International Conference Restructuring and Transforming Law 2026
Volume 5, Issue 1, July 2026
e-ISSN :2963-931X
icrtlaw@ums.ac.id

Legal Protection of Retail Investors' Personal Data in The Digital Stock Trading Ecosystem: A Case Study of Stockbit Indonesia

Naufal Sheva Alfauzi

Law Science, Faculty of Law and Politic Science, Universitas Muhammadiyah Surakarta

C100220051@student.ums.ac.id

Wardah Yuspin,S.H.,M.Kn.,Ph.D.

Law Science, Faculty of Law and Politic Science, Universitas Muhammadiyah Surakarta

wy204@ums.ac.id

Abstract

The digital transformation of the capital market through securities companies like Stockbit has broadened retail investor access, but it also poses risks to personal data protection. This research uses a normative legal method with a statutory approach, referring to Law Number 27 of 2022 concerning Personal Data Protection and supported by secondary and tertiary legal materials. The results of this study indicate that although a legal framework governing data protection obligations exists, its implementation is not optimal, as reflected in the case of system disruptions and administrative sanctions against PT Stockbit Sekuritas Digital. The effectiveness of investor personal data protection depends heavily on the consistent implementation of legal obligations, strengthened oversight, and increased accountability of digital investment platform providers.

Keywords: Personal Data Protection, Retail Investors, Stock Transactions

Abstract

Digital transformation in the capital market through securities firms such as Stockbit has expanded access for retail investors, but at the same time poses risks to personal data protection. This study employs a normative legal method with a legislative approach, referencing Law No. 27 of 2022 on Personal Data Protection and supported by secondary and tertiary legal sources. The results of this study indicate that although a legal framework regulating data protection obligations already exists, its implementation has not been optimal, as reflected in the case of system disruptions and administrative sanctions against PT Stockbit Sekuritas Digital. The effectiveness of investor personal data protection is highly dependent on the consistent application of legal obligations, strengthened oversight, and enhanced accountability of digital investment platform operators.

Keywords: Personal Data Protection, Retail Investors, Stock Transactions

International Conference Restructuring and Transforming Law 2026
Volume 5, Issue 1, July 2026
e-ISSN :2963-931X
icrtlaw@ums.ac.id

INTRODUCTION

Digital transformation has fundamentally changed the landscape of Indonesia's capital markets, particularly in how people access and engage in investment activities. The integration of financial technology through fintech innovation has opened broader access for the public, including new investors, to investment instruments that were previously difficult to access. This digitalization not only streamlines transactions but also simplifies the entire investment process, from registration and product selection to routine portfolio monitoring. The emergence of digital investment platforms, such as Stockbit, signals a shift in the relationship between investors and the market, which now prioritizes ease of access and speed of information. (1)

This innovation makes it easier for people to access various financial services more quickly, efficiently, and simply, without the hassle of conventional procedures that often take a long time. One sector that has grown rapidly thanks to digitalization is the capital market, particularly stock investment by the general public. The development of the digital world in the capital market has encouraged the emergence of app-based investment platforms, which enable online stock transactions. Through these apps, the public and investors can open securities accounts, monitor stock price movements, analyze the market, and buy and sell shares directly via smartphone or gadget. This easy access ultimately encourages greater public participation in the capital market, especially retail investors who previously had difficulty obtaining investment information and facilities through digital investment applications. The public and investors can now open securities accounts, monitor stock prices, conduct market analysis, and buy and sell shares directly using only a smartphone or gadget. This convenience ultimately encourages wider public participation in the capital market, especially retail investors who previously had difficulty accessing investment information and facilities. (2)

One of the digital investment applications well-known among retail investors in Indonesia is Stockbit. This application functions as a platform for investing in stocks connected to securities companies and allows investors to conduct stock transactions online using electronic devices. Through this application, users can carry out various investment activities, including opening a stock account, monitoring stock price fluctuations, analyzing stocks, and conducting stock transactions directly via the internet. The facilities and efficiency offered make Stockbit a priority choice for people managing their stock investments. (3)

