Cybercrime in Global Digital Business: Criminal Law Response and Regulatory Challenges

Apitta Fitria Rahmawati[1], *Yuris* Tri Naili[2]
[1]Law Study Program, Universitas Harapan Bangsa, Purwokerto, Indonesia
[2]Law Study Program, Universitas Harapan Bangsa, Purwokerto, Indonesia

Abstract. The development of global digital business has significantly transformed modern economic activities through the expansion of e-commerce, financial technology (fintech), and artificial intelligence integration. While these advancements enhance efficiency and cross-border transactions, they also generate increasingly complex forms of cybercrime, including online fraud, data breaches, system hacking, and algorithm manipulation. These crimes pose serious risks not only to business actors but also to consumers within the digital economy ecosystem. This research aims to analyze the forms of cybercrime in global digital business and examine criminal law responses as well as regulatory challenges in addressing such crimes. This study employs a normative legal method using statutory and conceptual approaches, focusing on cybercrime regulation, criminal liability, and digital business governance. The results indicate that cybercrime in digital business has evolved into a transnational and technology-driven phenomenon characterized by the use of artificial intelligence and system exploitation. Conventional criminal law approaches are often inadequate due to jurisdictional limitations, challenges in digital evidence, and weak regulation of corporate liability. Furthermore, regulatory fragmentation and the rapid pace of technological innovation create significant obstacles in law enforcement. Therefore, an adaptive and risk-based regulatory framework, supported by international cooperation and strengthened cybersecurity standards, is essential to effectively combat cybercrime and ensure the sustainability of the global digital economy.

Keywords: criminal law; cybercrime; consumer protection; digital business; global regulation.

1 Introduction

Digital transformation has fundamentally reorganized the global economic structure thru the integration of information and communication technology into almost all business activities. This phenomenon has resulted in what is called the digital economy, which is an economic system based on data, connectivity, and technological innovation as the main sources of value

[1] Corresponding author: apittafitriarahmawati@uhb.ac.id

creation (Suwatno, 2021). In this context, business activities are not only tied to physical locations but also thrive in a digital ecosystem that enables real, efficient, and globally scaled transactions between countries.

This development is marked by the rapid growth of various digital business models such as e-commerce, financial technology (fintech), digital marketplaces, and application platforms connected with artificial intelligence (AI). These business models not only enhance operational efficiency and expand market access but also promote financial inclusion and broader economic participation in society. Thus, the digitalization of the economy has become one of the important foundations in the current development of the global economy (Rafli et al., 2025).

That progress is also accompanied by an increasing risk of cybercrime that is becoming more complex and organized. The heavy reliance on digital systems puts businesses and consumers in a situation vulnerable to various types of cyber attacks. In the world of digital business, cybercrime not only causes financial losses but also endangers data security, public trust, and the overall stability of the digital economy system.

Conceptually, cybercrime in digital business encompasses various types of crimes, including fraud in electronic transactions (online fraud), theft and misuse of personal information (data breach), unauthorized access to electronic systems (illegal access), as well as attacks on digital infrastructure such as ransomware and distributed denial of service (DDoS) (Habibi & Liviani, 2020). In addition, recent technological advancements such as artificial intelligence and big data analytics also create opportunities for the emergence of new types of crimes, including algorithm manipulation, deepfake fraud, and crime automation using intelligent systems.

The main characteristics of international cybercrime (transnational cybercrime) present significant challenges in the enforcement of criminal law. Criminal acts can be committed by perpetrators located in different jurisdictions from the victims, utilizing digital infrastructure spread across various countries. This situation gives rise to complex issues related to jurisdiction, extradition, digital evidence collection, and international cooperation in the law enforcement process. In this context, the principle of territoriality in classical criminal law is often insufficient to address the dynamics of cybercrime, which is international and borderless in nature (Hutajulu & Wahyuningsih, 2025).

