Journal of Human Security | 2023 | Volume 19 | Issue 2 | Pages 12-17
DOI: 10.12924/johs2023.19020002
ISSN: 1835-3800

Journal of Human Security

Research Article

Victim Protection Against Crimes Under the Guise of Electronic Investment in Indonesia

Herlina Manullang[1], M. Citra Ramadhan[2]

[1] Universitas HKBP Nommensen, Medan, Indonesia
Email: HerlinaManullang@uhn.ac.id
Orcid ID: https://orcid.org/0009-0005-6769-4806
[2] Universitas Medan Area, Medan, Indonesia
Email: citra@staff.uma.ac.id
Orcid ID: https://orcid.org/0000-0002-7897-2737

Submitted: 1 April 2022 |In revised form: 14 April 2023 | Accepted: 28 October 2023 |
Published: 2 December 2023

Abstract: The pervasive escalation of electronic transactions has profoundly reshaped the business landscape, offering diverse domestic and global investment prospects. Despite the opportunities, investors grapple with challenges in the realm of electronic investments, encompassing fraudulent activities, embezzlement, money laundering, and illicit investment practices. Consequently, this research endeavours to investigate mechanisms safeguarding victims from crimes perpetrated under the guise of electronic investment in Indonesia. Employing a normative judicial approach, the study involves the scrutiny of legal documents and pertinent regulations related to electronic investment crimes in Indonesia. To achieve its objective, the study relies on secondary qualitative data sourced from online databases such as Nexis, Lexis, JSTOR, Hein Online, and other relevant outlets, employing content analysis. Findings indicate a pronounced promotion of electronic transactions in Indonesia, with emphasis on adherence to the Investment Law, "Electronic Transactions and Information" (ETI) law, Consumer Protection Law, and the Indonesian Criminal Code (KUHP). Notably, punitive measures for individuals engaged in electronic investment fraud are outlined in Articles 372 and 378 of the KUHP. Nevertheless, a compelling necessity exists for the formulation and implementation of a tailored legal framework addressing victim protection against crimes associated with electronic investment in Indonesia. The study yields practical and theoretical implications, spotlighting enhancements required in the legal infrastructure governing electronic investments in the Indonesian context.

Keywords: Electronic Investment, Indonesia, Victim Protection, KUHP, Electronic Transactions and Information, Investment Law.

1. Introduction

Indonesia, as a burgeoning economy with auspicious prospects for business investments, is undergoing simultaneous economic and demographic expansions. A pivotal allure for investment lies in the substantial size of the Indonesian population. Against the backdrop of contemporary globalization characterized by swift technological and informational progress, online investment has emerged as a compelling choice. This phenomenon captivates the interest of millennials and other individuals enthusiastic about exploring novel avenues [1]. The attractiveness of online investment is predicated upon its perceived advantages in time efficiency, managerial simplicity, and profit potential. Empowered by a smartphone and accessible financial resources, individuals can readily assume the role of investors. The salient factor propelling interest among online investment users is the convenience proffered by digital investment applications. Nonetheless, the initial months of 2022 witnessed a downturn in confidence regarding online investment, as the public was disconcerted by the disclosure of fraudulent instances posing as bona fide investment opportunities [1]. Subsequent to police investigations, a multitude of instances of investment fraud were unveiled, culminating in substantial financial losses amounting to hundreds of billions of rupiah. The surge in electronic investment has precipitated a disconcerting rise in fraudulent activities within Indonesia. While the nation holds the potential for accelerated growth in its digital economy, a pressing challenge that demands immediate attention and intervention is the inadequacy of protective measures for victims ensnared in financial crimes related to electronic investments. The Criminal Code's Articles 372 and 378, prescribing a maximum sentence of four years' imprisonment or a fine of nine hundred thousand rupiahs, delineate the legal repercussions for individuals implicated in online investment fraud in Indonesia [2]. Legislation No. 11 of 2008 explicitly proscribes actions conducted through electronic systems; however, the existing provisions within the Criminal Code addressing fraud remain incongruent with such acts. This incongruity arises primarily from the prevalent use of email by individuals perpetrating fraud through online channels to communicate with their victims. Notably, legal activities conducted through computers or other electronic media fall under the classification of electronic transactions, as

© 2023 by the authors; licensee Librello, Switzerland. This open access article was published under a Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/).

librello

articulated in Article 1 Point 2 of Law Number 19 of 2016 Pertaining to Information and Electronic Transactions [3].

