Law and Justice
Vol. 9, No. 1, 2024, pp. 74-88
e-ISSN : 2549-8282
https://journals2.ums.ac.id/index.php/laj/article/view/6484

The Urgency of Identity Verification and Safeguarding Personal Information During Online Transactions

Anton Satila
Universitas Muhammadiyah Kendari

Sudirman
Universitas Muhammadiyah Kendari

Ismi Fadjriah Hamzah
Universitas Muhammadiyah Kendari
ismi.fadjriah@umkendari.ac.id

Wahyudi Umar
Universitas Muhammadiyah Kendari

Matthias Wetzal
Asia University, Taiwan

DOI: 10.23917/laj.v9i1.6484

Submission Track:

Received:
29 August 2024

Final Revision:
30 August 2024

Available Online:
30 August 2024

Corresponding Author:
Ismi Fadjriah Hamzah
ismi.fadjriah@umkendari.ac.id

ABSTRACT

The complexity of law enforcement in online trading fraud cases poses significant challenges. Sellers can carry out fraudulent activities through product counterfeiting or making transactions outside of e-commerce platforms, while buyers can commit fraud by falsifying identities and making fake orders. Despite efforts to address this problem through legal remedies, the prevalence of fraud has not decreased. In the normative research study, fraudulent behavior is studied related to the provisions contained in the Electronic Information and Transaction Law and the Personal Data Protection Law. These findings underscore the importance of implementing authentication measures to verify the identity of sellers and buyers during online interactions. Authentication methods like this can significantly reduce fraud by allowing for quick identification of perpetrators and tracking of their fraudulent activities, ultimately deterring them from engaging in fraudulent behavior.

Keywords: Verification; Personal Information; Online Transactions.

ABSTRAK

Kompleksitas penegakan hukum dalam kasus penipuan perdagangan online menimbulkan tantangan yang signifikan. Penjual dapat melakukan kegiatan penipuan melalui pemalsuan produk atau melakukan transaksi di luar

platform e-commerce, sementara pembeli dapat melakukan penipuan dengan memalsukan identitas dan membuat pesanan palsu. Meskipun ada upaya untuk mengatasi masalah ini melalui upaya hukum, prevalensi penipuan tidak berkurang. Dalam studi penelitian normatif ini, perilaku penipuan dikaji dengan aturan yang terdapat dalam UU ITE dan UU Perlindungan Data Pribadi. Temuan ini menggarisbawahi pentingnya penerapan langkah-langkah otentikasi untuk memverifikasi identitas penjual dan pembeli selama interaksi online. Metode otentikasi seperti ini dapat secara signifikan mengurangi penipuan dengan memungkinkan identifikasi pelaku dan pelacakan aktivitas penipuan dengan cepat, yang pada akhirnya menghalangi pelaku untuk terlibat dalam perilaku curang.

***Kata kunci**: Verifikasi; Informasi Pribadi; Transaksi Online*

INTRODUCTION

The recent surge in online trade has sparked public enthusiasm. NielsenIQ has reported a dramatic increase in the number of Indonesia consumers engaging in e-commerce, with a projected total of 32 million online shoppers in 2021. This figure increased by 88 percent compared to 2020, when the number reached 17 million. Rusdy Sumantri, Director of Nielsen Indonesia, attributed this growth to an increase in the internet user base in Indonesia by 32 percent, which increased from 34 million to 45 million people this year (Uli, 2021).

In addition, the implementation of government measures to limit mobility to combat the spread of COVID-19 has led to an increase in online consumer activity (Mahsuni & Wahono, 2023). Bank Indonesia estimates that the considerable growth in economic and digital transactions throughout 2021 is due to increasing public interest and e-commerce adoption. It is projected that the value of trade transactions will reach IDR 401 trillion by the end of the year (Aula & Suharto, 2021).

The rise of online transactions has revolutionized the way businesses market and sell their products, overcoming the traditional barriers associated with physical storefronts. This e-commerce model eliminates the need for physical retail space and empowers individuals to buy and sell products easily using just smartphones and social media. However, the convenience of transacting online has its own challenges. High-quality product images taken with advanced cameras can be misleading, as the actual condition of the product may not match the picture.

Additionally, the buyer may engage in fraudulent activities by using someone else's account or credit card information. The absence of face-to-face interaction complicates the authentication process, raising questions about the authenticity of buyer intent and seller trust. This unresolved problem has contributed to the many cases of fraud in the realm of e-commerce. For example, on January 18, 2019, there were 1,253 reports of data card breaches, resulting in

losses of approximately $16 billion due to these fraudulent and criminal activities (Silalahi et al., 2022).

