DIGITAL DECEPTION: EXPLORING VULNERABILITIES AND THE ROLE OF REGULATION IN COMBATING ONLINE FRAUD

Rudi Pardede *, Surizki Febrianto **

* *Corresponding author,* Faculty of Law, Universitas Lancang Kuning, Pekanbaru, Indonesia
Contact details: Faculty of Law, Universitas Lancang Kuning, Jl. Yos Sudarso Km. 8, Rumbai, Pekanbaru 28265, Riau, Indonesia
** Faculty of Law, Universitas Islam Riau, Pekanbaru, Indonesia

OPEN ACCESS

How to cite this paper: Pardede, R., & Febrianto, S. (2026). Digital deception: Exploring vulnerabilities and the role of regulation in combating online fraud. *Corporate Law & Governance Review, 8*(2), 20–28. https://doi.org/10.22495/clgrv8i2p2

ISSN Online: 2664-1542
ISSN Print: 2707-1111

Received: 29.07.2025
Revised: 25.10.2025; 19.11.2025; 05.02.2026
Accepted: 03.03.2026

JEL Classification: K42, L86, O33
DOI: 10.22495/clgrv8i2p2

Abstract

This study aims to measure the content of e-commerce regulations in overcoming the problem of digital trade transaction crimes. This research contributes to identifying the potential for cross-border digital trade crimes from a legal aspect. This study uses a qualitative analysis method. The content analysis approach is used to trace the substance of regulations governing e-commerce so that it can explicitly recommend regulations that are relevant to potential problems for the future (Han et al., 2022). The previous study approach was also used to support exploring the research discussion (Jansen et al., 2021). The study results indicate that the current regulations have not fully overcome the problems arising from e-commerce, such as data protection crimes and fraudulent goods not of the original. This study concludes that existing regulations must be discussed and evaluated by including clauses on the potential for cross-border digital trade crimes. Future regulations must touch on the artificial intelligence (AI) space, as it has been widely adopted by online platforms such as e-commerce. Although this study has revealed the limitations of e-commerce regulations, further research is important to discuss the supporting infrastructure for e-commerce activities, further facilitated by the state and equipped with an established legal foundation.

Keywords: Digital Crime, Digital, Online Fraud, Law, Regulation

Authors' individual contribution: Conceptualization — R.P.; Methodology — R.P.; Software — S.F.; Validation — R.P. and S.F.; Formal Analysis — R.P.; Investigation — R.P.; Resources — R.P. and S.F.; Data Curation — S.F.; Writing — Original Draft — R.P.; Writing — Review & Editing — S.F.; Visualization — S.F.; Supervision — R.P.; Project Administration — R.P. and S.F.; Funding Acquisition — R.P. and S.F.

Declaration of conflicting interests: The Authors declare that there is no conflict of interest.

Acknowledgements: The Authors thank Universitas Lancang Kuning for providing support to the research team.

1. INTRODUCTION

The development of digital technology can change every aspect of daily life, starting from aspects of communication, trade, education, and governance. During the advancement of digital technology, negative phenomena such as digital crime have emerged (Al Zaidy, 2024). Digital crime is a cybercrime involving various legal activities that use digital technology, such as hacking, identity

theft, and online fraud, as well as distributing hazardous software links (Peersman et al., 2022). The expansion of internet access in Indonesia has had significant positive and negative impacts. Businesses, government institutions, and individuals depend on digital platforms. The threat of digital crime from domestic and international online criminals is increasing. Digital crime is a serious challenge faced by society and the government. A sharp increase in cyber threats along with the digital transformation occurring in Indonesia (Wulandari et al., 2025). Indonesia will reach more than 210 million users in 2024 in terms of internet penetration (Muzakki & Suraji, 2024). The rapid growth of digital usage opens up new opportunities for cybercriminals. Digital crime activities with the criteria of online fraud, phishing attacks, ransomware, data breaches, and financial fraud target banks, government institutions, and e-commerce platforms (Metibemu, 2025).

Several studies on digital crime show that Indonesia is a preferred target for cyberattacks in Southeast Asia (Wibiwo et al., 2025). In 2023, Indonesia experienced a cyberattack, highlighting the urgent need for more comprehensive cyber risk mitigation (Ramadhani et al., 2025). The most common threats are malware distribution, defence attacks on government websites, and online financial fraud (Acharya & Joshi, 2020). The Indonesian Senate responded to digital crime by implementing the Electronic Information and Transactions Law (UU ITE). In substance, the law criminalizes various forms of cyber violations.

Regarding technology, using artificial intelligence (AI), threat intelligence platforms, and blockchain as source security monitors and digital forensics can help in digital crime. However, Indonesia is still not significantly utilising this sophistication. The 2024 Government AI Readiness Index report indicates that Indonesia's Technology Sector score is 48.06, suggesting that AI adoption is not yet significant (Nettel et al., 2024), and in addition to the limitations of inadequate cybersecurity infrastructure (Kipngetich, 2025). Digital literacy for modern society is still relatively limited, and public awareness is also still low regarding cybersecurity (Isabella et al., 2024). The government's initiative to educate internet users has increased, but has not yet reached the village level. Indonesia has made efforts to eradicate digital crime by designing a strict legal framework and developing institutions, but there are still gaps in adopting technology, law enforcement capacity, and public awareness of digital crime (Hidayat et al., 2025). So, to bridge the gap, a multidimensional approach needs to involve government policies, collaboration with the private sector, significant technology investments, and public education. This study aims to explore the current trends in digital crime in Indonesia, analyze the factors contributing to the increase in digital crime, and evaluate the effectiveness of existing legal and technological responses. By examining current case studies, national cybercrime statistics, and government policies, this study seeks to identify challenges and potential solutions to overcoming the threat of digital crime. Understanding the dynamics of digital crime is essential to developing a comprehensive national strategy that ensures digital security and encourages technological growth and public trust in a friendly digital ecosystem.