The use of digital-based investment platforms creates issues related to system security and the protection of users' personal information. In practice, investors are required to provide sensitive data, such as identity cards, national identification numbers, bank account information, and financial transaction data during the Customer Fund Account (RDN) opening and verification process. The characteristics of this data indicate that it is highly vulnerable if not protected by an appropriate security system. This issue is not merely theoretical; it has also occurred in practice on the Stockbit platform in Indonesia. On November 7, 2025, the Stockbit application experienced an error during the market opening on the Indonesia Stock Exchange, disrupting user transaction activity and generating complaints from investors who lost market opportunities. The resulting wave of user protests indicated dissatisfaction with the quality of service and system reliability provided by the Stockbit platform. This prompted some investors to demand compensation or a clear explanation of the cause of the system disruption. In fact, some responses indicated that users were considering reporting the issue to the Indonesian Consumers Foundation (YLKI) as an effort to protect consumer rights, given the potential financial losses that could result from transaction failures during market activity. This phenomenon shows that system problems in digital investment platforms not only affect technical aspects, but also have legal consequences and public trust. Losses experienced by investors, especially in the form of lost transaction opportunities, can be considered material losses that can trigger lawsuits if not handled properly by platform managers. On the other hand, the lack of clarity of information and slow responses from service providers can also worsen the views of users, resulting in a decrease in the level of trust in the digital investment system as a whole. (4) In addition, Stockbit also officially warns of various fraudulent methods that use the name of its platform, such as phishing and identity theft, which can lead to data breaches and financial losses for users. This reality shows that risks in the digital investment ecosystem are not only related to data confidentiality, but also include system resilience and external threats.(5)

The risks to the security of personal information on digital platforms cannot be ignored, especially with the increasing threat of cybercrime such as hacking, data theft, and misuse of information by irresponsible parties. Losses experienced by Stockbit users due to leaks or misuse of personal data can be classified into two main categories, namely material and non-material losses. Material losses include loss of funds due to unauthorized access to investment accounts or account hacking, misuse of identity for financial transactions, and the risk of fraud that exploits personal information. Conversely, non-material losses include disruption of security, loss of privacy, and decreased trust in digital investment platforms. These non-material losses also have legal implications, because they violate the right to privacy as part of human rights. If investors' personal data is not managed and protected properly, this has the potential to cause losses in both material and non-material forms, and can reduce public trust in the digital investment system. In the Indonesian legal system, protection for investors, including the protection of their data and information, is regulated in Law Number 27 of 2022 concerning Personal Data Protection. (6) The Capital Market provides a legal basis for the implementation of a transparent, orderly, and fair capital market. One of the important foundations of this provision is the principle of information transparency, which requires all parties involved in capital market activities to convey data accurately, clearly, and in a timely manner to investors.(7) This principle aims to provide legal protection to investors so that they can make logical investment decisions based on valid information. In addition, supervision of capital market activities is also carried out by the Financial Services Authority (OJK), which has the authority to regulate and supervise all activities in the financial sector. The OJK plays a crucial role in ensuring transparency and accountability in capital market investments, while protecting the interests of consumers and the public. Through its issued regulations, the OJK continues to strengthen investor protection, including supervision of securities companies and digital investment service providers.(8)

Thus, various challenges related to system security and investor protection in digital investment applications remain real in practice. This is reflected in the administrative sanction in the form of a written warning issued by the Indonesia Stock Exchange (IDX) to PT Stockbit Sekuritas Digital. Based on the audit results, the company was deemed to have not fully complied with the provisions related to the Direct Order Facility Guidelines and automated ordering, and have not consistently implemented operational information technology governance. These findings indicate that compliance with information technology standards and electronic system management remains a challenge for digital investment platform providers. This condition also confirms that the aspect of investor protection is not only related to the availability of regulations, but also to the technical implementation and operational compliance carried out by business actors in the capital market sector. (9) This condition has the potential to create a threat of loss for investors if not immediately addressed. This incident shows that although digital investment platforms offer various conveniences for investors, there are still risks related to system security, protection of personal information, and investor interests, therefore, a strong legal protection system is very necessary to guarantee the security and confidentiality of users' personal information in technology-based investment services. (10)