Based on Cekrekening.id data, 115,756 cases of online fraud were reported in September 2021, most of which involved e-commerce and online sales through social media platforms. E-commerce scams often involve enticing buyers to make transactions outside of the official e-commerce platform. In a scenario like this, the buyer is required to make payment for the ordered item, but the seller fails to process the order and then changes his contact information to avoid accountability (Liputan6.com, 2022).

Indonesia has carved out a reputation as the fastest-growing e-commerce market in the world, with 74% of respondents having made an online purchase. However, this rapid expansion is also accompanied by a significant increase in fraudulent activity. On average, 25% of e-commerce participants have experienced criminal fraud cases in various services. This concern was expressed by Dev Dhiman, Managing Director of Southeast Asia and Emerging Markets at Experian Asia Pacific (Utami, Irwan, & Nasution, 2023).

The surge in e-commerce activity in Indonesia has posed challenges such as cybercrime and security concerns. The lack of human resources and low trust in the security of e-commerce are highlighted as obstacles to the successful implementation of e-commerce (S. K. Rahayu, Ruqoyah, Berliana, Pratiwi, & Saputra, 2021). In addition, the adoption of e-commerce by small and medium enterprises (SMEs) in Indonesia is crucial for their survival in the information age and the increasingly digital economic landscape (R. Rahayu & Day, 2015). To address the risks associated with e-commerce transactions, legal frameworks such as the Civil Code play a role in providing protection and compensation to buyers and sellers in the event of unexpected losses, including cybercrime incidents during e-commerce transactions (Ady, Nisrina, Ramadhani, & Irawan, 2022).

Additionally, the design and usability of e-commerce platforms play a crucial role in influencing repurchase intent and user perceptions of usability, ease of use, and trust (Wilson, 2019). Furthermore, the growth of e-commerce in Indonesia not only contributes significantly to the growth of the national economy but also offers opportunities for SMEs to increase their competitiveness and market reach (Wijayanto, Jushermi, Nursanti, Novandalina, & Rivai, 2024). However, to fully take advantage of the benefits of e-commerce, businesses need to address issues related to trust, security, and user experience to foster customer loyalty and repurchase intent (Mulia & Adlina, 2023).

Therefore, research is urgently needed to explore potential authentication measures to address widespread fraud in online commerce. Additionally, it is important to investigate the level of personal data protection available to consumers within the framework of Indonesian law.

RESEARCH METHOD

Doctrinal or normative legal research, which uses law as a fundamental norm, is used in this type of research. The system of norms in question is related to principles, norms, and legislation regarding *the case quo* (Rustan, Hsieh, & Umar, 2021). The first stage of normative research consists of research with the aim of achieving objective law, by researching legal issues. The second stage of normative law research is aimed at obtaining subjective laws (Sung & Umar, 2020). This research will use a legal approach which means using the law as the basis for conducting research (Johnny, 2006).

RESULTS & DISCUSSION

The evolution and transformation of the role of the state are shaped by the process of modernization and democratization in the system of government. This evolution includes the transition from a political state to a state of law and, ultimately, to a welfare state. Each of these paradigms utilizes state authority as a decisive force in shaping the welfare of the people under its government. The emergence of the welfare state is a response to the social disparities inherent in the liberal economic system. Within the framework of the welfare state, the government has a "*freis ermessen*", which means the freedom to be actively involved in all social, political, and economic spheres with the main goal of improving the general welfare and bestuurzorg (Sintha Dewi, 2016).

Historically, the government has played a significant role in regulating the activities of its citizens. The government exercised considerable control over trade, including the licensing of traders, the regulation of goods, and the designation of sales locations. While not a fully regulated system, the regulations that have been established and are currently in place can be readily implemented, given the extensive government control over its people.

However, the modernization process has eliminated the government's authority to regulate its citizens. This is exemplified in the context of online commerce (e-commerce), where the government can no longer strictly regulate the location of sales, sellers, buyers, and imports of goods into Indonesia. Through the internet, individuals are empowered to sell their products through their own websites or virtual marketplaces, thus presenting challenges in law

enforcement and compliance. This situation makes it easier to violate certain laws, thus allowing for a scenario where a minor can easily buy items such as e-cigarettes that do not correspond to his age group while a teenager can easily sell jewelry stolen from his own home.