This research is structured as follows. Section 1 provides an introduction to the issue of digital crime and the challenges currently facing the government. Section 2 provides a literature review to strengthen the discussion of digital crime issues and the regulations adopted by developing countries to address environmental crimes. Section 3 involves research methods, which determine the analytical approach and data usage. Section 4 presents the results, presenting the data and explaining the research findings. Section 5 discusses the development of digital crime and the preventive measures the government must take to reduce the number of online fraud reports. Section 6 concludes the overall research and provides recommendations for further research.

2. LITERATURE REVIEW

Digital crime has become a global issue, entering developing countries such as Indonesia, which are facing unique problems due to rapid technological growth. However, cybersecurity readiness is not yet evenly distributed. Several studies analyze patterns, causes, and solutions to cybercrime problems.

2.1. Trends in digital crime in Indonesia

Digital crime in Indonesia has increased significantly, which is in line with the rapid growth in the use of the internet and digital services. Data from the National Cyber and Crypto Agency shows that over 1.6 billion cyberattacks have occurred in the malware, phishing, ransomware, and government website defacement sectors (Hutapea & Talita, 2021). The figure of 1.6 billion reflects the increase in the volume and complexity of threats caused by individual actors and organized groups. Several sectors, such as banking, e-commerce, and public services, are the primary targets of cyberattacks (Tn & Shailendra Kulkarni, 2023). Digital crimes that often occur in Indonesia include financial and e-commerce fraud. Phishing cases have increased, leading to mobile banking and digital wallets through fake sites and text messages (Astika et al., 2024). Other sectors, such as online shopping platforms, are often the target of fraud; individuals offer fictitious products or do not send products after successful payment (Rinaldy et al., 2025). Digital crime is influenced by low digital literacy in the new digital service user community. Several digital services, such as social media, Facebook, Instagram, and WhatsApp, are channels individuals use to spread digital crime (Daguatha, 2022). The spread of hoaxes, defamation, online bullying, and identity theft increasingly occurs through online platforms (Syafruddin et al., 2024). Young people who are still minimally aware of cybersecurity risks are the targets of social media crimes (Collier & Morton, 2024). Further attention is paid to digital crimes such as ransomware cases and data leaks. Several government agencies and universities have experienced cyberattacks resulting in operational disruptions and data loss (Wibowo et al., 2025). The loss of institutional and personal data is due to weak data protection and digital security

infrastructure. The involvement of cross-border cybercrime networks is also a trend in digital crime modes. Several digital crimes that occur in Indonesia are collaborations with international syndicates, due to the opportunities for weak law enforcement and the high number of internet users (Aziz & Daryanto, 2025). Dark web activities, the use of cryptocurrency for money laundering, and digital black markets are part of an increasingly complex digital crime ecosystem (Gjorgjev et al., 2025).

2.2. Legal and policy responses

The Indonesian government has responded to the surge in digital crime with various legal instruments and national policies. Law Number 11 of 2008 concerning information and electronic transactions is the legal basis for dealing with digital crime. Furthermore, the regulation was revised to become Law Number 19 of 2016. In substance, the Indonesian legal framework covers various violations, such as the distribution of illegal content, defamation, and illegal access to electronic systems. Criticism of Indonesia's Law on Electronic Information and Transactions (ITE Law) states that several clauses are subject to multiple interpretations, are prone to misuse, and are not yet strong enough to answer the complexity of modern cybercrime as a whole (Rusman & Kamaludin, 2024). There are still weaknesses in implementing the ITE Law, such as law enforcement and the uncertainty of law enforcement officers in dealing with digital cases at the technical level (Syahril & Aris, 2024). The technical capacity and digital forensic infrastructure are inadequate when resolving digital crimes (Syalendro et al., 2025). Indonesia's strategy for overcoming cyber threats is to establish the National Cyber and Crypto Agency as a government organization that acts as a national cybersecurity coordination centre. Special tasks are given to BSSN, such as detecting and responding to cyber incidents and fostering cross-sector cooperation to increase national digital resilience (Dwiaji et al., 2024). The agenda for formulating a national cybersecurity strategy is one of the important agendas in strengthening Indonesia's digital defence system (Wibowo et al., 2024). In terms of human resources, funding, low participation of the private sector, and the community are still significant obstacles for the BSSN Institution in handling digital crime cases (Roz et al., 2025). Indonesia's aggressive policies have not been fully implemented due to institutional readiness, user awareness, and integration into the national digital system.

2.3. Technological and educational solutions

Along with the high threat of digital crime, the Indonesian government faces challenges when developing and implementing effective technological solutions that prevent, detect, and deal with cyberattacks. Some innovations, such as using AI and Big Data analysis systems to detect cyber threats early (Katiyar et al., 2024). AI-based technology can be used to detect suspicious behaviour patterns during digital transactions (Wali & Sivathapandi, 2025). However, the sophistication of AI technology still finds obstacles to integration with existing infrastructure and limitations in established human resources in managing AI systems (Sandeep et al., 2025). Utilizing blockchain is one of the efforts to secure digital transactions and track various online activities used in several sectors in Indonesia (Arif et al., 2024; Hermanto et al., 2025). Blockchain technology offers reliability in providing transparent records of every transaction that is difficult to change, thus increasing security in e-commerce and financial transactions (George et al., 2024).

Education and digital literacy society's preventive seduce society's vulnerability to digital crime. Efforts to increase digital literacy among the community and students can reduce the success rate of online fraud, phishing, and misuse of personal data (Arsyad et al., 2024). Training programs focusing on cybersecurity, such as recognizing phishing emails or maintaining the confidentiality of personal data, need to be started in the elementary and secondary curriculum (Jagadeesan et al., 2023; Marshall et al., 2024). The equalization of the implementation of training programs needs to be evenly distributed to all regions. Increasing cybersecurity awareness is important for companies and government institutions (Odebade & Benkhelifa, 2023). Training for employees and government officials on cybersecurity has a positive impact on reducing data leaks and malware attacks (Adebayo et al., 2025). Some companies have implemented strict security policies, but small and medium-sized businesses do not yet have the resources to implement established security solutions (Dua et al., 2024; Stanchev et al., 2024). The role of the government is vital in facilitating education and training related to digital security (Margarov et al., 2021). Strategic efforts such as the National Digital Literacy Movement initiated by the Ministry of Information were carried out to increase public awareness of the importance of maintaining cybersecurity (Ariansyah et al., 2024).

