

The fading social trust capital due to cybercrime in e-commerce transactions in Indonesia: The perspective of the electronic information and transaction law

Any Farida¹, Khudzaifah Dimiyati², Absori³, Kelik Wardiono⁴, Arief Budiono^{5*}

¹Faculty of Law, Universitas Muhammadiyah Surakarta, Surakarta, Central Java Indonesia; any.farida@gmail.com (A.F.)

^{2,3,4,5}Faculty of Law, Universitas Muhammadiyah Surakarta Pabelan, kartasuro, Sukoharjo, Central Java Indonesia; kd255@ums.ac.id (K.D.), abs154@ums.ac.id (A.), kelik.wardiono@ums.ac.id (K.W.), ab368@ums.ac.id (A.B.)

Abstract: Trade through electronic systems (e-commerce) is a prominent innovation of this current era. The growth of e-commerce in Indonesia is the highest in the world. Even so, there are threats to security in e-commerce due to cybercrimes, especially system interference. This leads to society's fading trust to e-commerce businesses as a social capital. The Indonesian government has carried out efforts to prevent and handle cybercrimes through stipulations of the Law on Electronic Information and Transaction. Unfortunately, cybercrimes, especially disturbances to the electronic system, still rampantly happen. Therefore, this research focuses on how far the Indonesian Law on Electronic Information and Transaction can reach that cybercrime. This was normative legal research which was a form of doctrinal legal research. It employed a data searching method in the form of library research, i.e., studying primary and secondary legal sources and analyzing them using the descriptive qualitative method with deductive logic. Results of this research showed that the Indonesian Law on Electronic Information and Transaction which keeps on experiencing amendments has not reached cybercrimes, especially crimes related to disturbances to the electronic system (system interference). It is not yet effective in guaranteeing the security of e-commerce transactions, leading to the fading of trust as a social capital. The amendment of the Law on Electronic Information and Transaction must be followed with the amendment of its implementing laws. Society must also be introduced to the importance of the Indonesian Law on Electronic Information and Transaction through massive and intensive education programs.

Keywords: Cybercrime, E-commerce, Electronic information and transaction, Law, Trust, Indonesia.

1. Introduction

The massive development of knowledge and technology due to globalization has influenced various aspects of society's lives, including changes in its legal system [1]. Technological advancement has been used to ease the lives of human beings [2]. An example of how technologies bring ease to human life is the emergence of electronic commerce (e-commerce) which is used for trade transactions [3].

E-commerce means electronic transactions in the business world that encompasses the spread, the sales, the purchasing, and the marketing of goods and services without a direct meeting between the transacting parties through electronic systems such as the internet, televisions, websites (www/world wide web), or other computer networks [4]. The development of e-commerce in Indonesia has happened since 1996, with the founding of Dyviacom Intrabumi or D-Net (www.dnet.net.id). It was the pioneer of online transactions in Indonesia [3].

According to Matthew Driver, the President of Master Card for the Southeast Asian territory, Indonesia is one of the countries with the greatest growth in the e-commerce market in Asia Pacific, [5]. According to the report of the Bank of Indonesia's annual meeting in 2021, Indonesia's e-commerce transactions were projected to reach Rp 403 trillion in 2021. Then, even more impressively, it reached

Rp 530 trillion, meaning that it grew by 31.4% in 2022 [6]. This number is predicted to keep on rising to US\$ 81 billion by 2025 [7].

In 2022, Indonesia experienced an economic recovery after surviving the Covid-19 pandemic. A survey from Indonesia Statistics in 2023 showed that there was an increase in economic growth by 3.70 % in 2021. Then, it grew to 5.31 % in 2022. Concerning the growth in the number of e-commerce businesses in 2022, it was shown that there was an increase of 4.46 %, with a total of 2,995,986 businesses [8].

An e-commerce research agency from Germany, ECDB, stated that Indonesia is the country with the highest projection of e-commerce growth in the world in 2024, with a growth rate reaching 30.5%. This projection was almost thrice greater than the global average, which was 10.4%. The prediction of the country with the second highest e-commerce growth in the world was Mexico, which reached 26.8%. The third was Thailand with a growth rate of 22.9%. The fourth and fifth places were filled by Iran and Malaysia, each with a percentage of 22.1% and 21.4%. This list was then followed by the Philippines, Peru, India, to Vietnam, as shown in Figure 1. ECDB stated that the list of 10 countries with the highest projection of e-commerce growth was dominated by Asian countries [9].