The government was forced to transform from its traditional role as the ruler of the political state to a state of law, which eventually developed into a welfare state. The welfare state represents a form of democratic government that emphasizes the state's obligation to ensure the basic welfare of its citizens, directing the government to oversee the equitable distribution of state resources to prevent every individual from experiencing deprivation. Countries that fall into this classification usually integrate socialist elements, prioritizing welfare in both the political and economic spheres.

The state has four main functions in the economic field. The first is to provide welfare for the people, which includes support for economic growth and social welfare (Thirlwall & Pacheco-López, 2017). Second, as a regulator, where the state has a role in regulating economic activities to ensure justice, efficiency, and sustainability (Akmal & Fayzullokh, 2023). Third, the state plays the role of entrepreneurs through State-Owned Enterprises (SOEs), which are involved in the operation of certain sectors to advance the country's economy (Ting, Dollery, & Villano, 2014). Fourth, the state also plays a role in managing the budget and government expenditure to support economic growth.

Historically, Indonesia's constitutional framework has demonstrated a commitment to the principles of the welfare state. This commitment can be exemplified in the articulation of economic democracy in the Explanation of Article 33 of the 1945 Constitution which emphasizes the responsibility of the state to control the main branches of production that have an impact on the livelihood of many people. The rationale behind this regulatory framework is to prevent the consolidation of economic resources and the subsequent exploitation of society by those in positions of authority. Indonesia's unwavering commitment to the principles of a welfare state is reinforced by its designation as a constitutional state. By aligning with the ethos of the welfare state, the government is thereby empowered to utilize legal mechanisms for the regulation, control, and guarantee of the well-being of its citizens. It is therefore imperative that a comprehensive national legal framework be developed without delay in order to facilitate the realisation of this obligation.

Fraudulent Models in E-Commerce Transactions

Online scams involving e-commerce and social media platforms have become a significant concern due to the increasing popularity of online shopping and the integration of social elements into the shopping experience. The blend of shopping and social media, known as social commerce, not only improves the efficiency and convenience of online shopping but also plays a crucial role in building trust and loyalty among consumers (Pandowo, Rahmani, & Hapsari, 2024). This trust is crucial in an online environment, especially in the context of e-commerce scams. The growth of the e-commerce market, such as in Malaysia, has been accelerated by factors such as the COVID-19 pandemic, which has led to an increased risk of fraudulent victimization in online transactions (Mohamad, Ismail, & Abdullah Thani, 2023). The design features of the social trading platform utilizing social media and Web 2.0 technology aim to increase customer participation and provide socially rich information, creating a more trustworthy online transaction environment (Lu, Fan, & Zhou, 2016). However, despite these advancements, challenges remain, especially for small and medium-sized enterprises (SMEs), where the perceived benefits of e-commerce may not always align with actual results (Hashim & Abdullah, 2014).

Cybersecurity risks are a significant concern in the realm of digital social media, where the use of various online platforms can expose individuals and businesses to fraudulent activity (Khidzir, Ismail, Daud, Ghani, & Ibrahim, 2016). Malicious actors exploit social media for propaganda, radicalization, and recruitment purposes, further underscoring the vulnerabilities that exist in the online space (Chatfield, Reddick, & Brajawidagda, 2015). In addition, the COVID-19 pandemic has not only shifted cybercrime opportunities but has also raised concerns about cybersecurity implications for individuals, companies, and even state entities (Buil-Gil, Miró-Llinares, Moneva, Kemp, & Díaz-Castaño, 2021).

Strategies to increase public awareness and prevent online fraud are essential to address the rising cases of online fraud (Setyawan, Setyabudi, & Nita, 2023). Understanding the spatiotemporal patterns and driving factors of cyber fraud crime, as seen in studies focusing on regions like China, can provide insights to combat such criminal activities (Chen et al., 2021). Additionally, exploring patterns and classifications of fraud in online sales transactions can help identify attributes that signal potential fraudulent behaviour.

Authentication and application of digital data to minimize fraud rates.

In the realm of digital data, ensuring authenticity and minimizing fraud are important aspects that organizations and individuals need to address. Authentication mechanisms play a crucial role in maintaining data integrity and preventing fraudulent activities. Various techniques and strategies have been developed to authenticate and secure digital data

effectively. One approach to improve data security is through the implementation of watermarking protocols. Watermarking techniques, such as those based on timestamps and holograms, offer solutions for copyright protection and authentication in digital content such as images, videos, and audio (Dittmann, Steinebach, & Croce Ferri, 2002). These protocols provide a means to verify the ownership and authenticity of data, thereby reducing the risk of fraudulent manipulation.

