

Article

Unauthorized Access to Bank Accounts and E-Money in E-Commerce as Cyber-Economic Crime

Harri Prasetyo Rachmatullah

¹Master of Law, Faculty of Law, Universitas Pancasila, Jakarta, Indonesia

Article information	Abstract
DOI : xxx Correspondence : harriprasetyo1994@gmail.com	The development of digital technology has driven the growth of e-commerce and the use of electronic money (e-money). However, it has also given rise to new forms of crime, particularly cybercrime, which can cause financial losses to victims and potentially affect economic stability. This article systematically reviews the main ideas presented in documents discussing the unauthorized access to bank accounts and e-money in e-commerce transactions as forms of economic crime. The review demonstrates that cybercrime in this context is economically motivated, technology-enabled, transnational in nature, and difficult to address using conventional criminal law frameworks. The findings emphasize the need to reform criminal law, strengthen regulations governing electronic transactions, and enhance the protection of digital service users. Digital technology can accelerate a nation's economic growth; therefore, technology plays an important role in national development. Nevertheless, technological advancement has also been accompanied by the emergence of new forms of digital crime, particularly cybercrime as a form of economic crime. Accordingly, this study addresses the following research question: How does criminal law view the unauthorized access to bank accounts and electronic money in e-commerce as an economic crime? The study aims to examine the concept of criminal law in addressing cybercrime as a form of economic crime. The significance of this research lies in its contribution to criminal law reform in response to new forms of crime arising from contemporary technological developments. The research employs a normative juridical method. The findings indicate that cybercrime may be classified as an economic crime when its primary motive concerns property or financial gain. If such crimes are left unaddressed, they may negatively affect the national economy by reducing public confidence and willingness to conduct online transactions or deposit money in bank accounts, which may ultimately contribute to economic decline. In conclusion, crimes committed within cyberspace may constitute economic crimes. One example examined in this study is the unauthorized access to bank accounts, including incidents occurring in connection with e-commerce. E-commerce itself refers to transactions conducted through advanced technology between individuals who may be geographically distant from one another and who do not need to interact face-to-face.
Submission Track	
Submission : April 18, 2026 Final Review : May 20, 2026 Accepted : May 25, 2026	
Keywords	
Cybercrime, e-money, economic crime	



ess article under the CC BY
<https://creativecommons.org/licenses/by/4.0/>

INTRODUCTION

As human civilization develops, the level of advancement of a nation also progresses. A nation's advancement can be reflected in the development of intellectual capacity and the emergence of various fields of knowledge, including advances in science and technology. At present, almost every area of

human life utilizes Information and Communication Technology (ICT) in carrying out its activities. These areas include the economy, education, healthcare, government, banking, religion, and national defense and security systems. In particular, the digitalization of economic activities and the rapid shift toward remote financial interactions have transformed traditional commerce, rendering physical currency increasingly obsolete (Imran & Gunawa, 2025). This shift toward digital payment services and distributed infrastructure has fundamentally altered the landscape of financial offenses, introducing new, highly complex vectors for criminal activity (AllahRakha, 2024; Volkov, 2026).

However, internet-based technologies are also frequently misused by irresponsible parties, creating opportunities for unauthorized access, data theft, fraud, and other financially motivated offenses (Amoo et al., 2024; Duhaidahawi et al., 2020). Consequently, technological development has not only transformed legitimate economic activity but has also facilitated the emergence of new forms of criminal conduct. When technology is used as a means to obtain unlawful financial benefits, compromise digital systems, or cause economic harm, such conduct may constitute a criminal offense in the fields of telecommunications, information technology, and cybercrime. These developments demonstrate that the expansion of digital economic activity must be accompanied by effective legal protection, because conventional criminal-law frameworks may not adequately address offenses committed through rapidly evolving technological systems (Kumar, 2024; Noor, 2025).

Criminal offenses committed in cyberspace are commonly referred to as “cybercrime” or “cyber crimes.” The term “cybercrime” is also closely associated with the concept of “computer crime.” Cybercrime can be committed by virtually anyone, regardless of age, time, geographical boundaries, circumstances, weather conditions, or other conventional limitations. Furthermore, the absence of spatial and temporal convergence between perpetrators and victims complicates traditional investigative efforts, as crimes are no longer tethered to the physical location of the criminal act (Zhou et al., 2024). This jurisdictional fluidity allows threat actors to exploit varying international legal standards, effectively traversing borders to coordinate attacks while evading domestic enforcement mechanisms (Chen et al., 2023).

