AL FIDDHOH VOL. 4 (2) SEPTEMBER 2023

E-ISSN:2808-7690
P-ISSN:2808-7518

COLLEGE STUDENTS' UNDERSTANDING OF DIGITAL ECONOMIC CRIMES: A STUDY ON PERCEPTIONS AND CHALLENGES IN LAW ENFORCEMENT

Latifa Aulianisya
Institut Agama Islam Negeri Kerinci, Indonesia
Email: Latifa.aulia1501@gmail.com

ABSTRACT

Digital economic crimes pose a significant challenge in the rapidly evolving technological era, particularly for younger generations actively engaged in digital activities. This study aims to explore students' understanding of digital economic crimes, the challenges in law enforcement, and their critiques of existing regulations. The research adopts a qualitative design with a phenomenological approach, involving 10 students from the Faculty of Islamic Economics and Business, majoring in Sharia Financial Management, as informants. Data were collected through semi-structured interviews conducted in two sessions of 20 minutes each. Thematic analysis was employed to identify key themes. The findings reveal that while students are aware of digital risks, such as online fraud and identity theft, their preventive measures remain limited. Informants also identified challenges in law enforcement, including the technological gap between offenders and law enforcement agencies, lack of inter-agency coordination, and inadequate technological training for law enforcement personnel. Moreover, existing regulations, such as the Electronic Information and Transactions Law (UU ITE), are deemed insufficient in addressing the complexities of digital economic crimes. This study highlights the importance of enhancing digital literacy among students, reforming regulations to better adapt to technological advancements, and improving technological capacity and inter-agency coordination in law enforcement to establish a safer digital ecosystem.

Keywords: Digital Economic Crimes, Student Perceptions, Law Enforcement

ABSTRAK

Kejahatan ekonomi digital menjadi tantangan signifikan di era teknologi yang berkembang pesat, khususnya bagi generasi muda yang aktif dalam aktivitas digital. Penelitian ini bertujuan untuk menggali pemahaman mahasiswa terhadap kejahatan ekonomi digital, tantangan dalam penegakan hukum, serta kritik terhadap regulasi yang ada. Penelitian menggunakan desain kualitatif dengan pendekatan fenomenologi, melibatkan 10 mahasiswa Fakultas Ekonomi dan Bisnis Islam pada Program Studi Manajemen Keuangan Syariah sebagai informan. Data dikumpulkan melalui wawancara semi-terstruktur yang dilakukan dalam dua sesi masing-masing berdurasi 20 menit. Analisis data dilakukan menggunakan

metode tematik untuk mengidentifikasi tema-tema utama. Hasil penelitian menunjukkan bahwa meskipun mahasiswa memiliki kesadaran terhadap risiko digital seperti penipuan online dan pencurian data, tindakan preventif yang dilakukan masih terbatas. Informan juga mengidentifikasi tantangan dalam penegakan hukum, seperti kesenjangan teknologi antara pelaku kejahatan dan aparat penegak hukum, kurangnya koordinasi antar-lembaga, serta minimnya pelatihan teknologi bagi aparat. Selain itu, regulasi yang ada, seperti UU ITE, dinilai belum cukup efektif dalam menangani kasus kejahatan ekonomi digital yang kompleks. Penelitian ini memiliki implikasi penting, yaitu perlunya penguatan literasi digital di kalangan mahasiswa, reformasi regulasi yang lebih adaptif terhadap perkembangan teknologi, serta peningkatan kapasitas teknologi dan koordinasi antar-lembaga penegak hukum untuk menciptakan ekosistem digital yang lebih aman.

Kata kunci: Kejahatan Ekonomi Digital, Persepsi Mahasiswa, Penegakan Hukum

1. INTRODUCTION

The development of information technology has brought numerous conveniences and new opportunities across various sectors, particularly in the economic sphere. Digitalization has made transaction processes faster, more efficient, and accessible to a wider audience (Atkinson & McKay, 2011). Thanks to these advancements, innovations such as e-commerce, digital payment systems, and online banking have significantly contributed to global economic growth. However, alongside these advancements lies the darker side of technology: the rise of digital economic crimes, which have become one of the most significant challenges in the modern era (Clarke, 2019).

Digital economic crimes, also known as cyber financial crimes, involve illegal activities utilizing information technology for economic gain. These crimes encompass a wide range of offenses, including online fraud, identity theft, technology-based money laundering, and digital transaction data manipulation (Holt, Bossler, & Seigfried-Spellar, 2015). These crimes are not confined to local jurisdictions but often transcend national borders, complicating investigations and law enforcement efforts.