Basically, Indonesian law, attention to Personal Data Protection is regulated through various regulations, including Law Number 27 of 2022 concerning Personal Data Protection. This regulation serves as the legal basis for protecting people's personal data in various data processing activities, including digital financial services. Digital investment platform providers are legally responsible for ensuring that the processing of users' personal data is carried out safely, transparently, and in accordance with applicable regulations. (11) Thus, the importance of this research is rooted in the need to ensure legal protection for the personal data of retail investors, who are the most vulnerable group in the digital stock trading environment. The personal data provided, such as resident identity and financial details, has the potential to be misused if not managed securely, thus causing both material and immaterial losses, including the threat of identity theft and misuse of funds. Therefore, personal data protection is crucial to protect investors' privacy rights, as well as to maintain public trust in the capital market system. The selection of Stockbit as the object of this research is based on real considerations and normative relevance. As one of the digital investment platforms with many users in Indonesia and connected to an official securities company, Stockbit reflects the real practice of technology-based stock trading in the capital market ecosystem. Its existence reflects the digital shift in investment services, which requires high compliance standards, particularly in information technology and data protection. Furthermore, the discovery of administrative sanctions in the form of a warning letter from the Indonesia Stock Exchange to PT Stockbit Sekuritas Digital indicates a real problem with compliance with applicable regulations. This situation demonstrates that, despite the existing legal framework, its implementation in the field still faces various challenges. Novelty in this study is based on a research approach that emphasizes that the problem of personal data protection in the digital world is not only caused by the absence of legal norms, but also by the weak implementation and level of compliance of digital securities companies with applicable information technology standards and regulations. In this context, the study does not only focus on normative aspects, but also links them to the reality of practices that occur in the field. More specifically, this study uses Stockbit as a case study to examine the relationship between system disruptions, potential data security risks, and the form of legal responsibility of platform organizers. This analysis is important because it places the issue of data protection in a more comprehensive framework, namely as part of digital stock trading governance in Indonesia which demands accountability, system reliability, and protection of investor interests. (12)

Based on this background, this study aims to evaluate the existing forms of legal protection for retail investors' personal data in stock transactions through the Stockbit application and identify how protection mechanisms are implemented to maintain the security of users' personal data.

METHOD

This research is a normative legal study that focuses on examining legal norms related to personal data protection. The approach used includes a statutory approach to examine the applicable legal provisions and conceptual approaches to understand the principles of data protection and legal responsibilities in a digital context. The legal materials used consist of primary legal materials in the form of Law Number 27 of 2022 concerning Personal Data Protection and Law Number 8 of 1995 concerning Capital Markets.

Secondary legal materials include books, scientific articles, and relevant legal literature, while tertiary legal materials are used as supporting materials, such as legal dictionaries and other reference sources. All of these legal materials are analyzed qualitatively using normative analysis methods to obtain systematic conclusions. (13)

RESULTS AND DISCUSSION

1. Protecting Retail Investors' Personal Data in Stock Transactions Through the Stockbit Application

In practice, the use of stock trading applications such as Stockbit not only provides easy access, but also places retail investors in a vulnerable position to system security risks and personal data management. This vulnerability arises because all transaction activities are conducted through electronic systems that depend on the reliability of information technology and data governance by the platform provider. Every process, from registration to transaction execution, involves the processing of sensitive personal data. This situation shows that the issue of personal information protection cannot be separated from overall system security. There are risks that arise not only limited to data leaks, but also the possibility of improper use of information that can be detrimental to retail investors. (14)