Historically, criminal law was designed to protect individuals and citizens in relation to tangible interests, such as the human body, life, physical integrity, objects, and property—in other words, matters that could generally be perceived physically (Berman, 2002). When criminal codes were formulated and enacted, legislators could not have anticipated the emergence of technologies capable of creating, processing, storing, and transmitting various forms of digital data through computer systems. Consequently, conventional criminal-law provisions may be inadequate for addressing cybercrime, as the traditional elements required to establish an offense do not always correspond to criminal conduct occurring in cyberspace. The shift from a tangible, territorial environment to an intangible, dematerialized domain means that both the offenses and the investigative methodologies often fall outside the purview of pre-established, state-centric rules (Greco & Montinaro, 2020). Crime within society can also be understood from particular perspectives as part of a broader social process. Consequently, law enforcement must be considered within the framework of criminal policy, which encompasses both preventive measures aimed at preventing crime and repressive measures involving the enforcement of criminal law. The same approach applies to cybercrime.

Cybercrime is not an ordinary form of criminal conduct because offenders may possess sophisticated technological knowledge and capabilities that distinguish them from conventional offenders. In some circumstances, perpetrators possess a higher level of technological expertise than law enforcement officials. This creates significant difficulties for law enforcement agencies in investigating and prosecuting cybercrime. At the same time, Indonesian society must be protected against threats to both physical security and property. The rapid evolution of these digital threats necessitates a robust synchronization between national regulations and international standards to mitigate the vulnerabilities inherent in cross-border data flows (Erikha & Saptomo, 2024; Hasnia et al., 2025).

Criminal acts committed in cyberspace may harm a person's dignity and reputation, but many are also motivated by economic interests and are therefore related to material or financial gain. Nevertheless, some cyber offenses may be committed for purposes unrelated to financial benefit. In principle, every criminal offense involves an offender and a victim. In cybercrime, however, interactions between perpetrators and victims frequently occur in cyberspace, even though the ultimate objective of economically motivated cybercrime is often to obtain tangible financial benefits (Anastasia et al., 2019; Maimon & Louderback, 2018).

Accordingly, this study examines the following research question: How should criminal law conceptualize, classify, and address unauthorized access to bank accounts and electronic money in e-commerce as a form of economically motivated cybercrime? More specifically, the study analyzes the legal elements of such conduct, its classification under applicable criminal-law provisions, and the extent to which existing legal frameworks are capable of protecting financial assets and electronic payment systems from unauthorized access and related forms of exploitation.

METHODS

This legal study employs a normative legal research method. The analysis focuses on the framework of applicable laws and regulations, statutory provisions, relevant legal doctrines and theories, as well as perspectives derived from the sociology of law. The normative approach is applied by analyzing the legal issues under examination in relation to existing legal norms and theories. The research primarily relies on library-based or secondary legal materials. The analysis is grounded in legal principles and theories contained in statutory and regulatory provisions, which are subsequently examined in relation to the identified legal problems. Existing legal principles and theories are therefore employed as the principal analytical framework for evaluating the issues discussed in this study.

RESULT AND DISCUSSION

Cybercrime constitutes a category of criminal offense that requires particular attention. It presents complex legal challenges because activities in cyberspace are not confined by national territorial boundaries, particularly when perpetrators operate from different jurisdictions. Activities in cyberspace are also relatively intangible because offenses are committed within a virtual environment. Establishing evidence can be difficult because electronic data can be modified relatively easily and digital traces can be erased or concealed. Criminal conduct continues to evolve alongside technological developments within society. Indeed, criminal methods may develop more rapidly than the legal and institutional mechanisms designed to address them. Consequently, the modernization of criminal law is necessary to ensure that the legal system remains responsive to technological and societal developments.

Criminal acts committed in cyberspace may also reflect conduct that occurs in the physical world. Examples include defamation and sexual harassment conducted through digital media (cybersex-related offenses). Such conduct may be motivated by fear of confronting an opponent or competitor directly. Dissatisfied individuals may instead use cyberspace as a means of retaliation by threatening, insulting, intimidating, or otherwise harming their opponents, rivals, or competitors.