Online fraud is among the most prevalent forms of digital economic crime. It involves manipulative tactics such as phishing, fraudulent offers through e-commerce, or investment scams conducted on digital platforms (Cross, 2015). Identifying these schemes is often difficult because perpetrators use anonymous identities or untraceable IP addresses. Similarly, identity theft has become a serious threat in the digital era. Criminals often steal personal data, such as credit card numbers, identification documents, or bank account details, to impersonate victims and carry out illegal transactions. These crimes result in substantial financial and psychological harm, as victims not only lose assets but also face difficulties in recovering their stolen identities (Nokhbeh Zaeem, Manoharan, Yang, & Barber, 2017).

Technology-based money laundering is another phenomenon leveraging the complexities of digital financial systems (Tang & Ai, 2016). Criminals often use methods such as cryptocurrency to obscure the origins of illicit funds. Although blockchain technology offers significant benefits for transaction security, its untraceable nature is frequently exploited for illegal activities. Meanwhile, digital transaction data manipulation involves hacking or using unauthorized software to alter, conceal, or falsify financial data within a system. This crime often targets financial institutions like banks or large corporations reliant on information technology to manage their transactions (Demetis, 2009).

The effects of digital economic crimes are widespread. On an individual level, victims often suffer financial losses, psychological stress, and diminished trust in technological systems. For organizations, these crimes can result in substantial material and reputational damages. For instance, customer data breaches caused by hacking can harm a company's credibility and erode consumer trust. On a national scale, digital economic crimes can destabilize economies. These crimes often involve significant financial sums that disrupt the formal financial system. For example, money laundering not only diverts funds from legitimate channels but also influences market dynamics. Furthermore, large-scale fraud can undermine investor confidence, thereby hindering economic growth (Kshetri, 2010; Yang, 2025).

In Indonesia, this issue has become increasingly critical with the rising adoption of information technology across various societal levels. A report by the National Cyber and Crypto Agency (BSSN) highlights a significant increase in cybercrime, including digital economic crimes, over recent years (Cloramidine & Badaruddin, 2023). Unfortunately, law enforcement responses remain inadequate to address the complexities of these crimes. Many cases remain unresolved due to limited technological resources within law enforcement agencies, while perpetrators often use advanced technologies to protect their identities.

Students, as a technology-savvy younger generation, are an important group to study concerning their understanding of digital economic crimes. Their understanding reflects not only their awareness of the risks associated with these crimes but also provides insights into how they perceive the effectiveness of current law enforcement efforts. This research is particularly relevant because students often become either targets or potential perpetrators of digital economic crimes due to their high levels of online activity (Tang & Ai, 2016).

Academically, investigating students' perceptions of digital economic crimes is essential as it reflects their level of legal and technological literacy. Such literacy is vital for building a society that is responsive to the risks of the digital world. Moreover, students who

understand the legal consequences and societal impacts of digital economic crimes can serve as agents of change within their communities. Although students tend to have critical views of legal issues, many lack a comprehensive understanding of the technical aspects of digital crimes (Saputra, Romdony, & Hafizah, 2024).

Globally, addressing digital economic crimes involves three major challenges: (1) weaknesses in regulatory frameworks, (2) low public awareness, and (3) limited technological resources within law enforcement agencies (Reurink, 2018). Indonesia is no exception. While the government has implemented measures such as the Electronic Information and Transactions Law (UU ITE), its enforcement remains far from ideal. This issue is exacerbated by insufficient synergy among government institutions, law enforcement, and society in tackling digital crime cases.

Previous studies on digital economic crimes have largely focused on technical aspects, such as operational mechanisms and crime patterns (Leukfeldt, Lavorgna, & Kleemans, 2017). However, little research has examined students' perceptions of these issues, particularly in Indonesia. Understanding students' perspectives can provide broader insights into how younger generations identify digital threats and support law enforcement efforts. This study seeks to answer fundamental questions: How do students understand the concept of digital economic crimes? To what extent do they evaluate the effectiveness of existing laws in addressing these crimes? What challenges do they perceive in law enforcement efforts? By answering these questions, this research aims to contribute significantly to the development of strategies that enhance students' legal literacy in the digital era and strengthen law enforcement responses. This research is crucial because students represent the nation's future and will inevitably face increasingly complex challenges in the digital world. Without a solid understanding of the risks and legal implications of digital economic crimes, they risk becoming victims or perpetrators themselves. Therefore, this study is not only relevant in an academic context but also in supporting public policies that foster legal and technological literacy.