From a theoretical perspective, the issue of cybercrime in digital business can be examined using a transnational criminal law approach and the theory of criminal liability, particularly corporate criminal liability.Habibi and Liviani, Op.Cit. In many situations, criminals are not only individuals but also involve businesses or digital platforms that play a role in facilitating or neglecting the prevention of crime. Therefore, it is very important to investigate the extent to which companies can be held criminally liable due to their inability to protect the security of systems and user data(Tyas & Rahmahani, 2026).

On the contrary, regulatory challenges also pose a significant issue in addressing the development of cybercrime. Existing regulations are often reactive and lag behind the rapid pace of technological innovation. This condition creates regulatory gaps that can be exploited by criminals. In addition, differences in legal systems between countries also pose an obstacle to efforts to harmonize global regulations in addressing cybercrime (Ganesha et al., 2026). Digital entrepreneurs are required to implement adequate data protection and cybersecurity systems as a form of legal and ethical responsibility in business (Wicaksono et al., 2024).

Several previous studies have examined the phenomenon of cybercrime from various perspectives. First, research focusing on the economic aspects and impacts of cybercrime shows that cybercrime has evolved into a globally organized industry with significant economic losses. Anderson et al. assert that cybercrime is no longer individual in nature, but has instead formed a complex illegal economic ecosystem (Al, 2016). However, this research

places more emphasis on economic and technical aspects and has not yet deeply linked them with the criminal law framework in the context of the global digital business.

Second, studies in the field of cyber law indicate that cybercrime is a transnational phenomenon that challenges the traditional concept of jurisdiction in criminal law. Brenner argues that the cross-border nature of cybercrime poses challenges in law enforcement, particularly concerning jurisdiction determination and proof mechanisms (Brenner, 2006). Nevertheless, the study has not specifically linked this development to the increasingly complex dynamics of the global digital business.

Third, more recent research highlights the relationship between the development of digital technology and regulation, particularly in the context of data protection and the digital economy. Martin emphasizes that the development of a data-driven economy poses new challenges for regulation, especially in terms of privacy protection and cross-border data governance.(Martin, 2019) However, this research is still limited to the aspect of data regulation and has not yet integrated criminal law analysis as an instrument in combating cybercrime.

Based on the review, it can be concluded that there is still a research gap, namely the absence of a comprehensive study that integrates cybercrime, global digital business, and criminal law responses within a single analytical framework. In addition, studies specifically addressing regulatory challenges related to cybercrime based on cutting-edge technology are still limited.

Based on this background, this research focuses on examining several key issues, namely the forms of cybercrime in the global digital business, the criminal law response to cybercrime in digital business activities, and the various regulatory challenges faced in efforts to combat cybercrime amidst the rapid development of digital technology.

The novelty of this study lies in its integrated analysis of cybercrime in global digital business by combining the typology of cybercrime, the criminal law response, and regulatory challenges within a single legal framework. Unlike previous studies that tend to discuss cybercrime either from a technical, economic, or general regulatory perspective, this article specifically examines how criminal law responds to cybercrime arising from electronic transactions, digital platforms, personal data exploitation, artificial intelligence, and cross-border business activities. Therefore, this study contributes to the development of criminal law discourse by emphasizing the need for an adaptive, technology-sensitive, and internationally coordinated legal framework in addressing cybercrime in the global digital economy.

2 Methods

This research applies a normative legal method by analyzing legal norms, principles, and statutory provisions related to cybercrime and digital business. This method is appropriate because the study focuses on examining how criminal law regulates and responds to cybercrime in global digital business, rather than collecting empirical data.

This study uses statutory and conceptual approaches. The statutory approach examines relevant legal instruments, including Law Number 11 of 2008 on Electronic Information and Transactions, as amended by Law Number 19 of 2016 and Law Number 1 of 2024; Law Number 27 of 2022 on Personal Data Protection, particularly Articles 65 to 70; Law Number 1 of 2023 on the Criminal Code; and Law Number 1 of 2026 on Criminal Adjustment. These provisions are analyzed in relation to illegal content, misleading electronic information, illegal access, electronic system interference, personal data misuse, and corporate criminal liability.