The contemporary transition of diverse activities from the tangible domain to the digital milieu is notably conspicuous in commercial transactions, where the processes of buying, selling, and leasing have predominantly migrated to online platforms. In response to these digital transformations, legal frameworks have undergone revisions to align with the evolving landscape. Within the purview of Islamic law, the emergence of novel cases underscores the imperative of establishing a robust foundation capable of delineating new legal certainties. Simultaneously, the trajectory of technological progress has reshaped the dynamics of international currency exchanges within the contemporary business paradigm. The direct exchange of currencies between nations has witnessed a diminishing trend, particularly in light of the ascendancy of binary options trading systems [4]. The vicissitudes witnessed in foreign exchange transactions hinge upon the economic and political circumstances prevailing in the pertinent nations. Within this realm, three principal stakeholders actively participate: investors, exporters, importers, and speculators, each motivated by distinct requirements for currency conversion [5]. Investment, a common commercial endeavour, presents potential returns but is inherently accompanied by corresponding risks. The risk level associated with an investment aligns directly with its profit potential. The Foreign Exchange (Forex) phenomenon plays a pivotal role in Indonesia's economic development, drawing significant attention from both investors and the public. This form of trade entails the continuous exchange of a country's currency against those of other nations in global money markets, operating 24 hours a day. With a daily trading volume exceeding USD 4 trillion, Forex trading stands as the world's largest financial market, as affirmed by existing scholarly literature [6, 7].

In the present-day societal landscape, the ubiquitous progress in information and communication technology exerts a profound influence on diverse aspects of existence, particularly within the corporate sphere. A paradigmatic concept, electronic business (e-business), has surfaced as a transformative influence. Enabled by Electronic Data Interchange (EDI), email, electronic bulletin boards, electronic cash transfers, and other network-based technologies, this business model fosters the seamless exchange of information and advocates for the conduct of paperless corporate transactions [8, 9]. Indonesia distinguishes itself as a prospective nation undergoing swift progress in the realm of e-business or e-commerce. Nevertheless, businesses within the region have not fully capitalized on the opportunities presented by e-business technologies. In light of the increasing popularity of online investment platforms, particularly among millennials and individuals seeking alternative avenues for capital growth, it becomes imperative for Indonesia to address crimes perpetrated under the guise of electronic investment. The prevalence of fraudulent schemes poses a substantial threat to public trust and financial security, potentially resulting in significant monetary losses. To safeguard investors from falling victim to such deceptive activities, the establishment of robust victim protection measures is essential. The objective is to preserve the integrity and legitimacy of Indonesia's online investment landscape by fostering a secure environment that instils confidence and trust among potential investors. This, in turn, is envisaged to fortify the sustained expansion and development of the industry.

2. Literature Review

2.1 Surge in Electronic Investment

The investigation conducted by LubİS, et al. [10] and Kong and Lin [11] underscores the distinctive attributes of Non-Fungible Tokens (NFTs) as a pivotal factor influencing price premiums in the domain of electronic investments. Furthermore, investors strategically positioned within the NFT network through assertive trading and early adoption experience favourable price outcomes. Notably, seasoned investors demonstrate an ability to acquire NFTs at reduced costs. Positioned as a distinct asset class, NFTs exhibit a unique risk-return profile, presenting elevated yields and associated risks compared to traditional assets, particularly in a low-interest-rate environment. In this context, NFTs outperform other alternative assets, including luxury items, private equity, and artwork. Adrian and Mancini-Griffoli [12] propose that certain types of digital currencies could experience rapid adoption due to their facilitation of electronic investing, notwithstanding potential reliability concerns in comparison to other currencies. The examination delves into potential merits and drawbacks of this trend. A risk mitigation strategy could involve mandating that central bank reserves be entirely collateralized by specific digital currencies [13]. Fuelled by robust infrastructure and innovations tailored to the extensive Chinese market, local enterprises swiftly transitioned from leisure pursuits to formal business ventures, thereby transforming the world's most populous nation into an active online consumer base. China's ascent above the United States in retail e-commerce and digital payments is attributed to this explosive growth in electronic investment [14, 15]. While China demonstrated adeptness in incorporating digital technologies into established business-to-business and customer-to-customer ventures, it encountered challenges in attaining comparable success in the realm of business-to-business services. Regarding the foundational general-purpose technologies underpinning the digital economy, the United States remains at the forefront [15, 16].

