian Alan Setiawan SH 2023)In Indonesia, the main legal framework used to combat this crime is Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), which has been amended twice, namely through Law Number 19 of 2016 and Law Number 1 of 2024.(Sasuang, Borman, and Handayati 2024)This study aims to analyze the effectiveness of the ITE Law, systematically and critically, in tackling phishing crimes by sharpening the knife of legal analysis.(Dhadha et al. 2021)

Normatively, the ITE Law is a lex specialis for crimes related to electronic systems. This law introduces legal instruments to combat the misuse of information technology, including crimes that rely on digital deception such as phishing.(Rianto, Zarzani, and Saragih 2024)Several key provisions in the ITE Law that have the potential to be used to ensnare phishing perpetrators include:

- Article 28 paragraph (1):

"Any person who intentionally and without authority spreads false and misleading news that results in consumer losses in Electronic Transactions."

- Article 30:

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

- Article 35:

"Any person who intentionally and without authority or against the law manipulates, creates, changes, removes or destroys Electronic Information and/or Electronic Documents with the aim of making it appear as if it were authentic data."

These articles are accompanied by criminal provisions in Article 45A and Article 51 of the ITE Law, which regulate criminal sanctions of imprisonment and fines for violators.

From the legal construction above, it can be seen that the ITE Law seeks to provide protection against manipulative crimes using digital technology, including phishing. However, a critical examination of the suitability of these normative elements to the characteristics of phishing is necessary.

To determine the effectiveness of the ITE Law against phishing, it is important to analyze how the normative elements of these articles can be applied to forms of phishing crimes. For example:

a. Article 28 paragraph (1) – "Fake and misleading news"

This article is often used as a basis for phishing charges because perpetrators typically spread false information (for example, pretending to be a bank, marketplace, or authority) to deceive victims. However, from a legal perspective, the element of "false and misleading news" requires concrete proof that the information conveyed is completely untrue and results in real harm to the victim.

However, in practice, this proof is not simple. Many phishing cases do not result in direct financial transactions, but rather involve data harvesting, which is then used for other crimes. Therefore, the element of "consumer loss in electronic transactions" in Article 28 paragraph (1) is debatable if the loss is not yet in concrete financial form.

b. Article 30 – Illegal Access

Phishing often involves stealing credentials to access another person's electronic system. When the perpetrator has obtained a username and password from the victim and used them to log into the victim's account, the element of Article 30 is fulfilled: "accessing another person's electronic system without authority." However, many phishing incidents only reach the initial fraudulent stage (social engineering), without the perpetrator directly logging in or accessing the system. In these cases, the application of Article 30 is weakened without evidence that the perpetrator actually accessed the target system.

c. Article 35 – Manipulation of Electronic Information

This article is relevant if phishing is carried out by creating a fake website that mimics the appearance of an official site. This involves "manipulation of electronic information" to appear authentic. In this context, the ITE Law opens up legal enforcement opportunities because phishing contains elements of technical deception. However, the ITE Law does not explicitly mention the term phishing, requiring strong legal construction by investigators and prosecutors to prove that the manipulation was carried out "with the aim of making the data appear authentic."

Meanwhile, another issue is: can inserting fake links into emails or chats (without creating fake websites) be categorized as "electronic information manipulation"? This interpretation requires interpretive courage from law enforcement officials.

Based on literature studies and law enforcement practices, the effectiveness of the ITE Law against phishing still faces various serious obstacles:

a. Law Enforcement Aspects

Despite the existence of legal norms, in practice, gaps in legal implementation remain. Many public reports of phishing go unanswered because investigators lack sufficient digital evidence or because victims don't understand the reporting mechanism. Furthermore, phishing is often conducted across borders, using foreign servers, hindering investigations due to jurisdictional constraints and access to digital data outside national legal jurisdictions.

b. Absence of Explicit Definition

c. One of the main criticisms of the ITE Law is the lack of an explicit definition of "phishing." This contrasts with other countries, such as the United States or the European Union, which include phishing under the category of cyber fraud with specific legal terminology. In Indonesia, law

enforcement officials must "force" the inclusion of phishing into the existing articles of the ITE Law, even though they are not fully compatible in theory. This creates the risk of legal uncertainty and opens the door to significant differences in interpretation.

d. Digital Evidence Problems

Phishing, as a technology-based crime, requires digital forensic evidence. However, in Indonesia, the competence and facilities for digital forensics are still limited outside of large institutions like the Criminal Investigation Agency (Bareskrim) or the National Cyber and Cyber Security Agency (BSSN). Investigators in the regions often lack the expertise or adequate equipment to prove that a phishing site was created and controlled by a specific suspect.

Law Number 1 of 2024, as the latest revision to the ITE Law, adds several new provisions, including:

- Article 27B paragraph (1):

"Any person who intentionally and without authority sends Electronic Information and/or Electronic Documents to someone containing threats or blackmail to obtain personal gain."