Secure authentication mechanisms are essential for reliable data storage in cloud computing. A multi-user authentication system has been proposed to improve data security in cloud environments, offering organizations comprehensive guidance to address the challenges, benefits, drawbacks, and implementation strategies (Shah & Dubey, 2024). By ensuring that only authorized users can access and manipulate data, these systems contribute to minimizing potential fraudulent activity.

Additionally, technological advancements have led to the development of innovative frameworks such as Communication Pattern-based Data Authentication (CPDA), which is specifically designed to process large data in multiple public cloud environments (Sirapaisan, Zhang, & He, 2020). The Communication Pattern-based Data Authentication framework focuses on ensuring data authenticity and non-repudiation of origin without sacrificing efficiency and scalability. By incorporating communication patterns into the authentication process, the framework strengthens data security measures and reduces the likelihood of fraudulent data changes.

Biometric-based authentication methods have also emerged as a reliable means of verifying user identities and improving data security. Biometric hash algorithms, which use unique biometric characteristics for authentication, offer a robust approach to ensuring data integrity. By leveraging biometric data for authentication purposes, organizations can build more secure and fraud-resistant systems for accessing and managing digital information. In addition to authentication techniques, digital signature algorithms play a crucial role in verifying the authenticity of digital content. Methods such as Digital Signature Algorithms based on Biometric Hashes provide a secure means of validating the integrity and provenance of data (Saxena & Anand, 2017). By incorporating digital signatures into the data verification process, organizations can build a strong foundation for detecting and preventing fraudulent activity in the digital environment.

Protection of Personal Data

Authentication entails validating or verifying a user's identity when seeking access to a specific file, application, or system. Advanced authentication methods may involve the use of personal information, such as biometric fingerprints, to improve account security and prevent unauthorized access by individuals with technical expertise to exploit system vulnerabilities. Effective authentication offers increased assurance that systems and data will be better protected from unauthorized individuals (Tripathi & Nishad, 2020).

Personal data protection is regulated by the Personal Data Protection Law (PDP Law) and the Electronic Information and Transaction Law. According to Article 26, paragraph (1) of Law Number 19 of 2016, the use of all information related to electronic media related to a person's personal data must be carried out with the consent of the person unless otherwise specified by law. Personal data consists of specific personal data and general personal data. Personal data generally includes health data and information, biometric data, genetic data, crime records, child data, personal financial data, and other similar data. It also includes personal details such as full name, gender, nationality, religion, marital status, and any combination of personal data that can be used to identify a person (Permana, 2022).

After the amendment of the 1945 Constitution, the right to privacy, including the protection of personal data, was recognized as a constitutional right of citizens. This is stated in Article 28G paragraph (1) of the 1945 Constitution, which affirms everyone's right to self-protection, family, honor, dignity, and dignity, as well as the property under their control. It also guarantees the right to feel safe and protected from threats or coercion, as well as safeguarding the freedom of individuals to exercise their human rights.

The principles that govern the protection of personal data in the Personal Data Protection Law include: (Anggen Suari & Sarjana, 2023)

1. The protection principle mandates that personal data be processed to prevent misuse and provide protection.
2. The principle of legal certainty ensures that all processing of personal data is carried out on a legal basis, thus guaranteeing legal recognition inside and outside the judicial system.
3. The principle of public interest emphasizes the need to consider the public interest and the wider community in upholding data protection.
4. The principle of usefulness states that regulations regarding the protection of personal data must serve the national interest, especially in realizing the ideals of public welfare.
5. The principle of prudence requires all parties involved in the processing and monitoring of personal data to consider all aspects that have the potential to cause harm.
6. The principle of balance is an effort to protect personal data while maintaining a balance between the right to personal data on the one hand and the legitimate rights of the state based on the public interest.

7. The principle of accountability requires all parties involved to act responsibly in handling personal data.
8. The principle of confidentiality establishes that personal data is protected from unauthorized access and processing.