2.2 Opportunities and Challenges in Electronic Investment

Cybersecurity breaches pose a formidable challenge that necessitates mitigation within the domains of businesses and e-commerce technology. The academic and business sectors are increasingly focusing on applications of e-commerce technology. This technological advancement has facilitated achievements that were previously unattainable for consumers and the business community. However, it has concurrently introduced cybersecurity challenges, with malware, denial of service attacks, social engineering, and assaults on personal information standing out as particularly critical issues among various cybersecurity concerns [17]. International enterprises make substantial investments in addressing the escalating risks of cybersecurity, an issue that continues to intensify each year. The perpetual quest by attackers to identify novel vulnerabilities in individuals, businesses, and technology renders the prospect of overcoming this obstacle a formidable task. E-commerce, since its inception, has consistently grappled with a significant and enduring challenge, predominantly arising from the persistent threat of cybersecurity [18]. Cybersecurity, a critical facet, plays a pivotal role in shielding computer systems from information disclosure, misdirection, and the unauthorized acquisition or impairment of electronic data, software, or hardware. Within the domain of e-commerce, emphasis is placed on electronic security concerning online commercial transactions. Despite persistent investments by businesses in technological measures aimed at mitigating cyber threats, unauthorized access to business systems and data remains an ongoing challenge. The cybersecurity landscape is inherently dynamic, marked by malicious actors perpetually refining their skills and adopting advanced technologies and methodologies to exploit vulnerabilities and target diverse organizations [17].

2.3 Laws for Victim Protection in Electronic Investment

In the realm of online business fraud, the establishment of legal safeguards is imperative to shield potential victims from imminent criminal activities. Article 4 of the Consumer Protection Act delineates the entitlement of consumers to compensation and reimbursement in instances where goods or services deviate from agreed-upon terms. Law Number 31 of 2014, amending Law Number 13 of 2006 on the Protection of Witnesses and Victims, specifically defines victims as individuals suffering physical, mental, or economic losses due to criminal acts. Despite the virtual nature of cyberspace, legal frameworks remain indispensable in shaping societal conduct [19]. Transactions conducted in the cyber domain bear tangible economic and non-economic repercussions in the real world. The emphasis lies on victim protection through procedural rights, affording victims the right to personal security against physical and psychological threats associated with their testimonies [20]. This encompasses entitlements such as the right to select forms of protection, legal counsel, providing information free from coercion, acquiring a new identity and residence, and covering transportation expenses. The legal framework governing cybercrime in Indonesia is established by Law Number 11 of 2008 on Information and Electronic Transactions, while consumer protection is anchored in Law Number 8 of 1999. These regulations are designed to shield individuals from technological crimes, acknowledging the burgeoning number of technology users. Victims of online business fraud, experiencing material losses, find protection under the Consumer Protection Act and the ITE Law. Article 4 of the Consumer Protection Act delineates consumer rights, encompassing the entitlement to comfort, security, and safety in the consumption of goods/services, along with the right to choose and receive goods/services in accordance with agreed-upon terms and guarantees. In the context of online business fraud, rights and obligations, though distinct, are intricately interlinked, constituting indispensable components of legal discourse [19].

The prevailing uncertainties present a significant peril of commercial risk to businesses, consumers, and the overall nation. In Kuwait, the adoption of e-commerce within the business sector has been sluggish, and the legal framework has yet to comprehensively regulate the cyberspace domain [21]. Alkhaldi [21] contended that with an increasing number of consumers transitioning to online shopping, businesses confront the complexities of cybersecurity and the potential consequences that may unfold.

Hence, it is crucial for the government to allocate substantial investments in cybersecurity to ensure the safeguarding of businesses operating within its jurisdiction. The research conducted by Fathul and Ana [22], underscores the pressing necessity for legal safeguards for Indonesian consumers utilizing online lending services, particularly in the context of economic adversities prompting increased reliance on such services. The absence of specific regulations addressing the rights and security of individuals engaging in online loans raises significant concerns.

A study conducted by Bossler, et al. [23] revealed that law enforcement agencies equipped with well-defined policies and procedures, constables possessing computer skills and experience in addressing online incidents, along with their capacity to empathize with victims of fraud, demonstrated a positive association with the preparedness of constables and sergeants to respond to instances of online fraud. Koutroumpis, et al. [24] suggested is the exploration of consequences related to the development of resources and training for first responders in the combat against cybercrimes. This inquiry investigates the ramifications of more robust data protection laws on cybersecurity hiring in the United Kingdom through an analysis of online job postings. The institutional changes stemming from the removal of the requirement to demonstrate substantial damage and distress in 2015 and the enactment of the Data Protection Act 2018 are examined as factors influencing data protection enforcement by the Information Commissioner's Office (ICO). The findings unveil that heightened data protection enforcement, as indicated by these legal modifications, significantly amplifies the demand for cybersecurity skills by up to 52%, particularly among data-intensive firms, those leveraging cloud technologies, and those with higher cash holdings [24].

International investment law may afford protection to digital operations if they meet the criteria qualifying them as investments. In this context, exception clauses within investment agreements play a pivotal role in aiding states in reconciling diverse objectives, including the promotion of an accessible, efficient, and secure Internet [25]. Nonetheless, the existing framework of international investment law predates the advent of the digital economy, rendering it inadequately equipped to regulate the complexities associated with cross-border data flows. A more intricate and equitable system is imperative to effectively address the challenges brought about by the digital revolution [26]. Furthermore, concerted efforts are essential to bridge the digital divide existing between less developed nations, technologically advanced countries, and smaller entities. The passage of the California Consumer Privacy Act of 2018 (CCPA) marked California as the inaugural state in the union to confer enhanced privacy rights upon its residents. Subsequent modifications to the CCPA have been instituted by the California legislature since its enactment [27].