An important question is whether cybercrime should be understood as an entirely new category of crime or merely as a conventional form of crime in which technology functions as the instrument, infrastructure, or target of the offense. Many characteristics of cybercrime resemble those of conventional crime. For example, computers, the internet, and telecommunications devices such as mobile phones may be used to commit defamation or fraud. The underlying conduct may resemble conventional offenses, while the principal difference lies in the medium through which the crime is committed. Traditionally, defamatory information might have been distributed through printed materials displayed in public places, while fraud could have been committed through direct verbal communication between individuals. Digital technology has transformed the methods through which essentially similar conduct can be carried out.

Unauthorized Access to Bank Accounts and E-Money as a Form of Cybercrime

Individuals who commit offenses by exploiting technological systems are commonly referred to as hackers. However, in the context of malicious activities, the term cracker is sometimes used to distinguish individuals who intentionally breach or damage computer systems from those who use technical skills for legitimate purposes. In the hacking literature, hacking may be understood as unlawfully or without authorization connecting an additional computer terminal to a computer network system (Sanchez & Omar, 2013). Furthermore, these activities encompass a broader spectrum of illicit operations, including the deployment of malware to compromise system integrity or the unauthorized extraction of sensitive data for criminal gain (Greco & Greco, 2020). In practice, hackers may engage in either constructive or destructive activities. Malicious hackers illegally penetrate or damage internet-based systems and networks. By contrast, ethical or security-oriented hackers may identify vulnerabilities and repair systems that have been compromised by malicious actors (Baddam, 2020). Nevertheless, unauthorized access may still raise legal concerns even where the individual claims to have acted with beneficial intentions, because access to the relevant system may have occurred without the authorization of its lawful owner.

If such conduct were interpreted by analogy with conventional crime in the physical world, unauthorized access to a computer system could be compared to entering another person's premises without permission, conduct historically addressed under Article 167 of the Indonesian Criminal Code (KUHP). Perpetrators who hack banking systems may also engage in carding. A carder may purchase goods or conduct transactions using another person's credit card number through e-commerce facilities after unlawfully obtaining or intercepting the victim's credit card details and security credentials. Such conduct involves manipulating electronic systems to obtain money or goods through e-commerce transactions. Such fraudulent practices often rely on data and program manipulation, including the unauthorized entry of instructions or the illicit alteration of input data to facilitate personal gain at the expense of rightful owners (Azizah et al., 2021).

A common problem in such cases arises when fraudulent transactions are discovered only after payment for the goods has been rejected by the bank while the perpetrator has already received the purchased goods. The seller consequently suffers financial loss as a result of fraudulent conduct. If such an act were committed outside cyberspace, it could generally be regarded as conventional fraud, historically regulated under Article 378 of the Indonesian Criminal Code.

Another form of cybercrime associated with e-commerce is online sales fraud. Goods may be advertised through websites, electronic communication platforms, smartphones, or online shops even though the seller does not actually possess the products offered to prospective buyers. From a consumer-protection perspective, appropriate safeguards and secure transaction mechanisms are therefore essential to reduce the risks associated with online transactions.

Direct transactions between sellers and buyers traditionally provide certain advantages in terms of security and identification because the parties can verify each other's identities (Li et al., 2011). In contrast, identifying and apprehending perpetrators of cybercrime may be considerably more difficult. Where an offense is committed through the internet, investigators may initially be able to identify only an IP address or the computer used in the commission of the offense. Investigations become even more complicated where publicly accessible computers or shared networks are used and adequate records identifying individual users are unavailable. Moreover, sophisticated perpetrators frequently employ techniques like IP address falsification and bouncing signals through global networks to mask their physical location and true identity (Karo & Sebastian, 2019).

This does not mean that Indonesia should reject technological development. Rather, preventive measures are required to reduce the risks of fraud, unauthorized access to accounts, and e-money theft. Computers, internet networks, smartphones, websites, and e-commerce applications facilitate online commercial transactions, but they may simultaneously create challenges for criminal investigations

because victims may never see or directly interact with perpetrators. Consequently, addressing these vulnerabilities necessitates a comprehensive approach that integrates robust cybersecurity frameworks—such as multi-factor authentication and advanced encryption—with enhanced digital literacy and legal enforcement.