The conceptual approach is used to examine legal concepts such as cybercrime, transnational criminal law, criminal liability, digital evidence, corporate responsibility, and

risk-based regulation. The legal materials consist of primary legal materials, including statutory regulations and international legal instruments; secondary legal materials, including books, journal articles, and research reports; and tertiary legal materials, including legal dictionaries and supporting references. The materials are analyzed qualitatively through legal interpretation, systematization of legal norms, and conceptual analysis.

3 Results and Discussion

3.1 Forms of Cybercrime in Global Digital Business

Cybercrime in the global digital business sector has developed rapidly along with the expansion of e-commerce, financial technology, digital marketplaces, cloud-based services, and artificial intelligence. The dependence of business actors and consumers on digital platforms has created new opportunities for criminal activities that are no longer limited by territorial borders (Industri & Nilai, 2021). Cybercrime in digital business is not merely a technical attack against computer systems, but also a form of economic crime that exploits data, trust, algorithms, and electronic transactions.

First, online fraud is one of the most common forms of cybercrime in digital business. This crime usually occurs through fake online stores, fraudulent investment platforms, phishing links, social engineering, account takeover, and identity manipulation. In electronic transactions, perpetrators often create false information to convince consumers to transfer money, provide personal data, or access malicious links. The legal issue arising from online fraud is that the act not only constitutes deception in the traditional sense, but also involves the manipulation of electronic information and digital trust. In the Indonesian legal context, this type of conduct is relevant to Article 28 paragraph (1) of the Electronic Information and Transactions Law, which prohibits the dissemination of false and misleading information resulting in consumer losses in electronic transactions, and Article 45A paragraph (1), which provides criminal sanctions for such conduct (Fraud et al., 2025).

Second, data breach and personal data misuse are serious forms of cybercrime in digital business. Personal data has become a valuable economic asset in the digital economy. Business actors collect and process consumer data for marketing, profiling, credit assessment, and platform optimization. However, weak cybersecurity systems and unlawful data processing may lead to data leaks, identity theft, account takeover, financial fraud, and the sale of personal data on illegal markets. In this context, cybercrime creates both economic loss and violation of privacy rights. Law Number 27 of 2022 on Personal Data Protection provides a more specific legal basis to address this issue. Article 65 prohibits unlawful acquisition, collection, disclosure, and use of personal data belonging to another person. Articles 67 and 68 provide criminal sanctions for unlawful acquisition, disclosure, use, and falsification of personal data. These provisions are important because data-related cybercrime cannot always be effectively addressed only through general provisions on fraud or illegal access (Serius et al., 2024).

Third, illegal access and system intrusion are forms of cybercrime that directly attack the confidentiality, integrity, and availability of electronic systems. These acts include unauthorized access to business databases, customer accounts, payment systems, cloud servers, and internal corporate networks. In digital business, illegal access may be committed to steal trade secrets, obtain customer data, manipulate transactions, or disrupt business operations. Under the Electronic Information and Transactions Law, illegal access is regulated under Article 30, while the manipulation, transfer, alteration, or destruction of electronic information and electronic documents is regulated under Article 32. These

provisions show that criminal law protects not only physical property but also electronic systems and digital information as legal objects.

Fourth, ransomware, malware, and distributed denial-of-service attacks are cybercrimes that threaten the continuity of digital business operations. Ransomware attacks encrypt company data or lock access to digital systems and demand payment from victims. Malware can be used to steal information, damage systems, or secretly monitor business activities. DDoS attacks overload digital infrastructure so that online services become inaccessible. These crimes create operational disruption, reputational damage, financial loss, and consumer distrust. From a criminal law perspective, these acts are related to provisions on interference with electronic systems and electronic information, particularly Articles 32, 33, and 36 of the Electronic Information and Transactions Law (Naila Aulia Amin, 2025). The challenge is that perpetrators often operate across jurisdictions, use anonymization tools, and demand payment through digital assets, making investigation and asset recovery more difficult.