Yusup [28] study outlines a threefold strategy for addressing illicit online investment entities in Indonesia. It involves regulatory initiatives to establish comprehensive regulations, supervisory efforts encompassing monitoring and assessment, and enforcement actions, which presently include sanctions like revoking licenses and blocking websites. Notably absent are measures ensuring legal protection and compensation for victims of illegal online investments.

3. Method

The methodological approach employed in this research adopts a normative juridical framework to qualitatively evaluate the safeguard mechanisms for victims of crimes associated with electronic investment in Indonesia. The qualitative nature of the study facilitates a comprehensive examination of the dynamics surrounding victim protection against crimes under the guise of electronic investment in the Indonesian context. This research aligns with the interpretivist research philosophy, prioritizing subjective truths, and proves particularly suitable for qualitative inquiries [29]. Interpretivism is chosen for its suitability in examining the legal and social aspects of victim protection in electronic investment crimes in Indonesia. The study adopts an inductive approach to comprehend the multifaceted consequences in this context.

The study derives primary data from legal documents and associated publications, enabling an in-depth investigation into victim protection against crimes under the guise of electronic investment in Indonesia. The use of official legal documents enhances the study's findings' authenticity, credibility, and reliability. Secondary data is obtained from scholarly publications on victim protection laws, accessed from platforms including Hein Online, JSTOR, NEXIS, Wiley Online Library, and West Law, offering a broader global context. Content analysis is applied to scrutinize the collected data, ensuring a comprehensive examination of both primary and secondary sources.

4. Results and Discussion

In the contemporary era of digitization, the acceleration of electronic investments has become prevalent across diverse sectors, underscoring the imperative for the establishment and

implementation of robust laws and regulations to safeguard investors and associated stakeholders. The study's objective is centred on electronic investments in Indonesia, with subsequent emphasis on investment law and protective measures against crimes within the electronic investment domain in Indonesia.

4.1 Electronic Investment in Indonesia

Amidst ongoing advancements in information technology (IT), the integration of electronic investments is experiencing swift proliferation in Indonesia. Consequently, diverse companies within the nation are actively engaging in various electronic investment activities [30], contributing to the enhancement of overall economic growth. Projections indicate that the total transaction value within Indonesia's digital investment market is anticipated to reach USD$33.26 billion in the year 2023. Moreover, an annual growth rate of 16.05% is envisaged for the transaction value during the period spanning 2023 to 2027 [31]. As per data presented by the "Alert Task Force" (ATF) of the "Otoritas Jasa Keuangan" (OJK), the financial services authority in Indonesia, the public incurred a loss of Rp. 117.4 trillion due to illicit investments during the period spanning 2011 to 2021 [32], underscoring the imperative of protecting victims in this domain. Article 4 of the "Consumer Protection Act" asserts that consumers affected by cybercrimes or other electronic transactions possess the right to reimbursement or compensation. Furthermore, Article 1 of "Law Number 31 of 2014" defines victims as individuals who endure economic, mental, or physical losses resulting from criminal activities [2]. Hence, in the realm of electronic investments, victims are more prone to experiencing economic setbacks.

4.2 Investment Law in Indonesia

The enactment of the "Investment Law No. 25 of 2007" occurred on April 26, 2007, in Indonesia. This law replaced "Law No. 6 of 1968" pertaining to domestic investment and "Law No. 1 of 1967" addressing foreign investment. Several factors contribute to the assessment of the ease of doing business (EoDB) within a country, encompassing fundamental regulations, decision implementation, and procedural efficacy. According to the 2019 EoDB report, Indonesia held the 73rd position in the rankings [33]. Hence, an observation has been made that the application of the Investment Law in Indonesia is not sufficiently effective in addressing investment disputes, underscoring the necessity for the development and implementation of an efficient regulatory framework in this domain. Consequently, investors encounter various issues while engaging in investments in Indonesia, encompassing concerns such as bankruptcy, money laundering, and related matters. To address these challenges, "Law Number 37 of 2004 concerning Bankruptcy and Postponement of Debt Payment Obligation" was introduced and implemented in Indonesia [33]. Likewise, additional anti-money laundering (AML) frameworks are advocated in Indonesia to establish a more secure environment for investors. However, the rigorous enforcement of diverse laws and regulations is deemed essential within the Indonesian context to foster electronic investments, thereby contributing to the nation's economic advancement [34].