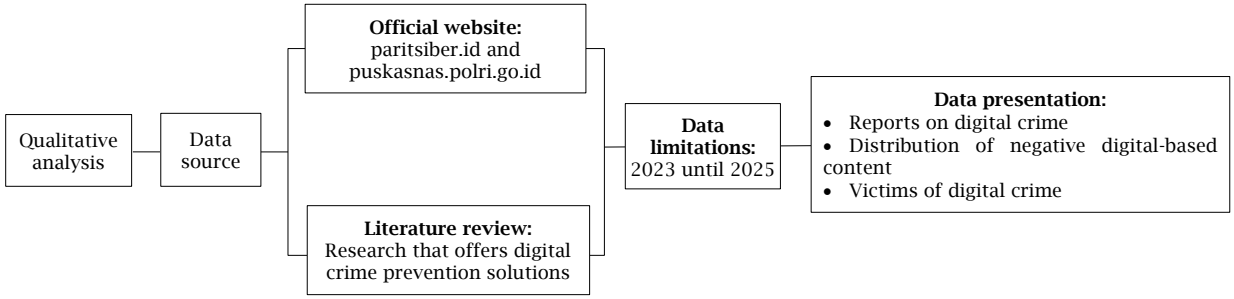
3. METHOD

This study uses qualitative analysis methods as an interpretive approach to understanding social phenomena and human behaviour in the context of digital crime practices (Tomczyk, 2021). By focusing on the meanings behind actions and interactions, this method allows for a deeper exploration of how digital crime occurs and how individuals and institutions respond to it (Rakhmanova & Pinkevich, 2020). The primary data sources in this study include content from official government websites that are widely used by the public to report digital crimes online. Structured metadata from open government data portals can contribute to supporting large-scale research (Amri et al., 2022). These sources provide insight into crime trends, public engagement, and institutional responses. In addition, this study combines findings from previous scientific research relevant to the issue of digital crime. These studies offer scientifically grounded recommendations and solutions that help frame discussions and support formulating effective strategies to address digital crime. This research also provides a relevant alternative approach to addressing digital crime, such as document analysis. Data sources from official documents owned by

institutions handling digital crime can also be mapped, along with recommendations for addressing digital crime.

This study explores various aspects of digital crime, starting with an analysis of digital crime trends across various aspects, including types of crime, technological advancements, and motivations behind the activity. The study will then focus on mapping areas with the distribution of harmful content that often leads to digital crime, such as illegal materials, misinformation, and harmful online behaviour. The study will identify the regions and platforms most vulnerable to this problem. It will examine the number of victims, the types of crimes they face, and the impact on individuals and organizations. Finally, the study will offer solutions to prevent digital crime attacks, including technological measures such as cybersecurity tools and encryption, policy recommendations, and best practices for individuals and businesses to reduce the risk of digital crime. Figure 1 presents the research framework.

Figure 1. Research framework



Source: Authors' elaboration.

Figure 1 explains the research stages. First, the study employed a qualitative analysis approach to gain a deeper understanding of the phenomenon of digital crime. Second, research data came from two categories: the Indonesian government's remission websites[1], which provide empirical data on digital crime reports and trends. The second source came from previous research discussing solutions and the development of digital crime prevention efforts. This study set the data limits used from 2023 to 2025. Furthermore, the collected data is presented in three forms: data on reports related to digital crime, data on the distribution of harmful digital-based content in Indonesia, and information on victims of digital crime.

4. RESULT

4.1. Digital crime trends in various aspects

The problem of digital crime has grown rapidly in recent years, thus having an impact on aspects of society, financial systems, privacy data, corporate security, and national infrastructure. The development of technology and digital platforms has made it increasingly integrated into everyday life. Cybercriminals are constantly making new and increasingly sophisticated efforts to exploit vulnerabilities. Crimes occur in identity theft, ransomware attacks, phishing schemes, and large-scale data breaches. Understanding the shift in digital crime is necessary to develop more effective prevention strategies and strengthen cybersecurity resilience in all sectors.

Table 1. Reports on digital crime

No.	*Types of digital crime*	*Number of reports*
1	Online fraud	14,495
2	Threat of violence	8,614
3	Defamation	6,556
4	Pollution threat	3,675
5	Pornography	952
6	Fake news	778
7	Unauthorized data manipulation	597
8	Provocation/Incitement	499
9	Prostitution	237
10	Online gambling	220
11	Illegal drugs	42
12	Human trafficking	36
13	Trade in protected animals	6

Source: Patroli Siber (2025).

Table 1 data on reports of various types of digital crimes in the Patroli Siber database owned by the Republic of Indonesia Police. Online fraud is the most dominant digital crime reported by the public, with 14,495 reports. Threats of violence in the online world have as many as 8,614 reports. Defamation has a total of 6,556 reports. The two types of digital crimes show that the digital aspect is often used in terms of intimidation and damage to an individual's reputation.

Furthermore, reports of crimes included in the low category, such as protected animal trade practices, as many as six reports; human trafficking, as many as 36 reports; illegal drug crimes, 42 reports. Unauthorized data manipulation crimes, as many as 579 reports, and provocation/incitement, 499 reports. These two types of crimes significantly impact information security and social stability. Reports of crimes containing sensitive content, such as pornography 952 reports, prostitution 237 reports, and online gambling 220 reports show that moral values and social norms are also part of the challenges in the digital era. So that the data presented in Table 1 covers financial, social, legal, and environmental aspects. Integrated Langkat,

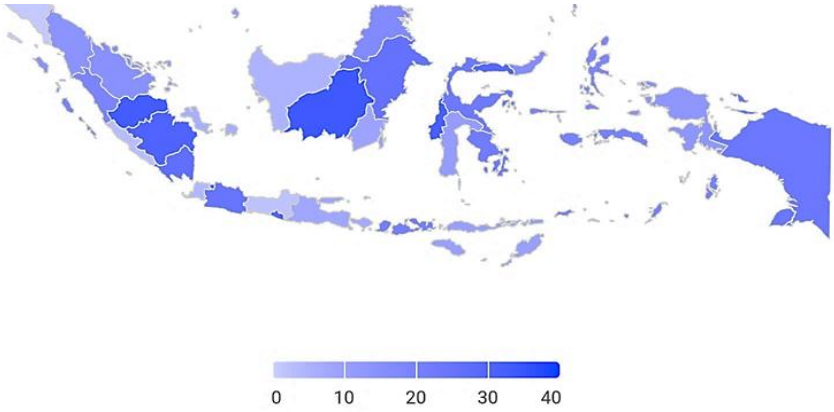
[1] paritsiber.id and puskasnas.polri.go.id

which includes education to the community, is very important in explaining to the public that digital crime is a significant threat. Efforts to improve the reporting system to be faster and more responsive are challenging for the government. Established law enforcement and regulations can overcome various forms of digital crime.