Fifth, platform and algorithm manipulation has emerged as a new form of cybercrime in the digital business environment. This type of crime does not always involve direct hacking. Instead, perpetrators exploit weaknesses in the design of digital platforms or algorithmic systems. Examples include fake reviews, click fraud, manipulation of ratings, price manipulation, fake engagement, automated bot activity, and exploitation of recommendation systems. These acts may distort market competition, deceive consumers, and create unfair advantages for certain actors. The legal challenge is that such conduct may fall between criminal law, consumer protection law, competition law, and platform governance. Therefore, criminal law must be interpreted in a manner that can address manipulation of electronic information, deception in electronic transactions, and unlawful economic advantage obtained through digital systems.

Sixth, artificial intelligence-enabled cybercrime has become an increasingly important issue in global digital business. Artificial intelligence can be used to generate deepfake videos, automate phishing messages, identify vulnerable targets, bypass security systems, and produce fraudulent content at scale. Deepfake technology, for example, can be used to impersonate company executives, manipulate consumer trust, or create false authorization in business transactions. AI-based cybercrime creates difficulties for criminal law because the act may involve automated systems, synthetic content, and unclear attribution of responsibility. The legal question is not only who committed the crime, but also whether the person, corporation, or platform that designed, deployed, or failed to control the technology can be held responsible.

Based on this classification, cybercrime in global digital business can be understood as a multidimensional phenomenon involving fraud, data exploitation, system attacks, platform manipulation, and AI-enabled criminal conduct. Therefore, an effective legal response must not only criminalize prohibited acts but also strengthen prevention, digital evidence mechanisms, corporate accountability, and international cooperation.

3.2 Criminal Law Response to Cybercrime in Digital Business

Criminal law is an essential instrument for responding to cybercrime in digital business because it provides the basis for criminalization, investigation, prosecution, and punishment. However, cybercrime requires a more specific criminal law response because the object of crime is often intangible, the evidence is digital, the victim and perpetrator may be located in different jurisdictions, and the crime may be committed through automated or anonymous systems (Salsabilla & Angelina, 2024).

The first criminal law response concerns online fraud in electronic transactions. In the Indonesian context, Article 28 paragraph (1) of the Electronic Information and Transactions

Law prohibits any person from knowingly and without authority disseminating false and misleading information that causes consumer losses in electronic transactions. Article 45A paragraph (1) provides criminal sanctions for this conduct. These provisions are highly relevant to digital business because consumer trust is the foundation of electronic commerce. False information in digital transactions may appear in the form of fake products, fraudulent advertisements, fake investment offers, fake payment confirmations, or manipulated platform information (Rahman et al., 2026). Therefore, criminal law functions not only to punish perpetrators but also to protect consumers and maintain trust in the digital marketplace.

The second response concerns illegal access and attacks against electronic systems. Articles 30 to 36 of the Electronic Information and Transactions Law provide the legal basis for addressing unauthorized access, interception, alteration, transfer, concealment, destruction, and interference with electronic information or electronic systems. These provisions are important for cases involving hacking, ransomware, malware, DDoS attacks, and manipulation of business databases. In digital business, the disruption of electronic systems can cause large-scale economic loss and affect consumers, investors, and business partners. Therefore, cyberattacks should not be viewed merely as technical disturbances but as criminal acts that threaten business continuity and public trust.

The third response concerns the protection of personal data. Law Number 27 of 2022 on Personal Data Protection strengthens criminal law protection against data-related cybercrime. Article 65 prohibits unlawful acquisition, collection, disclosure, and use of personal data belonging to another person. Article 66 prohibits the creation or falsification of personal data for unlawful benefit. Articles 67 and 68 provide criminal sanctions for these acts. In addition, Article 70 regulates corporate criminal liability when personal data crimes are committed by corporations. These provisions are significant because data breach and data misuse are among the most serious threats in digital business. Companies that collect and process consumer data must not only comply with administrative obligations but may also face criminal consequences when unlawful conduct occurs.