4.3 Protection Against Crimes within Electronic Investment in Indonesia

Electronic investments in Indonesia are shown to comply with the stipulations of "Law No. 11 of 2008." In this context, Articles 1 and 2 of "Law No. 19 of 2016 Concerning Electronic Transactions and Information" (ETI) delineate the medium (internet) employed for electronic investments [19]. These investments share similarities with traditional investments, differing primarily in the medium employed for transactions. To safeguard individuals against crimes associated with electronic investments, Articles 9 and 10 of the Information and Electronic Transactions (ITE) law underscore the inclusion of terms certification and contract information from a "Reliability Certification Agency." In this context, Article 10 of the Electronic Transactions and Information (ETI) law states:

"The Reliability Certification Agency offers certification to any business entity that organizes Electronic Transactions. A government regulation specifies how the aforementioned *Reliability Certification Agency will be established."* [1]

In Indonesia, various laws and regulations are enforced to safeguard electronic transactions. However, specific attention to electronic investments is notably absent in "Investment Law No. 25 of 2007," "Law No. 11 of 2008," and their association with "Regulation No. 19 of 2016." [35], contrarily, the penal provisions outlined in the Indonesian Criminal Code (KUHP), specifically Article 378, establish criminal sanctions imposed by the government on individuals engaged in electronic investment fraud. Furthermore, embezzlement offenses, delineated in Article 372 of the KUHP, incur a fine of 900 rupiahs and a four-year imprisonment for the involved individuals. Hence, all instances of embezzlement must adhere to the stipulated criteria in Article 372 of the KUHP, encompassing:

- The participation of a legal entity or an individual as a legal entity
- Violation of the law.
- Possessing an item that is either partially or entirely owned by another party.
- Abstaining from engaging in criminal activities when having access to the corresponding assets [1].
    - Subjective elements are additionally delineated in Article 372 of the Indonesian Criminal Code (KUHP), as indicated below:
    - The element of intentionality centres on the error aspect within embezzlement. In this context, error encompasses two forms: negligence, also referred to as Culpos, and intentional, known as Dolus.
- Elements which are against the law, incorporating the forbidden nature of a particular act. It also includes two different types which are “against the formal law” (in contrast to written law) and “against the martial law” (in contrast to society’s legal principles) [1].
- Presently, investors are driven by the desire for rapid wealth accumulation, often resulting in diverse material losses, underscoring the importance of effective public awareness. Article 372 of the Indonesian Criminal Code (KUHP) explicitly delineates the criminal aspect in the realm of electronic investment fraud, prioritizing the protection of equivalent deposits to safeguard the investor or user. Consequently, "Law Number 8 of 1999" concerning consumer protection in Indonesia encompasses businesses, the responsibilities of economic entities, standard provisions, and actions prohibited by various authorities within the framework of consumer protection. Article 3 of this law specifically outlines crucial objectives for the protection of users, as enumerated below:
- Foster the capacity, consciousness, and autonomy of clientele.
- Augmenting self-esteem by averting inefficient access to services and commodities.
- Bestowing users with increased control over their rights.
- Formulating regulations that encompass openness and

legal precision.

- Cultivating a sense of responsibility and integrity within enterprises, while heightening stakeholder awareness regarding the significance of safeguarding consumer interests.
- Enhancing the procurement of tangible assets and guarantees for the security and safety of users [1].

Hence, it is noted that considerable attention is directed towards victim protection in the domain of electronic investments in Indonesia. Nevertheless, the advocacy for specific laws and regulations in this context is imperative to achieve substantive outcomes.

5. Conclusion

Electronic investments have significantly transformed the global corporate landscape, exerting influence on the overall economic trajectories of diverse nations. The proliferation of technological advancements and innovations has motivated numerous businesses to adopt electronic transactions, yielding both opportunities and challenges. While enhancing the overall investment milieu, electronic transactions have concurrently exposed vulnerabilities to various online crimes, encompassing illegal investments, electronic investment fraud, embezzlement, money laundering, and related offenses. These online crimes are prevalent challenges faced by investors in Indonesia. Consequently, diverse laws and regulations have been instituted in Indonesia to address these issues. Notably, the Investment Law and the ITE law are perceived as effective instruments in protecting victims against crimes perpetrated through electronic investments in Indonesia. Furthermore, Articles 372 and 378 of the KUHP prescribe distinct sanctions for electronic investment fraud and embezzlement within the Indonesian context. However, there remains a necessity to advance the development and implementation of a specific framework dedicated to victim protection against crimes associated with electronic investments in Indonesia, with the aim of achieving substantial outcomes.