4.2. Mapping of areas with the distribution of negative content leading to digital crime

Mapping the area of the distribution of harmful content that has the potential for digital crime is part of a strategy to identify areas vulnerable to the spread of potentially harmful information, such as hate speech, online fraud, child pornography, and digital radicalism. Through location mapping analysis, the government and related institutions can get a more accurate picture of the distribution of dangerous content in cyberspace. Information on mapping the distribution of harmful content can support formulating policies for law enforcement to strengthen digital literacy in vulnerable areas so that crime prevention and handling strategies can be carried out effectively and on target.

Figure 2. Distribution of negative digital-based content



Source: https://patrolisiber.id/statistic/

Figure 2 explains the map of the distribution of harmful digital-based content in Indonesia. The image above is marked with a gradation of blue, and the darker the colour, the more intense the number of cases of harmful digital content in a region. The map shows several provinces, such as Papua, Central Kalimantan, and Sulawesi, showing a higher level of negative content distribution with a darker blue colour. At the same time, provinces such as East Java, Bali, and Sumatra have a lower intensity with a lighter blue colour. Several provinces with high intensity of negative content distribution have the potential for low digital literacy, low supervision of online activities, and limited infrastructure regarding information technology. Provinces with lower intensity have the potential for better digital education levels and more intense supervision. The purpose of this mapping is beneficial in strategic references for the government and institutions in determining regional priorities in digital literacy programs, educating the public, and strengthening regulations and law enforcement to suppress the growth of digital crime.

4.3. Digital crime victim report trends 2023–2025

The rapid development of digital technology has caused cybersecurity to become an important issue that is difficult to control. Reports on digital crime by the community are important to discuss to see the increase or decrease in digital crime. The following is Table 2 on the number of victims of digital crime.

Table 2. Victims of digital crime

No.	*Year*	*Total crime victims*	*Woman*	*Man*
1	2023	9,561	5,020	3,484
2	2024	11,938	6,145	4,670
3	2025	6,226	3,180	2,551

Source: Pusiknas.polri.go.id, 2025.

Table 2 shows data on the fluctuation in the number of victims of digital crime during the period 2023–2025. Starting in 2023, 9,561 people were recorded as victims. Furthermore, there was a significant increase in 2024, with the number of victims being 11,938 people. In 2025, data was found to have decreased drastically to 6,226 people. Reports based on gender show that women are consistently the group most often affected by digital crime, with as many as 5,020 in 2023.

Furthermore, in 2024, it increased to 6,145, decreasing drastically in 2025 to 2,551. The number of male victims showed the same pattern in 2023, with 3,484 victims. Furthermore, in 2024, it increased to 4,670 victims; in 2025, it decreased to 2,551. The difference in data between women and men shows that the female group is more vulnerable to digital crime. In the end, the decrease in the number of victims in 2025 drastically shows an increase in public awareness of digital security and the effectiveness of cyber regulations, as well as changes in crime patterns that have not been fully detected. The trends in the data above illustrate the importance of a more responsive and data-based protection strategy.

4.4. Digital crime attack prevention solutions

The increase in digital crime cases means that the need for more effective prevention solutions is a more serious government concern. Cyberattacks have targeted government institutions, the private sector, vital infrastructure, and individuals. Several digital crimes, such as phishing, data hacking, and the spread of malware, continue to develop, urging the government to determine concrete steps in adaptive and comprehensive prevention. Table 3, from several previous studies, provides solutions for preventing digital crime.

Table 3. Digital crime prevention solutions offered

No.	*Digital security tips*	*Explanation*	*Literature*
1	Using password management tools	Manage passwords to keep them strong and unique for each online account.	Fernando et al. (2023), Padalia et al. (2023)
2	Using the 2-factor authentication technique	Perform 2FA steps to add an extra layer of account security. This approach involves receiving a code on a phone or by email as identity verification.	Chavez et al. (2024)
3	Deepen the information and be educated	Update knowledge of every potential threat and online network fraud. Increased understanding can help in recognizing phishing techniques so they can be avoided.	Ali and Mohd Zaharon (2024), Ranjani et al. (2024)
4	Security software update efforts	Use a trusted antivirus and anti-malware. Update regularly to improve the system that is potentially from the latest cyber threats.	Parveen (2024), Rohith and Kaur (2021)
5	Be careful with personal information	Limit sharing of sensitive information on websites or with unknown contacts. Try to be skeptical of requests for personal information.	Ismail et al. (2021), Parker and Flowerday (2021), Taub et al. (2023)
6	Perform data backups routinely and regularly	Back up important files regularly. In case of a cyber attack, backup files can help in recovering data without data loss or extortion.	Mehra (2024), Tidke (2025)

Source: Authors' elaboration.

Table 3 provides various solutions from several studies related to digital crime. Password management tools allow users to store passwords securely, strongly, and uniquely for each online account. Two-factor authentication (2FA) is a powerful additional protection that prevents illegal access and involves double verification with a mobile phone or email. Increasing digital literacy makes well-educated users more aware of phishing threats and other online fraud. Routine security software updates, such as antivirus and operating systems, are used to cover for vulnerability gaps from malware attacks. Be careful when sharing personal information on sites or platforms that are less trusted to prevent data theft or social manipulation. Regular data backup efforts are also strategic efforts that can reduce the impact of ransomware cyber-attacks. Some solutions above are recommendations from various scientific literature and describe comprehensive approaches individuals and industries can take to strengthen digital security levels.