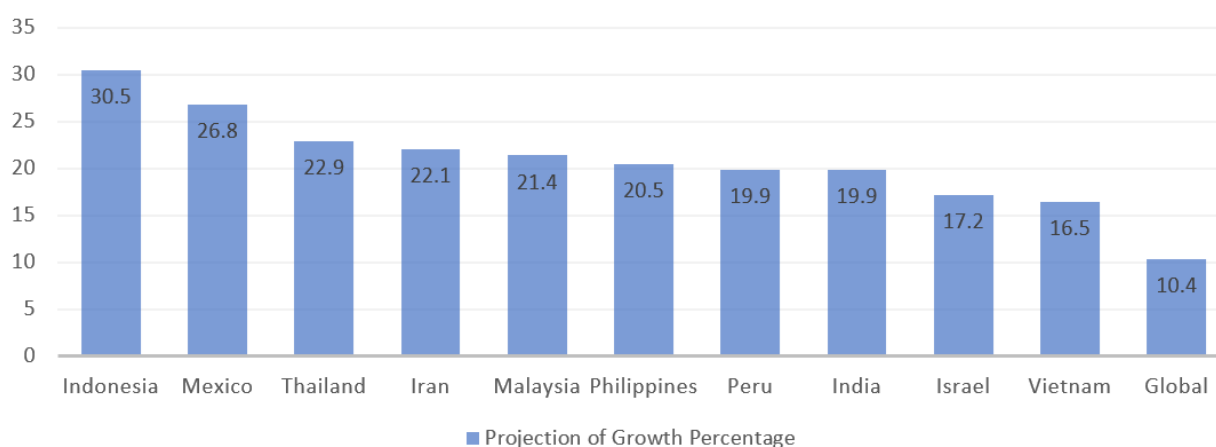







Figure 1. Countries with the highest projection of e-commerce growth in the world according to ECDB [9].

E-commerce data in Indonesia in 2024 showed that around 46.7 million people shop online. Then, in 2029, it is projected that it will reach 133.78 million people. Five e-commerce platforms in Indonesia that are most visited by consumers are shown in Table 1 [10].

Table 1. The five most visited e-commerce platforms in Indonesia.

No	E-Commerce platform	Visits per month	Direct	Male subjects	Age
1	 Shopee	442.4 million	67.7 %	57 %	25-34
2	 Lazada	280.7 million	19.57 %	61 %	25-34
3	 Tokopedia	239.4 million	55.6 %	59.61%	25-34
4	 Bibli	61.5 million	48.16 %	61.17 %	25-34
5	 Bukalapak	8.7 million	50.99 %	62.05 %	25-34

The increase in the e-commerce industry reflects the massive development of internet information technologies that keep on becoming more sophisticated [11]. However, the ease proposed by internet technologies also brings risks to security, such as the emergence of cybercrimes [12]. Cybercrimes in e-

commerce are often related to the security of personal data [13]. Some forms of cybercrimes in e-commerce include payment scams using credit cards (carding), personal data theft (phishing), and data forgery [14].

Cybercrimes bring losses to both e-commerce business owners and consumers. Examples of cybercrimes in Indonesian e-commerce sites/applications include:

1. On May 1st, 2020 there was a news report on the leakage of Tokopedia user data. A staggering 91 million data that were reported as Tokopedia user data were auctioned with a price of US\$5.000 in a hacker forum. In its official release, Tokopedia stated that they “have found the existence of the efforts of Tokopedia user data theft.”
2. On May 6th, 2020, as many as 12.9 million Bukalapak user data were sold. It was suspected that these data were leaked in March 2019. Meanwhile, in its official release, Bukalapak admitted that there was an invalid access to their cold storage.
3. On May 10th, 2020, 1.2 million data that were suspected to be data from the Bhinneka online shop were known to have leaked and were offered to be sold on the dark web. Bhinneka stated that it is still undergoing an investigation into the suspected case of leakage [11].

Even though e-commerce in Indonesia has a great potential market, there are still many hindrances in its application. Some examples of such issues are the issue of expeditions, where the delivery of goods requires much cost and frequently arrives late. Then, there is also a need for a product quality guarantee as well as a guarantee on the protection of consumer data privacy [15].