One form of cybercrime involving unauthorized access to account information is the infringement of privacy. Such offenses target information that is private and confidential and may be committed for the purpose of obtaining financial benefits. This may include unlawfully obtaining ATM card numbers, bank account details, and personal identification numbers (PINs). Such crimes are not limited to e-commerce transactions; they can occur whenever an offender obtains access to sensitive banking credentials. The involvement of individuals with privileged internal access to banking systems may further increase the risk. Regardless of the method employed, these offenses can cause both material and non-material harm to victims.

Cybercrime as a Category of Cyber-Economic Crime

In criminal law, a criminal offense or delict—derived from the Latin term *delictum*—generally refers to conduct prohibited by law and subject to criminal punishment when the prohibition is violated. One of the fundamental purposes of criminal law is to protect the social order by identifying conduct that must not be committed and establishing sanctions against those who violate such prohibitions. In broader terms, criminal law seeks to address conduct that causes harm to society (Sarnoff, 2022). Within the specific context of the digital era, this regulatory mandate extends to cyber-economic offenses, where the misuse of personal identity and data serves as a primary vehicle for unlawful financial gain (Haryono & Myharto, 2026).

Traditionally, the concept of society has referred primarily to communities existing in the physical world. However, developments in science and technology have indirectly created a new social environment: the virtual or cyber community. This virtual society may be understood as an extension or reflection of society in the physical world. Consequently, the rapid digitalization of this domain has enabled cyber-economic activities that mirror traditional property crimes, yet occur with a complexity and international reach that challenge conventional enforcement (Krishna, 2024). These illicit activities undermine global economic stability, as digital transformation has integrated data-intensive sectors—such as banking and telecommunications—into environments where criminals can disrupt systems or deceive users (Ombu, 2023).

The emergence of virtual communities inevitably creates opportunities for criminal conduct within those communities. It should be recognized that members of virtual communities are the same individuals who participate in physical society; what changes is primarily the locus or environment in which their interactions occur. Consistent with the constitutional principle that the state must protect the entire nation and promote public welfare, the government has an obligation to protect citizens against criminal conduct while simultaneously developing policies that facilitate economic activity and economic growth. To this end, the digital environment must be recognized as a sphere of circulation for assets of significant value, necessitating the adaptation of criminal legislation to address the reproduction of traditional property offenses within virtual spaces (Davydenko et al., 2025).

Crimes committed through advanced network-based technologies are generally described as cybercrime. However, not every cybercrime necessarily contains an economic element. Therefore, cybercrime should not automatically be categorized as economic crime. Cybercrime may instead constitute a specific or special category of criminal offense because its regulation and enforcement mechanisms may differ from those applicable to conventional crimes. Specifically, while economic cybercrimes are motivated by mercenary interests, other offenses such as cyber-harassment or cyber-terrorism operate on fundamentally different social or political drivers. Cyber-harassment generally involves unwanted communications directed at an individual, whereas ideologically motivated cyberattacks may seek to

advance political or religious objectives rather than obtain financial gain (Baak et al., 2022; Holt et al., 2017). Cybercrime should therefore be classified not only according to the technological means employed but also according to the offender's principal motive, the target selected, and the harm intended. Nevertheless, these categories may overlap in practice because a single cyberattack can pursue multiple objectives, including financial profit, revenge, publicity, or political influence (King et al., 2018; Sabillón et al., 2016).

Electronic media have become particularly important for business communities because national economic development is partly influenced by the ability of businesses to promote and distribute goods and services. Indonesian industries produce numerous products with the potential to reach international markets. Business actors must therefore be capable of utilizing internet-based facilities effectively. Economic crises should also serve as lessons encouraging society and national institutions to strengthen economic resilience. Internet and computer networks represent important instruments that can be utilized by society to promote Indonesian products, businesses, and economic opportunities.

Criminal Law Perspectives on Unauthorized Access to Bank Accounts and E-Money Through Electronic Media in Cyberspace

Numerous internet-based applications operating on Android and iOS platforms now provide online shopping services, including Tokopedia, Bukalapak, Lazada, and Shopee. Application-based transportation and other services, such as Gojek and Grab, have similarly transformed commercial transactions. Payments made through such platforms increasingly rely on electronic payment systems, including e-money, in which monetary value is transferred without the physical exchange of cash.