The fourth response concerns corporate criminal liability. In the digital business ecosystem, cybercrime may involve corporations either as direct perpetrators, facilitators, or negligent actors (Yusup, 2026). Corporate liability becomes relevant when a company knowingly benefits from unlawful data use, fails to implement adequate security measures, ignores repeated cyber risks, or allows its platform to be used for systematic fraud. Law Number 27 of 2022 expressly recognizes corporate liability in personal data crimes. In addition, the new Criminal Code under Law Number 1 of 2023 provides a broader foundation for corporate criminal responsibility in Indonesian criminal law. This development is important because cybercrime in digital business is often connected to organizational systems, platform design, and corporate governance failures.

The fifth response concerns digital evidence. Cybercrime cases rely heavily on electronic information, electronic documents, system logs, metadata, IP addresses, transaction records, and digital communication. The challenge is that digital evidence is vulnerable to alteration, deletion, encryption, and cross-border storage. Therefore, criminal law enforcement must be supported by digital forensic capacity, proper chain of custody, and cooperation with electronic system providers. Without reliable digital evidence mechanisms, criminal law provisions may become ineffective even when the prohibited conduct is clearly regulated.

The sixth response concerns transnational law enforcement. Cybercrime in global digital business often involves perpetrators, victims, servers, payment systems, and data storage located in different countries. This creates challenges related to jurisdiction, extradition, mutual legal assistance, and recognition of electronic evidence. International cooperation is therefore necessary. The Budapest Convention on Cybercrime provides an important reference for harmonizing cybercrime provisions and facilitating international cooperation in investigation and evidence collection. Although not all countries have the same legal

framework, the principles of harmonization, procedural cooperation, and rapid preservation of electronic evidence are increasingly relevant in addressing cybercrime in global digital business.

Therefore, the criminal law response to cybercrime in digital business should not be limited to punishment after the crime occurs. It must also include prevention, corporate compliance, cybersecurity obligations, consumer protection, protection of personal data, and international cooperation. Criminal law must become adaptive enough to respond to technological development while still maintaining the principles of legality, proportionality, and legal certainty.

3.3 Regulatory Challenges in Addressing Cybercrime in the Global Digital Economy

The global growth of digital businesses presents increasingly complex and diverse regulatory challenges. One of the main challenges is the gap between technological advancement and regulation (regulatory lag), where laws often do not keep up with technological innovations. This condition results in existing regulations becoming irrelevant or unable to cover new types of crimes.(Siregar et al., 2024)

In addition, fragmented regulations between countries also pose a challenge in addressing cybercrime. Each country has different legal systems, policies, and regulatory norms, making it difficult to harmonize laws in a global context. Without uniformity in standards, criminals can exploit those regulatory differences (regulatory arbitrage) to evade law enforcement. Another challenge faced is the lack of international coordination and collaboration in addressing cybercrime. Although there are various international forums and cooperation methods, their implementation still faces challenges such as differing national interests, limited resources, and issues of national sovereignty.

The development of technologies such as artificial intelligence and blockchain also poses new challenges in regulation. These technologies have decentralized characteristics and are difficult to control, thus requiring innovative and adaptive regulatory approaches. Regulation must not only be able to govern but also encourage innovation without hindering technological development. In the context of global business law, the regulatory approach needed is one that is adaptive, collaborative, and risk-based. Countries need to develop policies that are not only repressive but also preventive and responsive to technological dynamics. Therefore, strengthening regulations in addressing cybercrime needs to be carried out thru several strategic steps, including:

3.3.1 Harmonization of cybercrime regulations at the international level

Harmonization is necessary because cybercrime often involves perpetrators, victims, servers, digital platforms, and financial transactions located in different jurisdictions. Variations in national legislation could lead to legal loopholes that let offenders escape punishment in the absence of unified legal standards. Harmonization calls for shared principles on the criminalization of unauthorized access, data theft, online fraud, electronic system interference, digital evidence, and cross-border cooperation, but it does not compel all nations to enact the same criminal laws.