6. Recommendations

To enhance victim protection against crimes masquerading as electronic investments in Indonesia, the following recommendations are suggested:

- Consider the formulation of a dedicated regulatory framework targeting crimes associated with electronic investments, serving as a deterrent for entities and relevant individuals involved in illegal investments and electronic fraudulent activities. Such an initiative can contribute to fostering a secure environment for electronic investments.
- Ensure the adherence of electronic investors and businesses to key laws and regulations, encompassing the ITE law, KUHP, investment laws, and other pertinent regulations, to cultivate a more transparent electronic investment environment. This measure aims to enhance the overall economic growth of the country.
- Furthermore, encourage the involvement of international organizations in shaping the legal framework for electronic investments. This strategy can prove effective in enhancing the overall legal framework and law enforcement in the realm of electronic investments. It is crucial to continually adapt the electronic investment environment to the evolving landscape of emerging technologies for this purpose.

7. Research Implications

The present juridical research possesses both practical and theoretical significance, contributing to its overall efficacy. Specifically, this study has proven instrumental in advancing the literature on victim protection within the sphere of electronic investments in Indonesia. It serves as a valuable resource for enhancing public awareness regarding the importance of law enforcement in electronic investments, ensuring the safety of investors and associated entities. Additionally, the research underscores the pivotal role played by investment law and the Electronic Transactions and Information (ETI) law in safeguarding individuals involved in electronic investments. The insights gleaned from this study may inspire future researchers to delve into other laws and regulations pertinent to electronic investments in Indonesia.

Furthermore, the research has the potential to motivate authorities to formulate and enact robust laws and regulations to protect investors and related stakeholders in the realm of electronic investments. Advocating for the development of a specific regulatory framework dedicated to victim protection against crimes associated with electronic investments in Indonesia is a noteworthy aspect that can lead to substantive outcomes. Additionally, the study identifies limitations within the existing regulatory framework pertaining to victim protection in electronic investment crimes, providing impetus for policymakers to address these deficiencies. This approach contributes to enhancing the effectiveness of the study, positioning it as a vital scholarly work in the domain of victim protection against electronic investment crimes.

8. Limitations and Future Research

This study is subject to several limitations. Its exclusive focus on Indonesia may constrain the generalizability of its findings to other contexts. Given that legal documents constitute the primary data source, practical nuances may be inadvertently overlooked. Variations in victim protection that transcend regional boundaries may exist, underscoring the necessity for cross-cultural research to enhance the study's global applicability. Furthermore, the study's restricted timeframe and the rapid evolution of the electronic investment landscape warrant consideration of longitudinal analyses in future research to capture dynamic changes over time. To bolster the study's robustness, cross-verification across multiple nations is recommended. This approach can uncover both context-specific and universal elements influencing victim protection. Additionally, employing quantitative methods in conjunction with triangulation is advocated to mitigate subjectivity associated with the interpretivist approach and achieve a more comprehensive understanding. Notably, the study relies solely on secondary qualitative data analysis due to the ease of data accessibility, which may impede an effective and real-time approach. Subsequent investigations may delve into the efficacy of specific legal measures and draw comparisons across various legal systems, contributing to a more comprehensive comprehension of victim protection in the rapidly evolving landscape of electronic investments.

References

[1] Deliani, Yusriana, S. Istiawati, and N. Elisa, "Criminal Actions Against Online Investment Fraud and Legal Protection Against Investors," *Russian Law Journal,* vol. 11, no. 4, pp. 316-320, 2023. [Online]. Available: https://www.russianlawjournal.org/index.php/journal/article/view/2388.

[2] A. Rahmawati, D. Sugihardana, F. B. Lestanto, N. N. Sha'adah, R. A. Faturohman, and T. R. Fauziah, "Cyber Crime Protection Law in Indonesia on the Risk of Loss of Binary Option," in *Proceeding International Conference Restructuring and Transforming Law*, 2022, pp. 47-55.

[3] T. Phan, C. DeMarino, F. Kashanchi, Y. Kuang, D. Anderson, and M. Emelianenko, "Characterizing Transcriptional Dynamics of HIV-1 in T-cells and Macrophages Using a Three-State LTR Model," *Letters in Biomathematics,* vol. 8, no. 1, pp. 133-150, 2021, doi: https://doi.org/10.30707/LiB8.1.1647878866.063128.