Electronic payment systems provide numerous practical advantages. One distinction traditionally identified between certain forms of e-money and debit or credit cards concerns the information associated with the holder. Certain forms of e-money may not require the same level of personal identification information traditionally associated with debit or credit cards. Moreover, depending on the payment system and service provider, fee structures applicable to e-money may differ from those associated with debit and credit cards. These inherent structural differences in data requirements and transaction protocols present unique vulnerabilities that malicious actors exploit to conduct unauthorized account infiltration or fraudulent electronic transfers (Arifin et al., 2020; Ramadhan et al., 2020).

E-money can generally be defined as an electronic payment instrument in which monetary value is stored electronically. Users typically provide funds to an issuer before using the electronic value for transactions. Once a transaction is completed, the stored electronic value decreases by the corresponding amount and may subsequently be replenished through a top-up mechanism. The electronic medium used to store monetary value may be based on a chip or server. Regardless of the underlying storage architecture, the security of these electronic wallets is increasingly paramount, as incidents of unauthorized account access frequently lead to significant financial losses for consumers (Octora, 2021).

The use of electronic money as an innovative and practical payment instrument is intended to facilitate efficient payment processes, particularly for high-volume, rapid, and low-value economic transactions. Since electronic money offers the benefit of making transactions simpler, quicker, and less expensive, it is extremely possible that adoption will continue to accelerate among the general public. The regulation of e-money in Indonesia was historically addressed through Bank Indonesia Regulation No. 11/12/PBI/2009 concerning Electronic Money, subsequently amended, including through Bank Indonesia Regulation No. 18/17/PBI/2016, together with Bank Indonesia Circular Letter No. 11/11/DASP dated 13 April 2009 concerning Electronic Money.

Under this regulatory framework, electronic money is issued based on monetary value initially deposited by the holder with the issuer and subsequently stored electronically on a medium such as a server or chip. Thus, e-money circulating in cyberspace should not simply be understood as abstract

money without an underlying value. Rather, it represents monetary value initially provided in conventional currency and subsequently converted or recorded in electronic form. Consequently, the value managed by the issuer does not constitute a traditional bank deposit, distinguishing it legally from the funds held in conventional savings or checking accounts (Putri & Prasetyo, 2020). Moreover, Bank Indonesia Regulation Number 20/6/PBI/2018 further clarifies that this electronic value must be disseminated by the issuer based on these advances, ensuring that the stored funds are distinct from deposits as defined under banking legislation.

Electronic money in Indonesia continues to represent value denominated in Indonesian rupiah. Certain service providers may express promotional or reward value in the form of “points.” For example, digital platforms may cooperate with electronic payment providers and offer point-based systems. Such points should not automatically be regarded as independent currencies; rather, their value and convertibility into rupiah depend on the terms and mechanisms established by the relevant service provider.

Criminal Law Perspectives on Unauthorized Access to Bank Accounts and E-Money in E-Commerce as Economic Crime

Criminal law recognizes the principle of legality, under which an act cannot ordinarily be treated as a criminal offense unless it has been defined and prohibited by law. As society and technology develop, however, new forms of conduct continually emerge, accompanied by new opportunities for criminal activity. This situation is reflected in the legal maxim *Het Recht Hinkt Achter de Feiten Aan*, which broadly conveys the idea that law tends to lag behind social developments and emerging forms of conduct. Accordingly, the development and expansion of e-money inevitably create opportunities for new forms of criminal behavior. Unauthorized access to bank accounts and e-money may therefore be understood as manifestations of the continuing evolution of crime in response to technological change.

Based on the examples and forms of criminal conduct discussed above, unauthorized access to bank accounts in e-commerce transactions presents significant risks to customers conducting financial transactions online. Perpetrators may hack or penetrate electronic systems for economic purposes through various methods. These methods range from relatively simple forms of electronic fraud conducted through mobile phones, text messages, or fraudulent online transactions to sophisticated attacks designed to bypass security systems and obtain confidential banking credentials.

The common objective of such conduct is material or financial gain. Even relatively simple schemes may be committed without direct interaction between the offender and the victim. Because the parties do not meet face-to-face and transactions may depend substantially on trust and electronic authentication, online commercial environments may be particularly vulnerable to fraudulent conduct. Such offenses may therefore be classified as cyber-economic crimes when they contain a clear economic motive or are intended to produce financial benefits. These activities are facilitated by the inherent depersonalization and distance between the owner and their digital assets, which complicates traditional security measures and creates opportunities for third-party misappropriation (Vozniuk et al., 2020).