2. LITERATURE REVIEW

This literature review focuses on three main aspects that form the foundation of the study: awareness of digital risks, challenges in law enforcement for combating digital economic crimes, and existing regulations addressing such crimes.

a. Awareness of Digital Risks

Awareness of digital risks is a crucial aspect in preventing digital economic crimes. Browning and Arrigo (2021) observed that although public awareness of digital threats has

increased, the implementation of preventive measures remains significantly lacking. This is evident in behaviors such as using weak passwords, sharing personal information on social media, and failing to utilize security features like two-factor authentication.

According to Holt, Bossler, and Seigfried-Spellar (2015), personal and social experiences play a vital role in shaping vigilance against digital risks. Individuals who have direct experiences or know victims of cybercrimes tend to exercise greater caution in their digital activities. Educational strategies based on real-life experiences have proven effective in enhancing public awareness of digital threats (Susetyo & Firmansyah, 2023).

b. Challenges in Law Enforcement

Digital economic crimes often involve advanced technologies that are difficult for law enforcement agencies to trace. Reurink (2018) highlighted that digital crimes, such as blockchain-based money laundering, present significant challenges due to their anonymous and hard-to-access nature. Law enforcement often lags behind in understanding the latest technologies, creating gaps that criminals exploit.

The lack of technological training for law enforcement personnel is a key issue highlighted by Holt and Bossler (2015). Law enforcement officials without sufficient technical expertise struggle to address increasingly complex crimes. Investing in technological training and developing digital infrastructure within law enforcement agencies is urgently needed to enhance the effectiveness of handling digital economic crime cases (Dinda, 2024).

c. Regulations for Combating Digital Economic Crimes

Existing regulations, such as the Electronic Information and Transactions Law (UU ITE), are often considered insufficient in addressing the complexities of digital economic crimes. Manurung and Heliany (2019) noted that the UU ITE is frequently applied to minor cases, such as defamation, rather than more serious cases like online fraud or digital money laundering. Moreover, regulations related to emerging technologies like cryptocurrencies remain limited, creating legal loopholes often exploited by criminals (Reurink, 2018).

The flexibility of regulations is another critical concern. Simbolon, Kesuma, and Wibowo (2021) emphasized the importance of periodic updates to regulations to ensure their relevance to rapidly evolving technologies. Responsive and specific regulations tailored to the demands of the digital era can help close legal gaps and strengthen law enforcement efforts.

3. METHOD

This study adopts a qualitative approach with a phenomenological design, aiming to deeply understand the experiences and perceptions of students regarding digital economic crimes. The phenomenological method allows the researcher to explore the subjective meanings of informants' experiences, which cannot be quantified (Creswell, 2014). Primary data were collected through semi-structured interviews conducted in two sessions of 20 minutes each. These interviews focused on students' understanding of digital economic crimes, the challenges they identified in law enforcement, and their views on the effectiveness of existing laws in addressing these issues.

The study involved 10 students from the Faculty of Islamic Economics and Business, majoring in Sharia Financial Management, selected through purposive sampling. Selection criteria included active engagement in digital activities and baseline knowledge of legal concepts. Data were analyzed using thematic analysis to extract key themes from the interview transcripts. The process involved transcription, coding, identifying themes, and generating thematic reports. Themes such as "awareness of digital risks," "challenges in law enforcement," and "criticism of existing regulations" were revisited for accuracy and alignment with the raw data. The analysis emphasized in-depth interpretations supported by direct quotes from informants to enhance validity.

Data credibility was ensured through triangulation, member checking, and prolonged engagement with the informants. Transferability was achieved by providing a detailed description of the research context, while dependability and confirmability were strengthened through a documented audit trail, ensuring that findings are grounded in the original data.

4. RESULTS AND DISCUSSION

This study identified three main themes reflecting students' understanding of digital economic crimes: awareness of digital risks, challenges in law enforcement, and criticisms of existing regulations. The findings are based on interviews conducted with 10 informants.

a. Awareness of Digital Risks

The majority of informants demonstrated a basic awareness of digital risks, particularly those related to digital economic crimes such as online fraud, identity theft, and the misuse of financial information. They understood that activities like online shopping, using banking applications, or sharing personal information on social media increase the risk of becoming victims of digital crimes. However, their understanding of the specific mechanisms behind these crimes varied.