[4] Y. Firmansyah, I. Haryanto, T. A. Purnama, and E. Destra, "Compensation for Fraud (Gambling) Operations Under The Guise of Investment-Restitution as a Complex or Easy Way Out Mechanism?(Learning from Various Restitution and Law Cases in Indonesia)," *East Asian Journal of Multidisciplinary Research,* vol. 1, no. 3, pp. 545-572, 2022, doi: https://doi.org/10.55927/eajmr.v1i3.280.
[5] Z. Mukarromah, "Forex Online Tranding (FOT) Dalam Perspektif Hukum Ekonomi Islam (Telaah Kasus Para Pengguna FOT)," *At-Turost: Journal of Islamic Studies,* vol. 7, no. 1, pp. 54-72, 2020, doi: https://doi.org/10.52491/at.v7i1.38.
[6] A. Pratami, N. Feriyanto, J. Sriyana, and I. Pratama, "Are Shariah Banking Financing patterns pro-cyclical? An Evidence from ASEAN Countries," *Cuadernos de Economía,* vol. 45, no. 127, pp. 82-91, 2022. [Online]. Available: https://cude.es/submit-a-manuscript/index.php/CUDE/article/view/222.
[7] M. Azmi, "Transaksi Jual Beli Foreign Exchange Secara Online Perspektif Hukum Islam," *Jurnal Syariah dan Hukum,* vol. 2, no. 02, pp. 117-127, 2020, doi: https://doi.org/10.35961/teraju.v2i02.157.
[8] D. Atrizka, H. Lubis, C. W. Simanjuntak, and I. Pratama, "Ensuring Better Affective Commitment and Organizational Citizenship Behavior through Talent Management and Psychological Contract Fulfillment: An Empirical Study of Indonesia Pharmaceutical Sector," *Systematic Reviews in Pharmacy,* vol. 11, no. 1, pp. 545-553, 2020, doi: http://dx.doi.org/10.5530/srp.2019.2.04.
[9] W. Setyowati, R. Widayanti, and D. Supriyanti, "Implementation of E-Business Information System in Indonesia: Prospects and Challenges," *International Journal of Cyber and IT Service Management,* vol. 1, no. 2, pp. 180-188, 2021, doi: https://doi.org/10.34306/ijcitsm.v1i2.49.
[10] H. LubÍS, M. D. Kumar, P. Ikbar, and S. Muneer, "Role of psychological factors in individuals investment decisions," *International Journal of Economics and Financial Issues,* vol. 5, no. 1, pp. 397-405, 2015. [Online]. Available: https://dergipark.org.tr/en/pub/ijefi/issue/31972/352310.
[11] D.-R. Kong and T.-C. Lin, "Alternative investments in the Fintech era: The risk and return of Non-Fungible Token (NFT)," *Available at SSRN 3914085,* 2021, doi: https://dx.doi.org/10.2139/ssrn.3914085.
[12] T. Adrian and T. Mancini-Griffoli, "The Rise of Digital Money," *Annual Review of Financial Economics,* vol. 13, no. 1, pp. 57-77, 2021, doi: https://doi.org/10.1146/annurev-financial-101620-063859.
[13] R. Li and Y. Gao, "Research on Agricultural Enterprise Accounting Information Resource Sharing Model Based On Big Data Technology," *Journal of Commercial Biotechnology,* vol. 27, no. 1, 2022, doi: https://doi.org/10.5912/jcb1043.
[14] E. Susilawati, H. Lubis, S. Kesuma, and I. Pratama, "Antecedents of Student Character in Higher Education: The role of the Automated Short Essay Scoring (ASES) digital technology-based assessment model," *Eurasian Journal of Educational Research,* vol. 98, no. 98, pp. 203-220, 2022. [Online]. Available: https://ejer.com.tr/manuscript/index.php/journal/article/view/708.
[15] H. Jiang and J. P. Murmann, "The Rise of China's Digital Economy: An Overview," *Management and Organization Review,* vol. 18, no. 4, pp. 790-802, 2022, doi: https://doi.org/10.1017/mor.2022.32.
[16] C. W. Utami, A. T. L. Indrianto, and I. Pratama, "Agricultural Technology Adoption in Indonesia: The Role of the Agriculture Extension Service, the Rural Financing and the Institutional Context of the Lender," *International Journal of Innovation, Creativity and Change,* vol. 7, no. 7, pp. 258-276, 2019. [Online]. Available: https://www.ijicc.net/images/vol7iss7/7719_Utami_2019_E_R.pdf.
[17] X. Liu *et al.*, "Cyber security threats: A never-ending challenge for e-commerce," *Frontiers in Psychology,* vol. 13, p. 927398, 2022, doi: https://doi.org/10.3389/fpsyg.2022.927398.
[18] M. Kianpour, S. J. Kowalski, and H. Øverby, "Systematically Understanding Cybersecurity Economics: A Survey," *Sustainability,* vol. 13, no. 24, p. 13677, 2021, doi: https://doi.org/10.3390/su132413677.