Criminal conduct committed through electronic media, whether through internet-connected or non-networked systems, may be regarded as economically motivated when it causes financial harm or is undertaken for financial gain. The relationship between cybercrime and economic crime can therefore be identified where the elements of a cyber offense include an economic motive, financial objective, or interference with property and economic interests. Such criminal activities often exploit the digitalization of trade to facilitate illicit financial flows, demonstrating how cyber-enabled offenses function as direct threats to the integrity of modern electronic commerce (Truntsevskiy & Ketsko, 2020).

Even where the formal elements of a particular cyber offense do not explicitly contain an economic component, its economic consequences may still be relevant. Conversely, certain offenses involving information and communication technologies may constitute purely cyber-related crimes without any

significant economic motive or consequence. Nonetheless, the absence of a universally accepted definition for economic crime complicates efforts to standardize the legal classification of these hybrid offenses (Fedorov et al., 2025). Furthermore, this ambiguity is exacerbated by the distinction between offenses where computer systems are the targets of a criminal attempt and those where they function merely as instruments for illegal activity (Šturc et al., 2022).

Cybercrime therefore has varying characteristics. A distinction may be drawn between cybercrime as a specialized category of criminal conduct and cybercrime that specifically constitutes or relates to economic crime. Unauthorized access to bank accounts through the penetration of electronic systems can, by analogy, be compared with conventional offenses involving unauthorized entry into another person's protected premises. This illustrates that many offenses committed in cyberspace have conceptual similarities with conventional crimes, although their methods, objects, and environments differ.

Accordingly, addressing cybercrime may require the development and expansion of legal concepts traditionally applied to conventional offenses. Such interpretation must nevertheless remain consistent with the principle of legality and the applicable statutory framework. The evolution of cybercrime therefore demonstrates the need for criminal law to respond appropriately to technological developments while maintaining legal certainty, protecting individual rights, and safeguarding economic interests.

CONCLUSION

The development of information technology has contributed significantly to the growth of e-commerce and the increasing use of electronic money (e-money), providing various forms of convenience and efficiency in economic activities. However, these technological advances have also given rise to new forms of criminal activity, particularly cybercrime involving unauthorized access to bank accounts and the misuse of electronic money. Such cybercrimes possess characteristics that distinguish them from conventional criminal offenses because they are committed through electronic media, may transcend national borders, present significant evidentiary challenges, and often require sophisticated technological capabilities. Unauthorized access to bank accounts and e-money may be categorized as a form of cyber-economic crime when the conduct is motivated by the intention to obtain financial gain or results in economic losses to victims. Such offenses not only cause harm to individuals but may also undermine public confidence in banking systems and electronic transactions. A decline in public trust may, in turn, negatively affect the broader development and stability of the national economy. From the perspective of criminal law, technological development demonstrates that legal frameworks may struggle to keep pace with rapidly evolving forms of criminal conduct. Therefore, criminal law reform and the strengthening of regulations governing electronic transactions are necessary to ensure that the legal system can adequately address emerging and continuously developing forms of cybercrime. In addition, preventive measures, enhanced digital security systems, and effective cooperation among government institutions, financial institutions, digital service providers, law enforcement agencies, and the public are essential to protecting users of electronic services against cybercrime.

REFERENCES

- AllahRakha, N. (2024). Cybercrime and the legal and ethical challenges of emerging technologies. *International Journal of Law and Policy*, 2(5), 28–36. <https://doi.org/10.59022/ijlp.191>
- Amoo, O. O., Atadoga, A., Abrahams, T. O., Farayola, O. A., Osasona, F., & Ayinla, B. S. (2024). The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. *World Journal of Advanced Research and Reviews*, 21(2), 205–217. <https://doi.org/10.30574/wjarr.2024.21.2.0438>
- Anastasia, P., Asher, F., & Nicola, H. (2019). *The human factor of cybercrime*. Routledge. <https://doi.org/10.4324/9780429460593>