In the context of stock trading that takes place through online platforms, investor personal data is of particular importance and requires legal protection. In general, investor personal information consists of user identity details such as full name, identity number, address, telephone number, email, and financial information related to their investment activities. (15) This data is considered sensitive because it is closely related to a person's identity and financial condition, so it can cause losses if it falls into the hands of irresponsible people. The case that occurred at Stockbit was not only a system disruption at market opening, but also has the potential for broader risks in the digital world, such as vulnerability to cyber attacks, phishing, and misuse of user identities. The relevance of this case to the issue of personal data protection lies in the direct link between system disruptions, weaknesses in information technology security, and the potential for unauthorized access to user data. Thus, this case is not only a technical issue, but also has a legal dimension related to the responsibility of electronic system providers in protecting investor personal data. Efforts to protect personal data in electronic systems are actually an obligation for every system provider that manages user data (16). In the case of digital investment platforms, application providers have a responsibility to ensure that investors' personal data is managed securely and not misused by other parties. This is in line with the principles of personal data protection which underscore the importance of supervision of the collection, processing, storage, and use of personal data by authorized parties. (17) The Stockbit application, as a platform for digital stock trading, has a responsibility to implement an information security system for each of its users that is sufficient to protect personal data. This protection is implemented through various digital security mechanisms designed to prevent unauthorized access to the system and user data. The implementation of a data security system is a crucial aspect in the provision of digital services, because it plays a role in protecting the confidentiality, integrity, and accessibility of data processed by the system. In daily practice, the protection of personal information on digital platforms is carried out through various technical and managerial methods aimed at minimizing the risk of data leakage. Some of these methods include the use of encryption systems for data, the implementation of user verification systems, and regulating access to information systems.

By implementing this strategy, platform providers strive to ensure that users' personal information can only be accessed by authorized individuals. Furthermore, protection of personal data is related to the information management policies implemented by service providers. These policies are generally structured in a privacy document that explains how service providers collect, utilize, store, and protect users' personal data. (18) Privacy documents are an important tool for providing clarity to users about how their personal data is managed within the digital ecosystem. From a legal perspective, the protection of personal data for individuals investing in digital platforms is closely related to the responsibility of electronic system providers to maintain the security of the information systems they manage. Platform managers are obligated to ensure that the systems they use meet the necessary security criteria to protect user data from various cyber threat risks, such as hacking, information theft, and data misuse. (19)

Threats to cybersecurity are a major risk in the provision of digital services. Cyberattacks can occur in various ways, such as attempts to hack systems, information theft through malware, and exploiting information system weaknesses. Therefore, digital investment platform providers are required to consistently assess and strengthen existing security systems to address various potential threats that could harm users. Protecting investors' personal information is also related to the principle of prudence in electronic system management. Platform providers must ensure that all processes related to the processing of personal data are carried out responsibly and in accordance with applicable laws and regulations. This principle of prudence includes the obligation to maintain the confidentiality of user information, prevent data misuse, and take necessary action in the event of a system security breach. Therefore, protecting retail investors' personal data in stock transactions through the Stockbit application is a crucial element in providing safe and reliable digital investment services. This protection relates not only to the technical aspects of system security but also encompasses the legal aspects that govern the platform provider's responsibilities in managing users' personal data. (11)

2. Platform Operators' Legal Responsibilities for Investors' Personal Data

In the context of personal data protection, the legal responsibility of platform operators cannot be understood solely from a conceptual perspective but must also be examined through its practical implementation. In the case of PT Stockbit Sekuritas Digital, the Indonesia Stock Exchange (IDX) imposed an administrative sanction in the form of a written warning due to the company's failure to fully comply with the Automated Ordering Direct Order Facility Guidelines. In addition, the company was found to have inconsistently implemented information technology governance, including the Brokerage Office Front-End Information System (BOFIS) and internal control mechanisms. This sanction is included in the type of administrative sanctions that are applied because the company is deemed to have not fulfilled the requirements related to the information technology system and operational management on an ongoing basis.