[19] S. Harefa, "Criminal Law Protection On Online Victims Of Victims," *Veteran Law Review,* vol. 2, no. 1, pp. 33-45, 2019, doi: https://doi.org/10.35586/velrev.v2i1.690.
[20] T. Y. Rahmanto, "Penegakan Hukum terhadap Tindak Pidana Penipuan Berbasis Transaksi Elektronik," *Jurnal Penelitian Hukum De Jure,* vol. 19, no. 1, pp. 31-52, 2019, doi: http://dx.doi.org/10.30641/dejure.2019.V19.31-52.
[21] H. N. Alkhaldi, "Legal Challenges of E-commerce in Kuwait during the COVID-19 Pandemic," *Kilaw Journal,* vol. 8, no. 6, pp. 125-144, 2020. [Online]. Available: https://journal.kilaw.edu.kw/wp-content/uploads/2020/07/125-144-Hebah-Nassar-Alkhaldi.pdf.
[22] H. Fathul and F. Ana, "The Urgency of Legal Protection for Online Loan Service Users," in *Proceedings of the 2nd International Conference on Law and Human Rights 2021 (ICLHR 2021)*: Atlantis Press, 2021, pp. 215-221.
[23] A. M. Bossler, T. J. Holt, C. Cross, and G. W. Burruss, "Policing fraud in England and Wales: examining constables' and sergeants' online fraud preparedness," *Security Journal,* vol. 33, no. 2, pp. 311-328, 2020, doi: https://doi.org/10.1057/s41284-019-00187-5.
[24] P. Koutroumpis, F. Ravasan, and T. Tarannum, "(Under) Investment in Cyber Skills and Data Protection Enforcement: Evidence from Activity Logs of the UK Information Commissioner's Office," *Available at SSRN 4179601,* 2022, doi: https://dx.doi.org/10.2139/ssrn.4179601.
[25] S. Zhang, "Protection of Cross-Border Data Flows Under International Investment Law," in *Handbook of International Investment Law and Policy*, J. Chaisse, L. Choukroune, and S. Jusoh Eds.: Springer Singapore, 2020, pp. 1-23.
[26] M. Safan, "Controllability of Infections in SIR Models with Waned Childhood Vaccination-Induced Immunity and Booster Vaccination," *Letters in Biomathematics,* vol. 8, no. 1, pp. 119-131, 2021, doi: https://doi.org/10.30707/LiB8.1.1647878866.053027.
[27] S. P. Shatz and P. J. Lysobey, "Update on the California Consumer Privacy Act and Other States' Actions," *The Business Lawyer,* vol. 77, pp. 539-547, 2022. [Online]. Available: https://www.mcglinchey.com/wp-content/uploads/2022/04/011-ABA-TBL-77-2-Shatz_Lysobey.pdf.
[28] D. K. Yusup, "Law enforcement efforts for illegal online investment entities in Indonesia," *Baltic Journal of Law & Politics,* vol. 15, no. 2, pp. 890-904, 2022, doi: https://doi.org/10.2478/bjlp-2022-001054.
[29] M. Junjie and M. Yingxin, "The Discussions of Positivism and Interpretivism," *Global Academic Journal of Humanities and Social Sciences,* vol. 4, no. 1, pp. 10-14, 2022, doi: https://doi.org/10.36348/gajhss.2022.v04i01.002.
[30] M. Q. N. Arifin and S. Oktavilia, "Analysis the use of electronic money in Indonesia," *Economics Development Analysis Journal,* vol. 9, no. 4, pp. 361-373, 2020, doi: https://doi.org/10.15294/edaj.v9i4.39934.
[31] Statista. "Digital Investment - Indonesia." Statista Market Insights. https://www.statista.com/outlook/fmo/wealth-management/digital-investment/indonesia (accessed.
[32] W. Santoso, "The Rights of Victims of Illegal Investment Crimes Against Confiscated Goods," *Unnes Law Journal,* vol. 8, no. 2, pp. 355-376, 2022, doi: https://doi.org/10.15294/ulj.v8i2.56587.
[33] T. A. Purnama, Y. Firmansyah, A. M. T. Anggraini, E. R. Gultom, and I. Hartanto, "The Urgence of Renewal Investment Law and Investment Dispute Settlement in Indonesia," *Jurnal Riset Rumpun Ilmu Sosial, Politik dan Humaniora,* vol. 1, no. 2, pp. 104-118, 2022, doi: https://doi.org/10.55606/jurrish.v1i2.403.
[34] W. Wang and Y. Wang, "Research on image capture technology of intelligent terminal and multi exposure fusion to improve the resilience of agriculture production systems," *Journal of Commercial Biotechnology,* vol. 27, no. 2, 2022, doi: https://doi.org/10.5912/jcb1045.
[35] A. K. Jaelani and R. D. Luthviati, "The Crime Of Damage After the Constitutional Court's Decision Number 76/PUU-XV/2017," *Journal of Human Rights, Culture and Legal System,* vol. 1, no. 1, pp. 31-42, 2021, doi: https://doi.org/10.53955/jhcls.v1i1.5.