3.3.2 Strengthening cross-border cooperation in law enforcement

Since one nation cannot effectively combat cybercrime on its own, cross-border collaboration must be strengthened. Electronic evidence is frequently kept outside the victim's nation, and

offenders may operate covertly from a different state. Therefore, collaboration is crucial through information exchange, extradition procedures, mutual legal aid, and quick preservation of electronic evidence. To track down offenders and stop additional losses, law enforcement organizations must work closely with financial institutions, cybersecurity authorities, and suppliers of digital platforms.

3.3.3 Improvement of cybersecurity standards in the business sector

Cybersecurity standards must be improved because digital business actors are often the first line of defense against cybercrime. Companies that manage consumer data, electronic transactions, and digital platforms have a legal and ethical obligation to implement adequate security measures. These measures include risk assessment, data encryption, access control, incident response mechanisms, regular security audits, and employee cybersecurity training. Strong cybersecurity standards are important not only to prevent attacks but also to reduce corporate negligence and strengthen accountability when cyber incidents occur.

3.3.4 Strengthening personal data protection

The protection of personal data needs to be enhanced as it has emerged as a primary focus of cybercrime within the digital economy. Data breaches, identity theft, illegal data selling, and improper use of consumer information can lead to financial damage and infringe on privacy rights. Consequently, regulations on data protection must guarantee that business entities handle personal data in a legal, transparent, and secure manner. Moreover, businesses should be mandated to secure valid consent, restrict data gathering to legitimate reasons, safeguard stored information, and inform appropriate authorities and impacted users when a data breach takes place.

3.3.5 Enhancement of legal and digital literacy for the community and business actors

Improving legal and digital literacy is essential since numerous cybercrimes thrive due to the inadequate awareness of consumers and small business participants about digital threats, phishing tactics, counterfeit investment sites, deceitful online transactions, and safeguarding personal data. Enhancing digital literacy enables users to recognize dubious activities, safeguard their accounts, and react appropriately when cyber incidents arise. Simultaneously, legal literacy is crucial for business stakeholders to comprehend their obligations regarding electronic transactions, data privacy, cybersecurity adherence, and consumer rights.

Based on these measures, cybercrime regulation should not only focus on punishment after the crime occurs. It must also emphasize prevention, compliance, institutional cooperation, and public awareness. An effective regulatory framework should be adaptive, risk-based, and capable of balancing law enforcement, consumer protection, and digital business innovation.

4 Conclusion

Cybercrime is one of the main challenges in the development of the global digital business. Forms of cybercrime such as online fraud, personal data theft, attacks on digital systems, and manipulation of business platforms show that the development of digital technology also brings significant legal risks. Criminal law plays an important role in combating cybercrime thru the imposition of sanctions on offenders and legal protection for victims. However, the

enforcement of criminal law in cybercrime cases still faces various obstacles, especially related to the transnational nature of the crime and the complexity of digital evidence. To enhance the effectiveness of combating cybercrime in the global digital business, harmonization of regulations, capacity building for law enforcement, and strengthening international cooperation are necessary. Thus, the legal system can be more adaptive in facing the challenges of digital economic development in the era of globalization.

References

Al, R. A. et. (2016). Measuring the Cost of Cybercrime. *Journal of Cybersecurity*, *2*(2).

Brenner, S. W. (2006). Cybercrime Jurisdiction. *Crime, Law and Social Change*, *46*.

Fraud, O., Emotional, M., Prevention, S., & Online, P. (2025). Satan Scammer: Avoiding Online Scams. *JIPMAS: Journal of Vision of Community Service*, *06*(02), 133–145.