Data protection refers to a set of actions and regulations that aim to safeguard personal information and ensure that individuals have control over their own data. The data owner must have the ability to determine whether to share the information, who can access it, for what purpose, and for how long, as well as be able to change some of this information. The data protection law is intended to cover data and automated processing, as well as structured storage formats for manual data, including filing systems. This implies that the law must cover all data processing on electronic devices such as computers, telephones, IoT devices, and physical records. This also extends to public and private institutions. However, it is generally recognized that data management for personal or household purposes is exempt from legal provisions. In addition, data protection laws also consider cross-border data movements, which often creates jurisdictional complexity and potential conflicts with national laws.

Article 20 of the Personal Data Protection Law stipulates that the processing of personal data requires written or recorded consent from the data subject, either submitted electronically or in physical form. Without such consent, the processing is considered null and void. Any use of personal data in electronic media must obtain the consent of the data owner. Violation of this provision may result in legal action for the losses incurred. The protection of personal data includes protection against unauthorized use, protection by electronic system operators, and defense against unlawful access and interference.

Furthermore, personal information such as Family Card Number, Population Identification Number (KTP Number), date/month/year of birth, details of physical and/or mental disabilities, biological mother's NIN, father's NIN, and the contents of selected Important Event records available on the internet, as referred to in Article 84 of the Administrative Law, are personal data that must be protected.

Based on the Regulation of the Minister of Communication and Information Technology Number 20 of 2016 (PM 20/2016), which has been effective since December 2016, the protection of personal data includes the protection of the acquisition, collection, processing, analysis, storage, presentation, disclosure, transmission, dissemination, and destruction of personal data in electronic systems. As stated in PM 20/2016, electronic systems used to protect personal data must be certified and establish internal regulations related to the protection of

personal data, considering the application of technology, human resources, methodologies, and costs. Based on PM 20/2016, data owners have the right to maintain the confidentiality of their data, file complaints to resolve personal data disputes, access historical personal data, and request the deletion of certain personal data from electronic systems (Rista Maharani; Andria Luhur Prakoso, 2024).

This personal data is requested if we use the internet in connection with, for example, an e-commerce transaction. The personal data provided may only be used for the purposes approved by the data owner. Article 15 paragraph (2) of Government Regulation No. 71 of 2019 concerning Electronic Systems and Transactions explains that if there is a failure in the protection of personal data managed by it, the Electronic System Operator is obliged to notify in writing to the Personal Data Owner.

The article does not explain the meaning of failure in question. In general, these failures can be categorized into 2 (two). First, procedural failures in confidentiality and security in data processing. Second, system failure in terms of reliability and security aspects of the system used, as well as aspects of the proper functioning of the Electronic System (see Explanation of Article 15 paragraph [1] of the Electronic Information and Transaction Law).

System failures can result from both internal and external factors, with cybercrime being a common external factor. The occurrence of cybercrime activities, including hacking, cracking, phishing, and identity theft, can result in a range of adverse impacts. These may include the leakage of personal data, manipulation of data, violations of privacy, and damage to systems. In the event of a failure to safeguard the confidentiality of personal data, every electronic system implementation is obliged to provide written notification to the data subject. The aforementioned notice must include a detailed account of the reason or cause of the failure in question, as well as confirmation of receipt by the data owner in instances where the failure in question may potentially result in financial losses. It must be issued within 14 days after the failure is identified. In addition, the Personal Data Protection Law provides legal protection for the security of electronic data against unauthorized access, especially in the case of unauthorized system entry that may result in the loss, alteration, or leakage of confidential or personal data.

Based on Article 65 of the Personal Data Protection Law in conjunction with Article 67 of the Personal Data Protection Law, the following provisions are stipulated:

1. Whoever deliberately and unlawfully obtains or collects personal data that does not belong to him, with the intention of benefiting himself or others, resulting in the loss of personal data as referred to in Article 65 paragraph (1), shall be sentenced to

imprisonment for a maximum of 5 years and/or a maximum fine of IDR 5,000,000,000.00 (five billion rupiah).

2. Whoever deliberately and unlawfully discloses personal data that does not belong to him as referred to in Article 65 paragraph (2), shall be sentenced to imprisonment for a maximum of 4 years and/or a maximum fine of IDR 4,000,000,000.00 (four billion rupiah).
3. Any person who deliberately and unlawfully uses personal data that does not belong to him as referred to in Article 65 paragraph (3), is threatened with imprisonment for a maximum of 5 years and/or a maximum fine of IDR 5,000,000,000.00 (five billion rupiah).