- Arifin, R., Atikasari, H., & Waspihah, W. (2020). The intersection of criminal law, technology and business commercial law on carding as cyber fraud. *Jurnal Hukum Novelty*, 11(2), 235. <https://doi.org/10.26555/novelty.v11i2.a15700>
- Azizah, S., Asikin, Z., & Parman, L. (2021). Implementation of e-commerce crime law enforcement at the West Nusa Tenggara Regional Police. *International Journal of Multicultural and Multireligious Understanding*, 8(2), 7. <https://doi.org/10.18415/ijmmu.v8i2.2273>
- Baak, C. van, Maher, C. A., Protas, M. E., & Hayes, B. E. (2022). Victims and perpetrators of cyber harassment: The role of power and control and the use of techniques of neutralization. *Deviant Behavior*, 44(5), 690–707. <https://doi.org/10.1080/01639625.2022.2088317>
- Baddam, P. R. (2020). Cyber sentinel chronicles: Navigating ethical hacking's role in fortifying digital security. *Asian Journal of Humanity, Art and Literature*, 7(2), 147–158. <https://doi.org/10.18034/ajhal.v7i2.712>
- Berman, P. S. (2002). The globalization of jurisdiction. *University of Pennsylvania Law Review*, 151(2), 311. <https://doi.org/10.2307/3312952>
- Chen, S., Hao, M., Ding, F., Dong, J., Dong, J., Zhang, S., Guo, Q., & Gao, C. (2023). Exploring the global geography of cybercrime and its driving forces. *Humanities and Social Sciences Communications*, 10, Article 71. <https://doi.org/10.1057/s41599-023-01560-x>
- Davydenko, V. D., Kavunskas, A., & Barba, V. (2025). The role of operational units of the National Police in preventing cybercrime in the context of economic globalisation and existential challenges. *Baltic Journal of Economic Studies*, 11(3), 267–276. <https://doi.org/10.30525/2256-0742/2025-11-3-267-276>
- Duhaidahawi, H. M. K. A., Zhang, J., Abdulreda, M. S., Sebai, M., & Harjan, S. A. (2020). Financial technology (FinTech) and cybersecurity. *International Journal of Research in Business and Social Science*, 9(6), 123–133. <https://doi.org/10.20525/ijrbs.v9i6.914>
- Erikha, A., & Saptomo, A. (2024). Dilemma of legal policy to address cybercrime in the digital era. *Asian Journal of Social and Humanities*, 3(3), 499–507. <https://doi.org/10.59888/ajosh.v3i3.452>
- Fedorov, V., Antoshyna, I., & Biriukov, R. M. (2025). Theoretical and legal foundations of law enforcement collaboration in combating economic crime in Europe. *Baltic Journal of Economic Studies*, 11(4), 177–185. <https://doi.org/10.30525/2256-0742/2025-11-4-177-185>
- Greco, F., & Greco, G. (2020). Organised crime: Underground economy and regulations to combat cybercrime. *European Journal of Political Science Studies*, 4(1). <https://doi.org/10.46827/ejps.v4i1.935>
- Greco, G., & Montinaro, N. (2020). The phenomenon of cybercrime: From the transnational connotation to the need for globalization of justice. *European Journal of Social Sciences Studies*, 6(1). <https://doi.org/10.46827/ejss.v6i1.956>
- Haryono, H., & Myhart, W. S. (2026). Application of criminal law in cybercrime cases related to identity data protection. *Humaniorum*, 4(1), 17–20. <https://doi.org/10.37010/hmr.v4i1.141>
- Hasnia, H., Hafiz, A., Rasna, R., Nurahman, D., & Parhusip, J. (2025). Reconstruction of criminal law policy in handling cybercrime: Perspectives of technology law and human rights. *Jurnal Smart Hukum (JSH)*, 3(3), 254–264. <https://doi.org/10.55299/jsh.v3i3.1328>
- Holt, T. J., Freilich, J. D., & Chermak, S. M. (2017). Exploring the subculture of ideologically motivated cyber-attackers. *Journal of Contemporary Criminal Justice*, 33(3), 212–233. <https://doi.org/10.1177/1043986217699100>
- Imran, M. F., & Gunawa, H. (2025). Investigating the role of cybercrime and e-brand trust on purchase interest of e-commerce platforms. *International Journal of Data and Network Science*, 9(3), 561–574. <https://doi.org/10.5267/j.ijdns.2024.8.010>
- Karo, R. K., & Sebastian, A. J. (2019). Juridical analysis on the criminal act of online shop fraud in Indonesia. *Lentera Hukum*, 6(1), 1. <https://doi.org/10.19184/ejlh.v6i1.9567>
- King, Z. M., Henshel, D. S., Flora, L., Cains, M. G., Hoffman, B., & Sample, C. (2018). Characterizing and measuring maliciousness for cybersecurity risk assessment. *Frontiers in Psychology*, 9, Article