For example, one informant noted:

"I know there are risks like online fraud, especially when shopping on untrusted sites, but I don't know much about identifying more complex scams." (Informant 1, 21 years old).

This indicates that while general awareness of the dangers exists, not all students possess an in-depth understanding needed to identify specific crimes. Conversely, some informants displayed a more advanced understanding and implemented preventive measures.

"I always check the security of a website before entering my credit card information and avoid sharing sensitive information on social media," stated Informant 4 (22 years old).

This informant also emphasized the importance of two-factor authentication in securing their digital accounts. However, other informants exhibited behaviors that left them vulnerable to risks.

"I rarely change my passwords or check the security of my accounts because it feels tedious. Sometimes I use the same password for all accounts to make it easier," said Informant 7 (20 years old).

These responses highlight that while awareness is growing, the implementation of digital security measures remains suboptimal among students. Awareness is also influenced by personal experiences or those within their social environment. For instance, Informant 3 became more cautious after learning that a friend had fallen victim to online fraud:

"After finding out my friend was scammed through e-commerce, I've become more careful when shopping online, especially when discounts seem too good to be true." (Informant 3, 21 years old).

These findings suggest that direct or indirect experiences play a crucial role in increasing awareness of digital risks.

b. Challenges in Law Enforcement

The informants perceived that law enforcement in Indonesia is still far from effective in combating digital economic crimes. One major challenge identified is the technological gap between offenders and law enforcement agencies. Digital criminals often use advanced technology, whereas law enforcement agencies still rely on conventional methods.

"Digital criminals now use technology that's hard to trace, while our police don't have advanced tools to pursue them," explained Informant 6 (22 years old).

Another added :

> *"Money laundering cases or fraud involving cryptocurrency often remain unresolved due to the lack of tools capable of tracking such transactions."* (Informant 8, 21 years old).

Additionally, the lack of coordination among agencies was highlighted as a significant barrier. Informant 9 criticized the lack of synergy between law enforcement, the government, and digital service providers:

> *"Sometimes cases require cooperation with tech companies, but the process is slow due to lengthy bureaucracy."* (Informant 9, 23 years old).

This inefficiency often allows perpetrators sufficient time to cover their tracks. The shortage of trained personnel in technological fields also emerged as a concern :

> *"I think law enforcement officers need better training to understand new technologies because digital crime evolves so quickly,"* suggested Informant 10 (23 years old).

Another informant stressed the importance of establishing more digital forensic labs to facilitate investigations.

c. Criticisms of Existing Regulations

The informants provided critical perspectives on current regulations, particularly the Electronic Information and Transactions Law (UU ITE). While UU ITE is seen as a good starting point, many informants felt that its implementation remains insufficient to address the growing complexities of digital economic crimes.

> *“UU ITE is often used to address minor issues like social media conflicts, while major crimes like digital money laundering or online fraud rarely seem to be successfully prosecuted,”* noted Informant 2 (22 years old).

Another informant pointed out gaps in the regulation of cryptocurrencies:

> *"Many illegal crypto transactions slip through because our laws aren’t clear enough on this. Criminals exploit these gaps to launder money."* (Informant 5, 21 years old).

The lack of protection for victims of digital economic crimes was also criticized :

> *"Victims often don't receive enough attention from law enforcement. The focus is more on catching the perpetrators than on recovering the victims' losses,"* observed Informant 3 (21 years old).

This reinforces the view that regulations should target not only the perpetrators but also provide recovery and protection mechanisms for victims. Some informants proposed updating regulations to better address the challenges of the digital era :

> *"Current regulations aren't flexible enough to keep up with technological developments. The government needs to continuously update these rules to ensure they remain relevant,"* emphasized Informant 7 (20 years old).

The findings of this study reveal three main themes: awareness of digital risks, challenges in law enforcement, and criticisms of existing regulations. These themes highlight significant gaps in digital literacy, law enforcement capacity, and regulatory frameworks in addressing digital economic crimes. The findings align with previous studies and underscore the need for comprehensive strategies to address these challenges effectively in the digital era.

The students' awareness of digital risks reflects a fundamental understanding of potential threats, such as online fraud, identity theft, and the misuse of financial information. However, this knowledge has not been accompanied by adequate preventive actions. Some students admitted to using the same password for multiple accounts or failing to utilize security features such as two-factor authentication. These findings are consistent with previous research by Browning and Arrigo, which found that despite increasing public awareness of cybersecurity risks, the implementation of digital security measures remains insufficient (Browning & Arrigo, 2021; Chibuye, Phiri, & Lampi, 2023).