5. DISCUSSION

Online fraud practices are the most prominent and widespread digital crimes in general. The high level of online fraud is associated with the ease of committing crimes, such as low barriers to entry for perpetrators (Button & Cross, 2017). Online fraudulent acts include a variety of fraudulent practices such as phishing fraud, fake e-commerce sites, investment fraud, and identity theft. Internet anonymity makes perpetrators more daring, which opens up opportunities for perpetrators to operate across borders with limited risk of detection or prosecution (Danquah et al., 2022). The rapid growth of digital online transactions, online banking, and remote working environments during the COVID pandemic provides more opportunities for fraud to thrive (Isaia et al., 2024). Online fraudulent acts also cause significant financial and psychological harm to individuals and organizations (Kipngetich, 2025). A multi-layered strategy involving user education, stricter regulations, and technology protection (Kwizera & Micheal, 2024).

The decline in digital crime cases in 2023 and 2025 occurred drastically, but this trend cannot be interpreted as successful in cybersecurity. The decline could be due to the under-reporting of many victims of digital crime who choose not to report incidents because of shame (Kemp, 2022). Low awareness or limited trust in law enforcement in resolving cases is also a factor in low digital crime reports (Perez-Vincent et al., 2024). Digital crime is increasingly sophisticated, and approaches and tactics are used to avoid detection or operate in legal grey areas, making tracking and documenting violations more difficult (Cassidy et al., 2024). The decline in crime reports does not mean digital crime has decreased; fewer attacks can cause greater damage if they are more targeted and professional (Jones & Karger, 2023). Further investigation into reporting mechanisms and detection capabilities is needed.

Technological innovation and public awareness contribute to combating digital crime, but will be more effective if supported by stronger government regulations (Auliaurrahman et al., 2025; Chitsungo, 2024). The private sector's intention to develop secure software, two-factor authentication, and educational campaigns is often not supported by the authority and scope needed to enforce standards across the industry (Matelski, 2022). Without government support, cybersecurity practices will lack uniformity, and many organizations will forego proper protection in favour of cost-saving measures (Mujawar et al., 2024). Digital criminals often operate across national borders, making local enforcement inadequate unless accompanied by strong international digital crime laws and cooperation frameworks (Almuhaisen, 2024). Well-established government regulation is essential to ensure that digital platforms are held accountable for data breaches, reporting mechanisms are mandatory, and victims have legal recourse. Even the most sophisticated cybersecurity solutions risk being ineffective without a clear legal framework

and strict enforcement. Government engagement through legislation, oversight, and investment in digital infrastructure are fundamental pillar to ensuring long-term success in combating cybercrime.

6. CONCLUSION

Online fraud is a vast digital crime, such as phishing, extortion, and personal data violations. Such crimes urgently require a comprehensive strategy to overcome digital fraud. Women are a group that is more vulnerable to becoming victims of online fraud in terms of hacking social media accounts and phishing. The decline in reports of digital crime has not been fully used as a measure of success in eradicating digital crime. The low awareness that they have become victims also causes no reports to law enforcement. The shame of becoming a victim of online fraud is also a cause of low reports of digital crime. Individual security is critical to overcoming digital crime and is supported by a strong regulatory framework and government supervision. Government initiative regulations play a vital role in reducing the risk of online fraud. This study is still limited in exploring digital crime trends by interviewing actors directly involved. Asking for solutions for victims of digital crime will enrich data for further research. This research offers practical implications for legal institutions in designing effective mechanisms to encourage crime victims to share their negative experiences more openly, thereby supporting the eradication of digital crime. It also provides theoretical implications for approaches and concepts in handling digital crime. This research is important for the future because the problem of digital crime continues to grow, and it can serve as a reference in developing responsive digital protection strategies.

REFERENCES

Acharya, S., & Joshi, S. (2020). Impact of cyber-attacks on banking institutions in India: A study of safety mechanisms and preventive measures. *PalArch's Journal of Archaeology of Egypt/Egyptology, 17*(6), 4656–4670. https://archives.palarch.nl/index.php/jae/article/view/1714

Adebayo, A. S., Chukwurah, N., & Ajayi, O. O. (2025). Artificial intelligence and machine learning algorithms for advanced threat detection and cybersecurity risk mitigation strategies. *Engineering and Technology Journal, 10*(3), 4080–4094. https://doi.org/10.47191/etj/v10i03.18

Ali, M. M., & Mohd Zaharon, N. F. (2024). Phishing — A cyber fraud: The types, implications and governance. *International Journal of Educational Reform, 33*(1), 101–121. https://doi.org/10.1177/10567879221082966

Almuhaisen, H. J. (2024). Confronting cybercrimes under the provisions of public international law. G*lobal Journal of Politics and Law Research, 12*(1), 78–88. https://doi.org/10.37745/gjplr.2013/vol12n17888

Al Zaidy, A. (2024). Digital crimes and digital terrorism: The new frontier of threats in cyberspace. *Journal of Information Technology, Cybersecurity, and Artificial Intelligence, 1*(1), 18–29. https://doi.org/10.70715/jitcai.2024.v1.i1.003

Amri, P., Nurmandi, A., & Mutiarin, D. (2022). The role of policy actors in determining the direction of disruptive innovation policy [Special issue]. *Journal of Governance and Regulation, 11*(4), 374–386. https://doi.org/10.22495/jgrv11i4siart18

Ariansyah, A., Prayogi, S., Kurnia, N., Bilad, M. R., & Sutarto, S. (2024). Digital technology to support sustainable development goals (SDGs): Literature review. *Lensa: Jurnal Kependidikan Fisika, 12*(2), 315–358. https://doi.org/10.33394/j-lkf.v12i2.13557

Arif, Z., Zulfitria, Bariyah, O. N., Sopa, Supyadillah, A., & Darmansyah, D. F. (2024). Blockchain as a facilitator for secure migration: A case study of e-commerce in Indonesia. *Revista de Gestão — RGSA, 18*(2), Article 06342. https://doi.org/10.24857/rgsa.v18n2-164