If unauthorized access, such as breaking into someone else's system, leads to the potential loss, alteration, or leakage of confidential or personal data, the Personal Data Protection Law offers legal protection for electronic data security against illegal access. Any violation of the law that involves unauthorized access to and acquisition of electronic information/documents by violating the security system is a criminal offense based on Article 65 juncto Article 67 of the Personal Data Protection Law:

1. Whoever deliberately and unlawfully obtains or collects Personal Data that does not belong to him with the intention of benefiting himself or others, resulting in the potential loss of the Personal Data Subject as referred to in Article 65 paragraph (1), shall be sentenced to imprisonment for a maximum of 5 years and/or a maximum fine of IDR 5,000,000,000.00 (five billion rupiah).
2. Whoever deliberately and unlawfully discloses personal data that does not belong to him as referred to in Article 65 paragraph (2), shall be sentenced to a maximum of 4 years in prison and/or a maximum fine of IDR 4,000,000,000.00 (four billion rupiah).
3. Any person who deliberately and unlawfully uses Personal Data that does not belong to him as referred to in Article 65 paragraph (3), shall be sentenced to imprisonment for a maximum of 5 years and/or a maximum fine of IDR 5,000,000,000.00 (five billion rupiah).

The presence of the Personal Data Protection Law has the potential to boost consumer trust by mandating data managers and processors to uphold transparency in handling personal data. In addition, the Personal Data Protection Law creates a conducive environment for business

innovation, as it encourages competition between companies to demonstrate their proficiency in data security management.

CONCLUSION

Digital identity refers to a set of digital records that store a person's identity, which a specific institution manages. The system simplifies the documentation process for citizens and the collection of their important data. Equipped with authentication and advanced security measures, digital identity systems eliminate the risk of theft, forgery, or loss associated with manual identity systems. The presence of a digital identity system allows the financial industry to accelerate the verification and identification of prospective customer data. In addition, this system can also be used to authenticate online shoppers during purchase transactions.

Based on our previous discussion, it can be reaffirmed that sociologically, the online buying and selling system has had a significant impact on people's culture. This change is mainly seen in the identity of sellers and buyers. In offline sales, it is usually not necessary to know the identities of the parties involved in the transaction. Simply expressing the desire to buy, making payments, and facilitating the transfer of goods signifies the completion of the buying and selling process. Even if the parties know their names, residences, and other identities, it is often caused by the establishment of family relationships. This is known as *"tuna sathak profiti sanak"*, which means that building a family is more important than pursuing big profits. He believes that having more brothers brings blessings. In contrast, online buying and selling usually occurs without face-to-face interaction and often involves remote transactions. However, complete identity and details are required to minimize the risk of fraud or fraud. The disclosure of information in online buying and selling raises concerns about the potential misuse of data for criminal activities. In the context of online transactions, the relationship between sellers and buyers is fundamentally transactional and physical, lacking the emotional and mutually supportive elements that are characteristic of offline transactions. This differs from the offline process, which fosters familiarity and emotional relationships between parties, and is characteristic of Indonesia's communal society.

REFERENCES

Ady, E. N. S., Nisrina, F. B., Ramadhani, F., & Irawan, F. (2022). Urgensi KUHD Dalam Menangani Risiko Kejahatan Siber Pada Transaksi E-Commerce. *Journal of Law, Administration, and Social Science*, *2*(1), 45–55. https://doi.org/10.54957/jolas.v2i1.166

Akmal, A., & Fayzullokh, S. (2023). Analyzing the Link Between Government Budget Expenditures and Economic Growth: A Case Study of Uzbekistan's Experience. *International Journal of Professional Business Review*, *8*(7), e02816. https://doi.org/10.26668/businessreview/2023.v8i7.2816

Anggen Suari, K. R., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *6*(1), 132–142. https://doi.org/10.38043/jah.v6i1.4484

Aula, N. K., & Suharto, S. (2021). Pengaruh e-commerce terhadap Produk Domestik Bruto

Indonesia. *Jurnal Kebijakan Ekonomi Dan Keuangan*, *1*(1), 39–48. https://doi.org/10.20885/jkek.vol1.iss1.art4

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2021). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies*, *23*(sup1), S47–S59. https://doi.org/10.1080/14616696.2020.1804973

Chatfield, A. T., Reddick, C. G., & Brajawidagda, U. (2015). Tweeting propaganda, radicalization and recruitment. *Proceedings of the 16th Annual International Conference on Digital Government Research*, 239–249. New York, NY, USA: ACM. https://doi.org/10.1145/2757401.2757408