Additionally, direct or indirect experiences play a crucial role in raising awareness. Students with friends or family members who have been victims of online fraud tend to be more cautious in their digital activities. This observation aligns with the research of Holt and Bossler, who found that personal or social experiences significantly influence individuals' vigilance toward digital threats (Holt et al., 2015). Therefore, digital literacy programs incorporating real-life scenarios can be an effective strategy for improving students' awareness of digital risks (Susetyo & Firmansyah, 2023).

The primary challenge identified by students in law enforcement is the technological gap between criminals and law enforcement agencies. Students perceive that digital criminals

often use advanced technologies that are difficult to trace, while law enforcement agencies still rely on conventional methods. Reurink's research similarly noted that digital economic crimes often involve cutting-edge technologies, such as blockchain, which are challenging for law enforcement to access or understand (Reurink, 2018).

The lack of technologically skilled personnel within law enforcement agencies was also a significant concern. Officers who lack a deep understanding of technology face difficulties in addressing increasingly complex crimes. Holt and Bossler emphasized the importance of technological training for law enforcement personnel to enhance their capabilities in tackling digital challenges (Holt et al., 2015). Investments in education and technology training for law enforcement are thus urgently needed to bridge this gap (Dinda, 2024).

Students in this study provided critical insights into existing regulations, particularly the Electronic Information and Transactions Law (UU ITE), which they viewed as ineffective in addressing digital economic crimes. Many students felt that UU ITE is more often used for minor cases, such as defamation, than for serious issues like online fraud or digital money laundering. Similar criticisms were echoed in a previous study, which found that the implementation of UU ITE is often disproportionate and more focused on social activities than on economic crimes (Manurung & Heliany, 2019).

Students also highlighted the lack of regulations relevant to emerging technologies like cryptocurrencies. Reurink pointed out that slow regulatory development creates legal loopholes often exploited by criminals (Reurink, 2018). Additionally, existing regulations are perceived as insufficiently flexible to keep pace with rapid technological advancements. Regular updates to these laws are necessary to ensure their relevance to evolving digital threats. Regulatory reforms in Indonesia are crucial to creating a legal framework that is more responsive to the challenges of the digital era (Simbolon, Kesuma, & Wibowo, 2021).

This study has several limitations, including the small and homogeneous sample size of 10 students from the same program, which restricts the generalizability of the findings. The relatively short duration of the interviews—two sessions of 20 minutes each—may have limited the depth of exploration into the informants' perceptions. Additionally, the data relied on self-reports, which are subject to social desirability bias, while perspectives from other stakeholders, such as faculty members, law enforcement officials, or technology experts, were not included. Lastly, the rapid development of technology poses a challenge, as the findings may not fully reflect the current state of digital economic crimes.

5. CONCLUSION

The study reveals that although students are aware of the digital risks associated with digital economic crimes, their preventive measures remain limited. Additionally, challenges in law enforcement, such as technological gaps, lack of inter-agency coordination, and insufficient training for law enforcement personnel, pose significant obstacles to addressing these crimes effectively. Criticisms of existing regulations, particularly the Electronic Information and Transactions Law (UU ITE), highlight the urgent need for policy reforms that are more adaptive to technological advancements. These findings offer valuable insights into how students, as part of the digital generation, perceive risks and challenges in the digital economy era.

The results of this study have implications for various stakeholders. Educational institutions need to enhance digital literacy through educational programs that not only raise awareness but also develop practical skills to safeguard against digital threats. For policymakers, regulatory reforms that are more specific and responsive to technological developments should be a priority to close the legal loopholes often exploited by criminals. Meanwhile, law enforcement agencies must invest in training and technological infrastructure to bridge the capability gap with digital crime perpetrators. With synergy between education, policy, and law enforcement, a safer and more equitable digital ecosystem can be achieved.