Arsyad, A. A. J., Tamrin, U., Lande, J. P., & Umar, N. (2024). Meningkatkan kesadaran remaja terhadap phishing melalui literasi digital: Studi kasus di SMK Darussalam Makassar [Raising teen awareness about phishing through digital literacy: A case study at SMK Darussalam Makassar]. *Jurnal Pengabdian Literasi Digital Indonesia, 3*(2), 60–71. https://journal.artika.id/abdimas/article/download/122/88

Astika, I. P. B., Sujana, I. N., & Wijaya Caste, I. K. A. (2024). Legal protection of fund saving customers against cyber phising acts in Indonesia. *Global International Journal of Innovative Research, 2*(8), 1951–1961. https://doi.org/10.59613/global.v2i8.285

Auliaurrahman, A., Anshari, N., & Firdaus, S. U. (2025). The existence and regulation of cyber law: The government's role in combating digital crime in Indonesia. *Jurisprudensi: Jurnal Ilmu Syariah, Perundang-Undangan dan Ekonomi Islam, 17*(1), 206–223. https://doi.org/10.32505/jurisprudensi.v17i1.10612

Aziz, W. K., & Daryanto, E. (2025). The integration of strategic intelligence and cyber resilience in combating organized narcotics crime in Indonesia (A case study of Hydra Indonesia). *Security Intelligence Terrorism Journal (SITJ), 2*(1), 78–83. https://doi.org/10.70710/sitj.v2i1.34

Button, M., & Cross, C. (2017). *Cyber frauds, scams and their victims.* Routledge. https://doi.org/10.4324/9781315679877

Cassidy, A. A. T. J., Fuad, A., & Shofy, M. U. A. A. (2024). Emerging trends and challenges in digital crime: A study of cyber criminal tactics and countermeasures. *TechComp Innovations: Journal of Computer Science and Technology, 1*(1), 38–45. https://doi.org/10.70063/techcompinnovations.v1i1.25

Chavez, F., Fernandez-Reyes, A., & Byrne, M. D. (2024). Context contributes to two-factor authentication choices. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 68*(1), 1374–1379. https://doi.org/10.1177/10711813241261680

Chitsungo, C. (2024). Harnessing digital strategies to combat cryptocurrency-enabled crimes: Addressing money laundering, illicit trade, and cyber threats. *American Journal of International Relations, 9*(7), 77–106. https://doi.org/10.47672/ajir.2523

Collier, H., & Morton, C. (2024). Teenagers: A social media threat vector. *Proceedings of the 19th International Conference on Cyber Warfare and Security (ICCWS 2024), 19*(1), 55–61. https://doi.org/10.34190/iccws.19.1.1980

Daguatha, R. (2022). Use of digital platforms to commit nefarious activities globally. A critical literature review. *Journal of International Relations and Policy, 3*(2), 12–23. https://doi.org/10.47941/jirp.1106

Danquah, P., Kani, J. A., & Bibi, D. (2022). Internet fraud: The influence of identity flexibility and dissociative anonymity. *East African Journal of Information Technology, 5*(1), 39–52. https://doi.org/10.37284/eajit.5.1.673

Dua, S., Shah, P., & AbdAllah, E. G. (2024). Navigating the digital landscape: Enhancing small and medium business's security through asset management and data classification. *2024 11th IEEE Swiss Conference on Data Science (SDS)*, 55–61. https://doi.org/10.1109/SDS60720.2024.00016

Dwiaji, L., Widodo, A. M., Firmansyah, G., & Tjahyono, B. (2024). Analysis of knowledge management strategies for handling cyber attacks with the computer security incident response team (CSIRT) in the Indonesian aviation sector. *Asian Journal of Social and Humanities, 2*(6), 1341–1353. https://doi.org/10.59888/ajosh.v2i6.261

Fernando, W. P. K., Dissanayake, D. A. N. P., Dushmantha, S. G. V. D., Liyanage, D. L. C. P., & Karunatilake, C. (2023). Challenges and opportunities in password management: A review of current solutions. *Sri Lanka Journal of Social Sciences and Humanities, 3*(2), 9–20. https://doi.org/10.4038/sljssh.v3i2.96

George, E. P.-E., Idemudia, C., & Ige, A. B. (2024). Blockchain technology in financial services: Enhancing security, transparency, and efficiency in transactions and services. *Open Access Research Journal of Multidisciplinary Studies, 8*(1), 26–35. https://doi.org/10.53022/oarjms.2024.8.1.0042

Gjorgjev, J., Ramadhan, M. F. F., & Dhamayana, S. (2025). Blockchain forensics — Unmasking anonymity in dark web transactions. *International Journal of Criminology and Sociology, 14*, 68–75. https://doi.org/10.6000/1929-4409.2025.14.07

Han, S., Chen, H., Wu, Y., & Pérez-Escamilla, R. (2022). Content analysis of breast milk substitutes marketing on Chinese e-commerce platforms. *Maternal & Child Nutrition, 18*(2), Article 13332. https://doi.org/10.1111/mcn.13332

Hermanto, F. F., Hermawan, G., & Atmojo, R. N. P. (2025). Indonesian people's readiness for blockchain adoption in e-commerce. 2025 *International Conference on Advancement in Data Science, E-Learning and Information System (ICADEIS)*, 1–7. https://doi.org/10.1109/ICADEIS65852.2025.10932994

Hidayat, F., Khusaini, M., Efani, A, & Sukarmi. (2025). From threat assessment to action: Counterterrorism special detachment 88's perspective on combating cyber terrorism in Indonesia. *Journal of Lifestyle and SDGs Review, 5*(3), Article 05090. https://doi.org/10.47172/2965-730x.sdgsreview.v5.n03.pe05090

Hutapea, O., & Talita, A. S. (2021). Implementasi metode k-medoids untuk masalah intrusion detection system menggunakan bahasa pemrograman MATLAB [Implementation of the k-medoids method for intrusion detection system problems using the MATLAB programming language]. *Faktor Exacta, 14*(2), 84–91. https://doi.org/10.30998/faktorexacta.v14i2.9429