Ganesha, U. P., Tegal, B., & Buleleng, K. (2026). The role and challenges of artificial intelligence in its implementation in cyber law. *Journal of Academic Media*, *4*(2).

Habibi, M. R., & Liviani, I. (2020). Information Technology Crime (Cyber Crime) and Its Countermeasures in the Indonesian Legal System. *Al-Qanun: Journal of Islamic Law Thought and Reform*, *23*(2), 400–426. https://doi.org/10.15642/alqanun.2020.23.2.400-426

Hutajulu, A. F., & Wahyuningsih, S. R. I. E. (2025). Criminal Law Enforcement Against Cyber Crime In Indonesia. PROGRAM IN LAW, SULTAN AGUNG UNIVERSITY OF SEMARANG. *Encyclopedia Of Journal*, *7*(3), 79–89.

Industry, P., & Nilai, B. (2021). Cybercrime as an Inhibitor of E-Commerce in the Development of Industry 4.0 Based on Indonesian Cultural Values. *Tarumanagara University's Third National Seminar Series in 2021*, 277–286.

Martin, K. E. (2019). Ethical Implications and Accountability of Algorithms. *Journal of Business Ethics*, *160*.

Amin, A. P. M. (2025). Redefining Sovereignty in the Digital Age: Cybersecurity, Data Governance, and Regional Autonomy in Southeast Asia. *Triwikrama: Journal of Social Sciences*, *9*(9).

Rafli, M., Dwi, R., Budiman, M. R., & Wahjono, S. I. (2025). The Role of Financial Technology (Fintek) in Encouraging Financial Inclusion and Economic Growth in the Digital Era. *Journal of Innovative and Creativity*, *5*(2), 720–731.

Rahman, A., Hasibuan, H., Kelvin, A., Pakpahan, P., & Daeli, E. (2026). The crime of online fraud and its legal liability is based on the laws of the Internet in Indonesia. *Journal of Innovative and Creativity*, *6*(1), 5785–5790.

Salsabilla, A., & Angelina, J. (2024). The Role of Criminal Law in Dealing with Cybercrime in the Present: A Review of the Electronic Transaction Information Act. *Journal of Education, Religion, Humanities and Multidiciplinary*, *2*(2 SE-Articles), 1548–1554. https://doi.org/10.57235/jerumi.v2i2.4461

Serious, A., Era, D., Balaka, K. I., Hakim, A. R., & Sulistyany, F. D. (2024). Stealing Customer Information in the Banking Sector: *Judiciary*, *10*(3), 105–130.

Siregar, O. K., Apriliza, A., & Satria, A. (2024). Supervision and Law Enforcement of Digital Businesses. *Doctrine: World Journal of Law and Political Science*, *2*(2), 136–141.

Suwatno. (2021). *Digital Transformation Towards the Digital Society Era as an Acceleration of National Economic Revival*. UPI The Education University. https://berita.upi.edu/transformasi-digital-menuju-era-digital-society-sebagai-akselerasi-kebangkitan-ekonomi-nasional/

Tyas, E. S., & Rahmahani, A. P. (2026). Analysis of legal certainty related to the prevention

of online fraud crimes based on the ITE Law. *Journal of Community Service and Educational Research*, *4*(3), 17990–18002.

Wicaksono, A. T., Yasin, I. F., &ampel, U. I. N. S. (2024). Sectoral Cyber Protection Reformulation of Criminal Law Through Omnibus Law as a Sectoral Cyber Protection Solution The Indonesian state, as a country adhering to the civil law system, has from cybercrime. 2 With a co. *Al-Jinayah Islamic Journal of Criminal Law*, 237–261.

Yusup, A. (2026). Corporate Fault Construction As The Architecture Wildlife Trade In Transnational Networks From A Psychopathy Theory Perspective. *Jurnal Penelitian Hukum De Jure*, *26*(1), 19–44.