Chen, S., Gao, C., Jiang, D., Hao, M., Ding, F., Ma, T., … Li, S. (2021). The Spatiotemporal Pattern and Driving Factors of Cyber Fraud Crime in China. *ISPRS International Journal of Geo-Information*, *10*(12), 802. https://doi.org/10.3390/ijgi10120802

Dittmann, J., Steinebach, M., & Croce Ferri, L. (2002). Watermarking Protocols for Authentication and Ownership Protection based on Timestamps and Hologram. In E. J. Delp III & P. W. Wong (Eds.), *Security and Watermarking of Multimedia Contents IV* (Vol. 4675, pp. 240–251). https://doi.org/10.1117/12.465281

Hashim, N. A., & Abdullah, N. L. (2014). Catastrophe of E-Commerce among Malaysian SMEs – Between Its Perceived and Proven Benefits. *Jurnal Pengurusan*, *42*, 145–157. https://doi.org/10.17576/pengurusan-2014-42-12

Johnny, I. (2006). Teori dan Metodologi Penelitian Hukum Normatif. *Bayumedia Publishing*, 299. Retrieved from http://staffnew.uny.ac.id/upload/131808346/pendidikan/metodologi-penelitian.pdf

Khidzir, N. Z., Ismail, A. R., Daud, K. A. M., Ghani, M. S. A. A., & Ibrahim, M. A. H. I. (2016). Critical Cybersecurity Risk Factors in Digital Social Media: Analysis of Information Security Requirements. *Lecture Notes on Information Theory*, *4*(1), 18–24. https://doi.org/10.18178/lnit.4.1.18-24

Liputan6.com. (2022). Waspada Penipuan Terkait E-Commerce, Jaga Kerahasiaan Data! Retrieved July 10, 2024, from Liputan6.com website: https://www.liputan6.com/bisnis/read/4921585/waspada-penipuan-terkait-e-commerce-jaga-kerahasiaan-data

Lu, B., Fan, W., & Zhou, M. (2016). Social presence, trust, and social commerce purchase intention: An empirical research. *Computers in Human Behavior*, *56*, 225–237. https://doi.org/10.1016/j.chb.2015.11.057

Mahsuni, A. W., & Wahono, B. (2023). Dampak Pandemi Covid-19 Terhadap Perekonomian Usaha Mikro Kecil Dan Menengah (Umkm) Kripik Singkong Kelurahan Pandanwangi Kecamatan Blimbing Kota Malang. *Fair Value : Jurnal Ilmiah Akuntansi Dan Keuangan*, *5*(7), 3133–3144. Retrieved from http://repository.uisu.ac.id/bitstream/123456789/1160/1/Cover%2C Bibliography.pdf

Mohamad, Z., Ismail, Z., & Abdullah Thani, A. K. (2023). Determinants of Fraud Victimizations in Malaysian E Commerce: A Conceptual Paper. *International Journal of Academic Research in Business and Social Sciences*, *13*(12). https://doi.org/10.6007/IJARBSS/v13-i12/20395

Mulia, N. T., & Adlina, H. (2023). The Effect of Perceived Trust And Perceived Enjoyment on Repurchase Intention (Study on Tokopedia Users in Medan City). *Journal of*

Humanities,Soccial Sciences And Business, *3*(1), 295–305. Retrieved from https://ojs.transpublika.com/index.php/JHSSB/

Pandowo, A., Rahmani, S., & Hapsari, A. A. (2024). Social Commerce Surge: The Fusion of Shopping and Social Media. *Journal of Economic, Bussines and Accounting (COSTING)*, *7*(4), 7902–7907. https://doi.org/10.31539/costing.v7i4.10435

Permana, S. (2022). Pengaturan Perlindungan Data Pribadi Konsumen Jasa Keuangan dalam Penggunaan Uang Elektronik Berbasis Server. *Veritas et Justitia*, *8*(2), 386–414. https://doi.org/10.25123/vej.v8i2.5213

Rahayu, R., & Day, J. (2015). Determinant Factors of E-commerce Adoption by SMEs in Developing Country: Evidence from Indonesia. *Procedia - Social and Behavioral Sciences*, *195*, 142–150. https://doi.org/10.1016/j.sbspro.2015.06.423

Rahayu, S. K., Ruqoyah, S., Berliana, S., Pratiwi, S. B., & Saputra, H. (2021). Cybercrime dan dampaknya pada teknologi e-commerce. *Journal of Information System, Applied, Management, Accounting and Research*, *5*(3), 632. https://doi.org/10.52362/jisamar.v5i3.478

Rista Maharani; Andria Luhur Prakoso. (2024). Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital Protection of Consumer Personal Data by Electronic System Providers in Digital Peningkatan substansial dalam penggunaan platform e-commerce di Indonesia telah. *Jurnal Usm Law Review*, *7*(1), 333–347.