This article opens up the opportunity to ensnare phishing if the perpetrator uses a fake email containing threats or coercion to get the victim to hand over an OTP, password, or make a money transfer. However, not all phishing is accompanied by elements of "coercion" or "threats", so its application remains limited. In addition, the wording changes in Article 28 paragraph (1) are now more focused on "consumer losses in electronic transactions", which tends to direct the context of phishing only to economic transactions, even though phishing also occurs outside the economic context, for example to access social media accounts, personal emails, or private data.

In other words, Law No. 1 of 2024 has not addressed the need for a specific legal norm explicitly addressing phishing, nor has it refined the expansion of legal subjects and electronic evidence required in cybercrime proceedings. From these various reviews, it can be concluded that the ITE Law's effectiveness in combating phishing is potentially effective, but in practice, it is not yet optimal. Therefore, the following legal reform measures need to be considered:

- A specific article on phishing should be formulated, including elements of "digital identity fraud," "creation of fake websites," and "collection of personal data without permission." This article should be formulated as a formal offense to facilitate proof and prevent crime from its early stages (preventive).
- Preparation of technical implementing regulations, for example in the form of Government Regulations or Regulations of the Minister of Communication and Information, which explain the phishing reporting mechanism, the authorities authorized to block phishing sites, and the real-time technological intervention mechanism.
- Establishment of integrated cybercrime units at the regional level, with digital forensic facilities and phishing investigation authority, especially for cases not handled centrally.
- Increased international cooperation, especially with global platforms such as Google, Facebook, or international domain providers, to quickly cut off access to phishing sites based on reports from national legal authorities.

IV. CONCLUSIONS AND RECOMMENDATIONS

Based on the above description, it can be concluded that although the ITE Law normatively provides a legal basis for combating phishing crimes, its effectiveness in practice remains limited due to a number of obstacles, such as the lack of an explicit definition of phishing, limited technical capacity of law enforcement officials, difficulties in digital evidence, and suboptimal international cooperation and inter-agency coordination. Therefore, more specific regulatory reforms, increased law enforcement resources and infrastructure, and the establishment of a responsive and integrated phishing handling system are needed so that combating this crime can be more effective and adaptive to technological developments.

REFERENCE LISTAN

Dewantoro, Naufal Mahira, and MH Dian Alan Setiawan SH. 2023. "Law Enforcement of Phishing-Based Cybercrime in the Form of Application Package Kit (APK) Based on the Electronic Information and Transactions Law." In Bandung Conference Series: Law Studies, 3:892–900.

Dhadha, Tegar Pan, Laras Atika Rahayu, Dewi Sito

Resmi, and Dora Kusumastuti. 2021. "The Effectiveness of the Role of the ITE Law in Protecting and Safeguarding All Cyber Activities in Indonesia." Legal Standing: Journal of Legal Studies 6 (1): 40–48.

Indra Utama Tanjung. 2024. BASICS OF LEGAL RESEARCH METHODS. Karanganyar: CV Pustaka Dikara). https://scholar.google.com/citations?view_op=view_citation&hl=id&user=rToGqjUAAAAJ&cstart=20&pagesize=80&citation_for_view=rToGqjUAAAAJ:Wp0gIr-vW9MC.

Majid, Marina Abdul, Zarina Othman, and Muhammad Isa Md Onzer. 2022. "The History, Modus Operandi and Challenges of Combating Drug Smuggling at Langkawi Island with Its Links to the Golden Triangle." Journal of Islamic, Social, Economics and Development 7 (45).

Rianto, Rianto, T Riza Zarzani, and Yasmirah Mandasari Saragih. 2024. "Legal Responsibility of Online Media Corporations and Social Media Users for Broadcasting News Shared to the Public Containing ITE Criminal Acts." JIIP-Jurnal Ilmiah Ilmu Pendidikan 7 (1): 393–98.

Sasuang, Rio Heronimus Kaluara, M Syahrul Borman, and Nur Handayati. 2024. "REVERSE PROOF SYSTEM FOR CORRUPTION CRIMINAL ACTS ACCORDING TO LAW NUMBER 20 OF 2001." COURT REVIEW: Journal of Legal Research (e-ISSN: 2776-1916) 4 (06): 70–78.

Setiawan, M Nanda. 2021. "Criticizing Article 27 Paragraph (3) of the ITE Law from the Socio-Political Perspective of Indonesian Criminal Law." DATIN Law Journal 2 (1): 1–21.

Sidik, Suyanto. 2013. "The Impact of the Electronic Information and Transactions Law (ITE Law) on Legal and Social Changes in Society." Widya Scientific Journal 1 (1): 1–7.

Sutarli, Ananta Fadli, and Shelly Kurniawan. 2023. "The Role of the Government Through the Personal Data Protection Law in Combating Phishing in Indonesia." Innovative: Journal of Social Science Research 3 (2): 4208–21.

Winarno, Wahyu Agus. 2011. "A Study of the Electronic Information and Transactions Law (UU ITE)." Journal of Accounting and Management Economics 10 (1).

Yudistira, Muhammad, and Ramadani Ramadani. 2023. "Legal Review of the Effectiveness of Handling Cybercrimes Related to Personal Data Theft According to Law No. 27 of 2022 by KOMINFO." UNES Law Review 5 (4): 3917–29.