Legally, a written warning has several impacts. First, this sanction becomes a record of compliance for the company, which can influence the regulator's assessment of the company's performance and governance in the future. Second, the warning is an early warning that if not followed up can lead to more severe sanctions, such as administrative fines, restrictions on business activities, and even license suspension. Third, from a non-legal perspective, this sanction has the potential to reduce investor confidence, especially regarding system reliability and data security on the platform. This sanction shows that the legal responsibility of the platform organizer includes the obligation to ensure system reliability and the security of user data management. (20) These findings indicate that the legal responsibility of the platform organizer does not stop at providing services, but includes the obligation to ensure that the electronic system operates according to established security and governance standards. Within this framework, preventive responsibility is reflected in the obligation to build a reliable information security system, including access control and system monitoring. Meanwhile, repressive responsibility arises when violations occur, which requires corrective action and remediation to protect investor interests. (21)

The legal responsibility of platform providers is closely related to the principle of accountability in electronic system management. This principle emphasizes that electronic system providers are required to be accountable for every data processing activity carried out within the systems they operate. Therefore, platform providers must establish efficient internal oversight mechanisms to ensure that all data processing is carried out in accordance with established guidelines. Indeed, breaches of personal data security can have various negative impacts on users. Leaks of individual information can trigger data misuse by irresponsible parties, such as fraud, identity theft, and various other types of cybercrime.(22)

In the event of a personal data breach, Stockbit app users have the right to report the breach to the company and to the relevant authorities, such as the Financial Services Authority (OJK) and agencies overseeing personal data protection. Under Law Number 27 of 2022 concerning Personal Data Protection, data controllers are required to notify data subjects in the event of a failure to protect personal data. Investors can also pursue legal action through administrative, civil, or criminal mechanisms, depending on the severity of the breach. These mechanisms demonstrate that the legal system provides a means of protection, although their effectiveness depends heavily on implementation and awareness among the parties. In this context, personal data protection is a crucial aspect in maintaining public trust in digital platforms, particularly the Stockbit app. In the event of a data breach, platform providers are obligated to immediately take mitigation measures to limit the impact, including handling security incidents, system recovery, and providing information to affected parties. This obligation demonstrates the provider's legal responsibility for managing electronic systems. Furthermore, the Indonesia Stock Exchange and the Financial Services Authority (OJK) play a crucial role through their oversight and compliance enforcement functions, ensuring that digital investment service providers comply with data protection obligations in accordance with applicable law.

In the context of the capital market in Indonesia, investor protection is not only the responsibility of securities companies or digital investment service providers, but also involves capital market regulatory institutions, one of which is the Indonesia Stock Exchange (IDX) which is also an entity that manages and provides systems and facilities for securities transactions, playing an important role in ensuring that all stock trading activities take place in an orderly, fair, transparent and efficient manner, including in managing the security of data and information owned by investors who use digital platforms such as Stockbit. (8) The IDX's obligation to protect investor data is basically carried out through supervision, regulation of trading systems, and implementation of information technology standards that must be complied with by securities companies and providers of electronic securities trading systems.