39. <https://doi.org/10.3389/fpsyg.2018.00039>
- Krishna, L. S. (2024). Navigating legal frontiers: Contemporary challenges and regulatory strategies in combating cybercrime. *International Journal for Research Publication and Seminars*, 15(1), 340–351. <https://doi.org/10.36676/jrps.v15.i1.1667>
- Kumar, C. R. (2024). Cybercrime and the law: Challenges in prosecuting digital offenses. *Indian Journal of Law*, 2(5), 20–25. <https://doi.org/10.36676/ijl.v2.i5.53>
- Li, F., Pieńkowski, D., van Moorsel, A., & Smith, C. (2012). A holistic framework for trust in online transactions. *International Journal of Management Reviews*, 14(1), 85–103. <https://doi.org/10.1111/j.1468-2370.2011.00311.x>
- Maimon, D., & Louderback, E. R. (2019). Cyber-dependent crimes: An interdisciplinary review. *Annual Review of Criminology*, 2, 191–216. <https://doi.org/10.1146/annurev-criminol-032317-092057>
- Noor, M. A. F. (2025). Cybercrime and data protection: Emerging legal challenges. *International Journal of Law and Policy*, 3(9), 66–79. <https://doi.org/10.59022/ijlp.369>
- Octora, R. (2021). Regulation on electronic system security for e-wallet in order to protect consumers from financial loss due to cyber fraud based on Indonesian law. *International Journal of Social Science and Human Research*, 4(9). <https://doi.org/10.47191/ijsshr/v4-i9-01>
- Ombu, A. (2023). Role of digital forensics in combating financial crimes in the computer era. *Journal of Forensic Accounting Profession*, 3(1), 57–75. <https://doi.org/10.2478/jfap-2023-0003>
- Putri, C. A., & Prasetyo, P. E. (2020). Money supply, counterfeit money, and economic growth effect to e-money transaction. *Efficient: Indonesian Journal of Development Economics*, 3(1), 634–649. <https://doi.org/10.15294/efficient.v3i1.35951>
- Ramadhan, M., Ariyanti, D. O., & Ariyani, N. (2020). Pencurian e-money pada e-commerce dalam tindak pidana cybercrime sebagai tindak pidana ekonomi. *Reformasi Hukum*, 24(2), 169–188. <https://doi.org/10.46257/jrh.v24i2.179>
- Sabillón, R., M., J. J. C., Reyes, V. C., & Ruiz, J. S. (2016). *Cybercrime and cybercriminals: A comprehensive study*. RECERCAT (Consorti de Serveis Universitaris de Catalunya). <http://hdl.handle.net/10609/78507>
- Sanchez, T., & Omar, A. (2013). Hackers portfolio and its impact on society. *International Journal of Computer Science and Business Informatics*, 3(1). <http://ijcsbi.org/index.php/ijcsbi/article/download/72/21>
- Sarnoff, J. (2022). *Crimes and risks*. Deep Blue, University of Michigan. <https://doi.org/10.7302/6177>
- Šturm, B., Gurova, T., & Chernov, S. (2022). The specifics and patterns of cybercrime in the field of payment processing. *International Journal of Criminology and Sociology*, 9, 2021–2030. <https://doi.org/10.6000/1929-4409.2020.09.237>
- Truntsevskiy, Y., & Ketsko, K. V. (2020). Criminal threats of e-commerce: International and national aspects. *Public International and Private International Law*, 6, 18–22. <https://doi.org/10.18572/1812-3910-2020-6-18-22>
- Volkov, S. S. (2026). Criminal legal characteristics of economic crimes committed using digital technologies. *Police and Investigative Activities*, 1, 200–213. <https://doi.org/10.25136/2409-7810.2026.1.78259>
- Vozniuk, A., Savchenko, A. V., Tarasevych, T., Dudorov, O., & Klymenko, O. A. (2020). Electronic money and payments as means of committing crimes. *Academic Journal of Interdisciplinary Studies*, 9(4), 150. <https://doi.org/10.36941/ajis-2020-0069>
- Zhou, Y., Tiwari, M., Bernot, A., & Lin, K. (2024). Metacrime and cybercrime: Exploring the convergence and divergence in digital criminality. *Asian Journal of Criminology*, 19(3), 419–439. <https://doi.org/10.1007/s11417-024-09436-y>