REFERENCES

Atkinson, R. D., & McKay, A. S. (2011). Digital Prosperity: Understanding the Economic Benefits of the Information Technology Revolution. *SSRN Electronic Journal*, (March). doi: 10.2139/ssrn.1004516

Browning, M., & Arrigo, B. (2021). Stop and Risk: Policing, Data, and the Digital Age of Discrimination. *American Journal of Criminal Justice*, *46*(2), 298–316. doi: 10.1007/s12103-020-09557-x

Chibuye, M., Phiri, J., & Lampi, E. (2023). he Readiness, Risks and Mitigation Measures of Quantum Supremacy to Current Digital Security Measures and Infrastructure. *Proceedings of International …*, 153–158. Retrieved from https://ictjournal.icict.org.zm/index.php/icict/article/view/294%0Ahttps://ictjournal.icict.org.zm/index.php/icict/article/download/294/148

Clarke, R. (2019). Risks inherent in the digital surveillance economy: A research agenda. *Journal of Information Technology*, *34*(1), 59–80. doi: 10.1177/0268396218815559

Cloramidine, F., & Badaruddin, M. (2023). Mengukur Keamanan Siber Indonesia Melalui Indikator Pilar Kerjasama Dalam Global Cybersecurity Index (GCI). *Populis : Jurnal Sosial Dan Humaniora*, *8*(1), 57–73. doi: 10.47313/pjsh.v8i1.1957

Creswell, J. . (2014). *Research Design: Qualitative, Quantitative and Mixed Methods Approaches (4th ed.)*. Thousand Oaks, CA: SAGE Publications. Retrieved from https://edge.sagepub.com/creswellrd6e

Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology*, *21*(2), 187–204. doi: 10.1177/0269758015571471

Demetis, D. S. (2009). Data growth, the new order of information manipulation and consequences for the AML/ATF domains. *Journal of Money Laundering Control*, *12*(4), 353–370. doi: 10.1108/13685200910996056

Dinda, A. L. S. (2024). Efektivitas Penegakan Hukum Terhadap Kejahatan Siber di Indonesia. *AL-DALIL: Jurnal Ilmu Sosial, Politik, Dan Hukum /*, *2*(2).

Holt, T., Bossler, A., & Seigfried-Spellar, K. (2015). *Cybercrime and Digital Forensics: An Introduction*. London: Routledge. doi: 10.4324/9781315296975

Kshetri, N. (2010). Diffusion and Effects of Cyber-Crime in Developing Economies. *Third World Quarterly*, *31*(7), 1057–1079. doi: 10.1080/01436597.2010.518752

Leukfeldt, E. R., Lavorgna, A., & Kleemans, E. R. (2017). Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime. *European Journal on Criminal Policy and Research*, *23*(3), 287–300. doi: 10.1007/s10610-016-9332-z

Manurung, E. H., & Heliany, I. (2019). Peran Hukum Dan Tantangan Penegak Hukum Dalam Menghadapi Era Revolusi Industri 4.0. *Jurnal Penelitian Hukum*, *1*(2), 128–135.

Nokhbeh Zaeem, R., Manoharan, M., Yang, Y., & Barber, K. S. (2017). Modeling and analysis of identity threat behaviors through text mining of identity theft stories. *Computers & Security*, *65*, 50–63. doi: https://doi.org/10.1016/j.cose.2016.11.002

Reurink, A. (2018). Financial Fraud: A Literature Review. *Journal of Economic Surveys*, *32*(5), 1292–1325. doi: https://doi.org/10.1111/joes.12294

Saputra, A. E., Romdony, M., & Hafizah, A. (2024). Pandangan Mahasiswa Mahasiswi IAIN Terhadap Negara Hukum Dan Penegakan Hukum Di Indonesia. *JURNAL HUKUM, POLITIK DAN ILMU SOSIAL*, *3*(3).

Simbolon, M. M., Kesuma, I. G. K. W., & Wibowo, A. E. (2021). Kejahatan Siber pada Penyelenggaraan Perdagangan Berbasis Sistem Elektronik Dalam langkah Pengamanan Pertumbuhan Ekonomi Digital Indonesia. *Defendonesia*, *5*(1), 1–12. doi: 10.54755/defendonesia.v5i1.98

Susetyo, D. P., & Firmansyah, D. (2023). Literasi Ekonomi, Literasi Keuangan, Literasi Digital dan Perilaku Keuangan di Era Ekonomi Digital. *Economics and Digital Business Review*, *4*(1), 261–279.

Tang, J., & Ai, L. (2016). New Technologies and Money Laundering Vulnerabilities. In M. Dion, D. Weisstub, & J.-L. Richet (Eds.), *Financial Crimes: Psychological, Technological, and Ethical Issues* (pp. 349–370). Cham: Springer International Publishing. doi: 10.1007/978-3-319-32419-7_17

Yang, Y. (2025). The development of digital finance and the crime rate of theft. *Finance Research Letters*, *71*, 106422. doi: https://doi.org/10.1016/j.frl.2024.106422