In practice, the Stockbit app functions as an investment platform connected to an authorized securities company, so all transactions conducted through the app remain under the supervision of the trading system operated by the IDX.The implementation of Two-Step Verification (2FA) through the Trusted Device feature enhances the security of user accounts and contributes to strengthening the Indonesian capital market ecosystem. This layered authentication model adopts a defense-in-depth framework by combining knowledge-based verification (passwords), possession-based authentication (trading PIN), and time-sensitive verification (OTP). These complementary security mechanisms work together to mitigate the risk of data breaches and unauthorized access. Moreover, the implementation of similar authentication systems on comparable platforms has been shown to significantly reduce the incidence of account takeover attacks. (23) The synergy among the OJK, the Indonesia Stock Exchange (IDX), and the Stockbit application is consistent with the principles of *principles-based regulation* as stipulated in POJK No. 77/POJK.01/2016 and Article 17 of POJK No. 13/POJK.02/2018. This synergy ensures a balance between digital innovation and consumer protection while supporting the IDX's mandate to maintain a secure, fair, and efficient capital market. While effective, the implementation of OTP-based authentication remains vulnerable to threats such as SIM swapping and phishing attacks. Therefore, these risks must be mitigated through secure communication channels, including the use of the WhatsApp Business API with end-to-end encryption. Furthermore, the scalability of this feature is crucial in responding to the rapid growth of post-pandemic digital transactions. As a result, the *Trusted Device* model may serve as a best practice that can be replicated by other financial intermediaries, with future potential for integration with biometric authentication technologies in line with the OJK's digital transformation roadmap. (24)

Furthermore, the Indonesia Stock Exchange (IDX) has the authority to oversee the compliance of securities companies. In practice, this authority is not merely normative but has also been exercised through concrete regulatory actions. One such example is the administrative sanction imposed by the Indonesia Stock Exchange (IDX) on PT Stockbit Sekuritas Digital in the form of a written warning for its failure to fully comply with the provisions governing the Automated Ordering Direct Order Facility. Additionally, the company was found to have inconsistently implemented operational information technology governance standards. The imposition of these sanctions is a commitment that BEI supervision includes technical aspects, especially in the management of information technology systems that are directly related to the security of transactions and investor data. In the context of personal data protection, securities companies have an obligation to implement security systems such as encryption, network security, and access restrictions as part of the standards that must be met by exchange members. Thus, BEI's action against Stockbit is not only administrative, but also functions as a compliance enforcement mechanism to ensure the reliability of the trading system and protect investor interests. (9) The purpose of this supervisory system is to ensure that securities companies and digital investment platforms function in accordance with existing regulations and maintain a secure trading system. The role of the Indonesia Stock Exchange in maintaining the security of the digital trading system can also be seen from the supervisory actions and enforcement of regulations against investment platforms that are deemed not to have fully complied with operational provisions. This step shows that the Indonesia Stock Exchange plays an active role in maintaining the integrity of the trading system and protecting the interests of investors. In addition to supervising the trading system, BEI also plays a role in increasing literacy and education to the public regarding safe investments in the capital market. Through a series of educational and outreach initiatives, the IDX encourages investors to recognize the potential risks of digital investment, as well as understand the importance of protecting their accounts and safeguarding personal information when using investment applications.(8)

Supervision by authorities is not merely normative but is carried out through structured procedures. The Indonesia Stock Exchange and the Financial Services Authority (OJK) implement supervision through routine inspections, audits of information technology systems, and assessments of the implementation of operational standards, which include system security and data management. In this case, violations of personal data not only give rise to administrative and civil liability but can also be categorized as criminal. If personal data is illegally used to access accounts or conduct transactions without consent, such actions can be categorized as a crime as stipulated in the provisions concerning illegal access to electronic systems. This demonstrates that personal data protection has a broad legal dimension, encompassing preventive, repressive, and penal aspects. In this case, authorities can impose administrative sanctions in stages, ranging from written warnings and fines to restrictions on business activities. Furthermore, platform operators are also required to report security incidents, implement system improvements, and enhance internal controls as a follow-up to supervisory findings.