Rustan, A., Hsieh, J., & Umar, W. (2021). Maladministration on Mining Business Licenses : Case Study " Mining Business License Production Operation PT . Aneka. *Varia Justicia*, *17*(3), 246–257.

Saxena, S., & Anand, D. (2017). A Novel Digital Signature Algorithm based on Biometric Hash. *International Journal of Computer Network and Information Security*, *9*(1), 12–19. https://doi.org/10.5815/ijcnis.2017.01.02

Setyawan, A., Setyabudi, C. M., & Nita, S. (2023). Strategy To Build Public Awareness In Preventing Online Fraud Crimes In The Jurisdiction Of The Cimahi Police. *International Journal of Social Service and Research*, *3*(10), 2641–2649. https://doi.org/10.46799/ijssr.v3i10.563

Shah, R., & Dubey, S. K. (2024). Multi User Authentication for Reliable Data Storage in Cloud Computing. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *10*(2), 82–89. https://doi.org/10.32628/CSEIT2410138

Silalahi, P. R., Salwa Daulay, A., Siregar, T. S., Ridwan, A., Islam, E., Ekonomi, F., & Islam, B. (2022). Analisis Keamanan Transaksi E-Commerce Dalam Mencegah Penipuan Online. *Jurnal Manajemen, Bisnis Dan Akuntansi*, *1*(4), 224–235.

Sintha Dewi, D. A. (2016). Pendayagunaan Freies Ermessen Pejabat Pemerintahan Dalam Konsep Negara Kesejahteraan. *Yustisia Jurnal Hukum*, *5*(1), 184–194. https://doi.org/10.20961/yustisia.v5i1.8730

Sirapaisan, S., Zhang, N., & He, Q. (2020). Communication Pattern Based Data Authentication (CPDA) Designed for Big Data Processing in a Multiple Public Cloud Environment. *IEEE Access*, *8*(1), 107716–107748. https://doi.org/10.1109/ACCESS.2020.3000989

Sung, M.-H., & Umar, W. (2020). A New Industry and Tax Base on Taxing Esports in Indonesia. *Jurnal Media Hukum*, *27*(2), 147–165. https://doi.org/10.18196/jmh.20200148

Thirlwall, A. P., & Pacheco-López, P. (2017). The Role of The State In Economic Development. In *Economics of Development* (pp. 257–280). London: Macmillan Education UK. https://doi.org/10.1057/978-1-137-57795-5_9

Ting, S. K., Dollery, B., & Villano, R. (2014). Administrative scale economies in local government: An empirical analysis of Sabah municipalities, 2000 to 2009. *Urban Studies*, *51*(13), 2899–2915. https://doi.org/10.1177/0042098013512873

Tripathi, D. R., & Nishad, D. K. (2020). Biometric Authentication Systems: A Survey. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *11*(3), 2878–2884. https://doi.org/10.61841/turcomat.v11i3.14653

Uli. (2021). Konsumen Belanja Online RI Melonjak 88 Persen pada 2021.

Utami, A., Irwan, M., & Nasution, P. (2023). Perkembangan Pasar Online (E-Commerce) Di Era Modern Dan Pengaruhnya Terhadap Kepercayaan Konsumen. *Jurnal Ekonomi Manajemen Dan Bisnis*, *1*(2), 126–132. Retrieved from https://doi.org/XX..XXXXX/JMEB

Wijayanto, G., Jushermi, J., Nursanti, A., Novandalina, A., & Rivai, Y. (2024). The Effect of E-commerce Platforms, Digital Marketing, and User Experience on Market Reach and Competitiveness of Indonesian MSMEs. *International Journal of Business, Law, and Education*, *5*(1), 811–823. https://doi.org/10.56442/ijble.v5i1.492

Wilson, N. (2019). the Impact of Perceived Usefulness and Perceived Ease-of-Use Toward Repurchase Intention in the Indonesian E-Commerce Industry. *Jurnal Manajemen Indonesia*, *19*(3), 241. https://doi.org/10.25124/jmi.v19i3.2412