Isabella, I., Alfitri, A., Saptawan, A., Nengyanti, N., & Baharuddin, T. (2024). Empowering digital citizenship in Indonesia: Navigating urgent digital literacy challenges for effective digital governance. *Journal of Governance and Public Policy, 11*(2), 142–155. https://doi.org/10.18196/jgpp.v11i2.19258

Isaia, E., Oggero, N., & Sandretto, D. (2024). Is financial literacy a protection tool from online fraud in the digital era? *Journal of Behavioral and Experimental Finance, 44*, Article 100977. https://doi.org/10.1016/j.jbef.2024.100977

Ismail, A., Hamzah, M. R., & Hussin, H. (2021). The roles of trust and perceived risks on online self-disclosure. *AIP Conference Proceedings, 2347*(1), Article 020191. https://doi.org/10.1063/5.0051808

Jagadeesan, S., Sameer, Singh, D., Ojha, R., Ibrahim, R. K., & Alazzam, M. B. (2023). Application of cybersecurity in e-learning education. In *2023 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE)* (pp. 932–937). https://doi.org/10.1109/AECE59614.2023.10428587

Jansen, S., Knippels, M.-C. P. J., & van Joolingen, W. R. (2021). Lesson study as a research approach: A case study. *International Journal for Lesson and Learning Studies, 10*(3), 286–301. https://doi.org/10.1108/IJLLS-12-2020-0098

Jones, T., & Karger, E. (2023). *School and crime* (CESifo Working Paper No. 10702). Center for Economic Studies and Ifo Institute (CESifo). https://doi.org/10.2139/ssrn.4610983

Katiyar, N., Tripathi, S., Kumar, P., Verma, S., Sahu, A. K., & Saxena, S. (2024). AI and cyber-security: Enhancing threat detection and response with machine learning. *Educational Administration: Theory and Practice, 30*(4), 6273–6282. https://doi.org/10.53555/kuey.v30i4.2377

Kemp, S. (2022). Fraud reporting in Catalonia in the Internet era: Determinants and motives. *European Journal of Criminology, 19*(5), 994–1015. https://doi.org/10.1177/1477370820941405

Kipngetich, A. (2025). A review of online scams and financial frauds in the digital age. *GSC Advanced Research and Reviews, 22*(1), 302–329. https://doi.org/10.30574/gscarr.2025.22.1.0025

Kwizera, I., & Micheal, S. (2024). Developing a multi-layered defence system to safeguard data against phishing attacks. *International Journal of Innovative Science and Research Technology (IJISRT), 9*(2), 2022–2033. https://doi.org/10.38124/ijisrt/ijisrt24feb1107

Margarov, G. I., Mitrofanova, E. A., & Anikeeva, L. V. (2021). Formation of a justified strategy of education in the sphere of information security in the digital economy. In E. G. Popkova, V. N. Ostrovskaya, and A. V. Bogoviz (Eds.), *Socio-economic systems: Paradigms for the future* (pp. 15–21). Springer. https://doi.org/10.1007/978-3-030-56433-9_2

Marshall, N., Sturman, D., & Auton, J. C. (2024). Exploring the evidence for email phishing training: A scoping review. *Computers & Security, 139*, Article 103695. https://doi.org/10.1016/j.cose.2023.103695

Matelski, S. (2022). Human-computable OTP generator as an alternative of the two-factor authentication. *Proceedings of the 2022 European Interdisciplinary Cybersecurity Conference*, 64–71. https://doi.org/10.1145/3528580.3532842

Mehra, T. (2024). The role of encryption in securing backup data against ransomware threats. *International Journal of Science and Research Archive, 13*(2), 1971–1974. https://doi.org/10.30574/ijsra.2024.13.2.2381

Metibemu, O. C. (2025). Financial risk management in digital-only banks: Addressing fraud and cybersecurity threats in a cashless economy. https://doi.org/10.2139/ssrn.5166723

Mujawar, S., Gupta, G., Kunchi, S., Rahangdale, P., Yadav, G., & Patil, S. K. (2024). The impact of government regulations on cyber security policy development. *Computer Fraud and Security, 2024*(8), 105–113. https://doi.org/10.52710/cfs.79

Muzakki, A. S., & Suraji, S. (2024). Legal protection of consumers in e-commerce through social media in Indonesia in the Industrial Era 4.0. *International Journal of Law, Crime and Justice, 1*(3), 297–302. https://doi.org/10.62951/ijlcj.v1i3.183

Nettel, P. F., Hankins, E., Stirling, R., Cirri, G., Grau, G., Rahim, S., & Crampton, E. (2024). *Government AI Readiness Index 2024*. Oxford Insights. https://oxfordinsights.com/wp-content/uploads/2024/12/2024-Government-AI-Readiness-Index-2.pdf

Odebade, A. T., & Benkhelifa, E. (2023). *Evaluating the impact of government cyber security initiatives in the UK*. ArXiv. https://doi.org/10.48550/arXiv.2303.13943

Padalia, H., Patel, H., Deshmukh, A., Patil, M., Kumar, A., & Nrip, N. K. (2023). A study on password manager: Users' perspective. *2023 International Conference on Computational Intelligence for Information, Security and Communication Applications (CIISCA)*, 72–75. https://doi.org/10.1109/ciisca59740.2023.00024

Parker, H. J., & Flowerday, S. (2021). Understanding the disclosure of personal data online. *Information & Computer Security, 29*(3), 413–434. https://doi.org/10.1108/ics-10-2020-0168

Parveen, K. (2024). Advanced techniques of malware evasion and bypass in the age of antivirus. *International Journal for Electronic Crime Investigation, 8*(3), 25–40. https://ijeci.lgu.edu.pk/ijeci/article/view/205/156

Patroli Siber. (2025). *Patroli Siber*. https://patrolisiber.id/about-us/

Peersman, C., Williams, E., Edwards, M., & Rashid, A. (2022). *Understanding motivations and characteristics of financially-motivated cybercriminals*. ArXiv. https://doi.org/10.48550/arXiv.2203.08642