Thus, the legal responsibility of platform operators does not stop at normative obligations, but includes concrete obligations to ensure the company implements legal compliance to protect data through the implementation of protection systems, periodic evaluations, and compliance with the results of authority supervision. This obligation is in line with Law Number 27 of 2022 concerning Personal Data Protection, which requires data controllers to guarantee data security and confidentiality, and Law Number 8 of 1995 concerning Capital Markets, which emphasizes investor protection and information transparency. In practice, procedures that must be carried out include the implementation of security systems such as layered encryption and authentication, data access restrictions, periodic system audits and evaluations, and incident reporting to authorities in the event of disruptions or violations. In addition, securities companies, in this case Stockbit, are required to handle any problems by quickly restoring the system and providing clear information to users regarding the problems that occur. This shows that the protection of investors' personal data depends not only on the existence of regulations, but also on the consistent implementation of procedures at each securities company regarding compliance with applicable legal standards. (21)

CLOSING

Based on the research results, the protection of retail investors' personal data in stock transactions through digital platforms has not been fully implemented optimally. A case involving the securities company PT Stockbit Sekuritas Digital resulted in administrative sanctions from the Indonesia Stock Exchange (IDX) despite being regulated by Law Number 27 of 2022 concerning Personal Data Protection. The analysis indicates that the legal responsibilities of securities companies, including PT Stockbit Sekuritas Digital, encompass both preventive and repressive obligations. Preventive responsibilities involve the implementation of robust security measures and effective personal data management systems, while repressive responsibilities relate to the handling of data security incidents, including response, mitigation, and accountability measures. However, these obligations have not been fully implemented consistently, particularly in the application of information technology standards. This is evidenced by the written warning sanction issued by the Indonesia Stock Exchange to PT Stockbit Sekuritas Digital. Therefore, this study confirms that the effectiveness of protecting retail investors' personal data in the digital stock trading ecosystem, in this case through PT Stockbit Sekuritas Digital, depends not only on the existence of regulations, but primarily on the consistency of legal compliance implementation, the level of commitment of platform providers, and the effectiveness of oversight by authorities. Therefore, strengthening aspects of law enforcement and information technology governance are key to ensuring the security of investors' personal data.

BIBLIOGRAPHY

1. Teknologi Dalam Transformasi Ekonomi Dan Bisnis Di Era Digital P, Khairi M, Rianto B, Jalil M, Juita H, Sudeska E, Et Al. Pengaruh Teknologi Dalam Transformasi Ekonomi Dan Bisnis Di Era Digital. 2025.
2. Anugrah M, Syahid Mn, Sahri, Azka Fm, Anwar Ms. Tantangan Hukum Dan Peran Pemerintah Dalam Pembangunan E-Commerce Di Indonesia. Jurnal Hukum Dan Ham Wara Sains. 2023 May 31;2(05):421–38. Doi:10.58812/Jhhws.V2i05.354
3. Kurniawan D, & Rma. Stockbit: Transformasi Cara Berinvestasi Bagi Generasi Digital. Khoerunisa, Editor. Bogor: Afdan Rojabi ; 2026.
4. Apriansyah N. Perlindungan Hukum Bagi Investor Dalam Transaksi Saham Pada Aplikasi Stockbit Di Indonesia. Nicko Apriansyah Jurnal Jejak Hukum Indonesia (Jhi). 2025.
5. Syakirah S, Sayyidah H. Urgensi Penguatan Implementasi Terkait Perlindungan Data Pribadi Bagi Pemodal Sektor Jasa Keuangan Equity Crowdfunding Di Indonesia (Studi Komparasi Terhadap Negara Malaysia). Padjadjaran Law Review. 2024 Jun 28;12(1). Doi:10.56895/Plr.V12i1.1410
6. Hermanto D, Lie G. Media Hukum Indonesia (Mhi) Published By Yayasan Daarul Huda Krueng Mane Perlindungan Hukum Bagi Investor Berdasarkan Undang-Undang Pasar Modal Di Era Digital Dalam Transaksi Reksa Dana [Internet]. Vol. 3. 2025;3(4):48–53. Doi:10.5281/Zenodo.17193978
7. Gusti Agung Wisudawan I, Sutrisno B, Ade Mulada D. Optimasi Pengawasan Oleh Otoritas Jasa Keuangan Di Bidang Pasar Modal Menurut Hukum Positif Di Indonesia