Perez-Vincent, S. M., Abril, V., Chen, C., Tayo, T., & Urrego Jimenez, A. (2024). *Crime underreporting in Latin America and the Caribbean*. IDB. https://doi.org/10.18235/0013215

Pusiknas Polri. (2025). *Victim data*. https://pusiknas.polri.go.id/data_korban

Rakhmanova, E. N., & Pinkevich, T. V. (2020). Digital crime concept. *2nd International Scientific and Practical Conference "Modern Management Trends and the Digital Economy: From Regional Development to Global Economic Growth" (MTDE 2020)*, 193–196. https://doi.org/10.2991/aebmr.k.200502.031

Ramadhani, E. H., Enriko, I. K. A., & Sari, E. L. I. P. (2025). Kajian strategik manajemen keamanan siber terhadap proyek telematika di Indonesia: Studi kasus kebocoran pusat data nasional [Strategic review of cybersecurity management for telematics projects in Indonesia: Case study of national data center leaks]. J*urnal Indonesia: Manajemen Informatika dan Komunikasi, 6*(1), 570–580. https://doi.org/10.35870/jimik.v6i1.1210

Ranjani, J., Kamala, B., Kalaiselvi, V. K. G., Aishwarya, R., & Abinaya, A. (2024). Phishing attack detector and awareness generator. *2024 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS)*, 1–6. https://doi.org/10.1109/icpects62210.2024.10780168

Rinaldy, L. Y., Salim, H. S., & Suhartana, L. W. P. (2025). Unilateral cancellation by the buyer in cash on delivery (COD) transactions via e-commerce according to Indonesian Positive Law. *Research Review International Journal of Multidisciplinary, 10*(1), 28–39. https://doi.org/10.31305/rrijm.2025.v10.n1.004

Rohith, C., & Kaur, G. (2021). A comprehensive study on malware detection and prevention techniques used by anti-virus. *2021 2nd International Conference on Intelligent Engineering and Management (ICIEM),* 429–434. https://doi.org/10.1109/iciem51511.2021.9445322

Roz, I. D., Saimima, J. M., Salmon, H. C. J., Wadjo, H. Z., & Fitrian, A. (2025). Sexual harassment crime in digital space: Legal challenges and solutions. *Journal of Strafvordering Indonesian, 1*(6), 14–23. https://doi.org/10.62872/h2afmb07

Rusman, R., & Kamaludin, A. (2024). Investigation of cyber crime in the Indonesian legal framework. *Journal la Sociale, 5*(6), 1576–1586. https://doi.org/10.37899/journal-la-sociale.v5i6.1367

Sandeep, M. M., Lavanya, V., & Balakrishnan, J. (2025). Leveraging AI in recruitment: Enhancing intellectual capital through resource-based view and dynamic capability framework. *Journal of Intellectual Capital, 26*(2), 404–425. https://doi.org/10.1108/jic-05-2024-0155

Stanchev, P., Tomov, Y., & Hinov, N. (2024). Problems and solution in ensuring cybersecurity of IoT devices for the needs of small and medium enterprises. *2024 12th International Scientific Conference on Computer Science (COMSCI)*, 1–4. https://doi.org/10.1109/COMSCI63166.2024.10778507

Syafruddin, Thaba, A., & Ananda, R. (2024). Ujaran kebencian netizen Indonesia pada akun Twitter es teh: Tinjauan linguistik forensik [Hate speech by Indonesian netizens on the es teh Twitter account: A forensic linguistic review]. *Semantik, 13*(1), 15–28. https://doi.org/10.22460/semantik.v13i1.p15-28

Syahril, M. A. F., & Aris, A. (2024). Strategies and dynamics of online fraud in Indonesia: Tracing the effectiveness of the implementation of the Electronic and Transaction Information Act. *Journal of Law Justice, 2*(3), 198–205. https://doi.org/10.33506/jlj.v2i3.3711

Syalendro, O., Lubis, A. F., & Putra, R. Y. A. E. (2025). Cyber crime crimes in Indonesian law and efforts to prevent and handle cyber crime cases. *AURELIA: Jurnal Penelitian Dan Pengabdian Masyarakat Indonesia, 4*(1), 335–347. https://doi.org/10.57235/aurelia.v4i1.3708

Taub, G., Elmalech, A., Aharony, N., & Rosenfeld, A. (2023). Monetary compensation and private information sharing in augmented reality applications. *Information, 14*(6), Article 325. https://doi.org/10.3390/info14060325

Tidke, S. (2025). Fortifying data resilience: A comprehensive approach to securing backup systems. *International Journal of Scientific Research in Engineering and Management (IJSREM), 9*(1), 8–11. https://doi.org/10.55041/IJSREM41174

Tn, N., & Shailendra Kulkarni, M. (2023). Zero click attacks — A new cyber threat for the e-banking sector. *Journal of Financial Crime, 30*(5), 1150–1161. https://doi.org/10.1108/jfc-06-2022-0140

Tomczyk, Ł. (2021). Evaluation of digital piracy by youths. *Future Internet, 13*(1), Article 11. https://doi.org/10.3390/fi13010011

Wali, G., & Sivathapandi, P. (2025). Suspicious transaction detection in bank transactions using agentic AI. *Cuestiones de Fisioterapia, 54*(2), 4827–4836. https://doi.org/10.48047/eed97w67

Wibowo, B., Hafiz, L., & Hidayat, T. (2025). Unveiling the cybercrime ecosystem: Impact of ransomware-as-a-service (RaaS) in Indonesia. *International Journal of Science Education and Cultural Studies, 4*(1), 11–21. https://doi.org/10.58291/ijsecs.v4i1.320

Wibowo, S. E., Hartono, A., Kiswanto, H., Louerens, J. T. A., & Primawanti, H. (2024). Securitization of cyber threats to the Indonesian government: A study of cyber defense strategy. *Global Political Studies Journal, 8*(2), 97–108. https://doi.org/10.34010/gpsjournal.v8i2.13817

Wulandari, R., Priyanto, P., & Hendra, A. (2025). The Indonesia's cyber security strategy in the face of evolving modern warfare threats. *Formosa Journal of Applied Sciences, 4*(2), 615–626. https://doi.org/10.55927/fjas.v4i2.5