[Internet]. 2021. Available From: Http://Journal.Unmasmataram.Ac.Id/Index.Php/Gara
8. Bursa Efek Indonesia. Pengumuman Sanksi Teguran Tertulis Kepada Pt Stockbit Sekuritas Digital No. Peng-00030/Bei.Ang/10-2022. Jakarta; 2022.
9. Ramadhan Nr, Alvito Hr, Matondang Ti, Nugroho Aa. Socius: Jurnal Penelitian Ilmu-Ilmu Sosial Pengaturan Umum Mengenai Investasi Serta Keuangan Elektronik Dalam Hukum Teknologi Dan Informasi [Internet]. Vol. 1. 2024;1. Doi:10.5281/Zenodo.12147717
10. Apriansyah N. Perlindungan Hukum Bagi Investor Dalam Transaksi Saham Pada Aplikasi Stockbit Di Indonesia. Nicko Apriansyah Jurnal Jejak Hukum Indonesia (Jhi). 2025.
11. Tahir R, Aigp, Wa, Pml, Rmm, Dnpp, . . . & Psr. Metodologi Penelitian Bidang Hukum: Suatu Pendekatan Teori Dan Praktik. Pt. Sonpedia Publishing Indonesia; 2023.
12. Serfiyani Dcy, Smh, Pirsd, Hi, & Smh. Capital Market Top Secret: Ramuan Sukses Bisnis Pasar Modal Indonesia. Penerbit Andi; 2021. 19 P.
13. Andrean Fernando. Perlindungan Hukum Bagi Investor Dalam Layanan Urun Dana Melalui Penawaran Saham Berbasis Teknologi Informasi Tesis Oleh. 2022.
14. Nainggolan B. Buku Ajar Hukum Pasar Modal. 2023.
15. Rohman Md, Kementerian P, Tinggi D, Teknologi U, Borneo T, Fakultas H. Skripsi Perlindungan Hukum Investor Pada Investasi Reksa Dana Dalam Jaringan. 2025.
16. Aryadi A, Ipt, Ka. Ekonomi Digital Dan Transformasi Bisnis Di Indonesia. Sri Gusty, Editor. Makasar: Cv Tohar Media; 2024. 9–14 P.
17. Indarta Y. Cyber Law: Dimensi Hukum Dalam Era Digital. Pustaka Galeri Mandiri.; 2025.
18. Ridho Z, Mujib A. Perlindungan Hukum Bagi Investor Pemegang Obligasi/Sukuk Terhadap Kasus Financial Statement Fraud. J-Alif : Jurnal Penelitian Hukum Ekonomi Syariah Dan Budaya Islam. 2024 May 3;9(1):19. Doi:10.35329/Jalif.V9i1.4936
19. Muhammad Fn. Pengawasan Pemerintah Terhadap Eror Sistem Aplikasi Broker Yang Berakibat Pada Kerugian Investor Saham [Internet]. 2025. Available From: Http://Urj.Uin-Malang.Ac.Id/Index.Php/Jibl
20. Khalid H. Hukum Dan Investasi: Aspek Perlindungan Hukum Oleh Otoritas Jasa

Keuangan Bagi Investor Pasar Modal [Internet]. Vol. 6. 2023;6(1). Doi:10.31933/Unesrev.V6i1

21. Azkiya A, Budi M, Ichsan P, Putra Na, Hasibuan F, Andrianti R, Et Al. Analisis Sistem Autentikasi Dua Faktor (2fa) Dan Efektivitasnya Dalam Meningkatkan Keamanan Akses. Vol. 2. 2026.
22. Akmal S, Dwi Andari Z, Dahlawi Mw, Salsabila M, Ramadhan R. Analisis Penerapan Keamanan Berlapis Melalui Autentikasi Dua Faktor Dalam Melindungi Privasi Komunikasi Digital Pada Platform Media Sosial Instagram. Vol. 2. 2026.