Therefore, there is a need for the transparency of e-commerce companies as well as strong state policies that provide protection against cybercrimes to build trust between e-commerce business owners and consumers. This is required to build a safe and trustworthy e-commerce environment [15].

As a form of digital transformation in the economy, e-commerce obliges the existence of the development of a trust framework from consumers. Trust may be defined as the consumers’ assessment of the vulnerability of a situation when carrying out a transaction with a company [16]. There are at least six issues that are directly related to consumer trust (the protection of online consumers), namely the protection of personal information, the protection from unsolicited electronic advertisements (spam messages), domestic regulation framework, transparency, cyber security, as well as the use of the internet for electronic trade [17].

Seeing the urgency of security in e-commerce transactions, in 2008, the Indonesian government issued a regulation that specially regulates transactions through the internet, namely Law No. 11 of 2008 on Electronic Information and Transaction, which was amended into Law No. 19 of 2016. Then, the last amendment was Law No. 1 of 2024 [18]. Apart from that, there was also Law No. 27 of 2022 on Personal Data Protection and Law No. 8 of 1999 on Consumer Protection. The Law on Consumer Protection was enacted by considering several principles in consumer protection, namely the principle of benefit, the principle of justice, the principle of security and safety, the principle of balance, as well as the principle of legal certainty [19].

From the description above, even though the government has issued legal regulations on Personal Data Protection, Consumer Protection, and e-commerce transactions, in reality, cybercrimes are still rife. This is the cause of the low trust index and consumer trust index in Indonesia. It is the obligation of governments from all countries of the globe to protect consumers by building effective security to prevent cybercrimes. A strong security system as well as an awareness of carrying out online transactions may protect people from cybercrimes [20]. Therefore, this research discusses how far the Indonesian Law on Electronic Information and Transaction can prevent cybercrime in e-commerce transactions as well as its implications towards trust as a social capital.

2. Literature Review

2.1. Trust as a Social Capital

Social capital is a resource whose value is directly related to the type of capital produced. Trust is the basis of interindividual cooperation, making it a key element in social capital [21]. Fukuyama in his book “The Social Virtues and The Creation of Prosperity” stated that “trust” is how far a person believes

that other people act responsibly for the good of the public [22]. Bryk and Schneider found that individuals tend to trust people who show respect, attention, competence, moral integrity, and commitment [23].

Trust is often identified as a social capital. It is the basis of the relationship between civil society members [24]. Trust may be defined as one's willingness to be sensitive to other people's actions, with the hope that these people will carry out specific actions based on those who trust them without needing to be monitored or controlled by the people who trust them [25]. Trust in the economic scope may be defined as a customer's assessment of a company's integrity and honesty. It also includes customers' perception and belief that the company will not disappoint them and will work hard to fulfil their interests [16].

In line with the development of technologies, the scope of community civilization keeps on penetrating the digital world, including the economic sector. This is marked by the emergence of social media and e-commerce websites/applications. Previous studies opined that trust as a social capital element plays an important role in determining a person's willingness to undergo various transactional activities with companies in the e-commerce sector, as all of its transactions are carried out online [26].

Previous research mentioned that there are at least four types of trust in the e-commerce context, namely: customers' trust to sellers, public trust, the trust to technologies, as well as sellers' trust to customers. Customers' concerns become the most severe hindrance in building trust in e-commerce. Meanwhile, the factors that take the main attention of online customers are privacy, security, risks in using technologies, as well as the issue of integrity [27].

2.2. E-Commerce

E-commerce or what is called electronic commerce is a combination of electronic and internet media for operating goods and services as well as processing digital information in business transactions [28]. The emergence of e-commerce has become one of the greatest technological developments in the last two decades, which has led to a revolution in the global trade industry. E-commerce has some advantages, including higher flexibility, greater market expansion, lower cost structures, quicker offers, more variation production channels, as well as offering more comfort and adaptation [29].

E-commerce becomes a source of information in transactional activities or commercial activities. It is supported by several features, such as social media, customer reviews, discussions, and recommendations for sharing. Three factors encourage society to carry out digital or online transactions, namely fulfilling needs, the availability of access, and time efficiency [30]. E-commerce is differentiated into several forms: Business to Business (B2B) e-commerce, which includes almost anything that encompasses electronic transactions carried out between companies; Business-to-Consumer (B2C) e-commerce or a type of e-commerce which is carried out between production companies and consumers; and Consumer to Consumer (C2C) e-commerce or a type of commerce with electronic transactions that is carried out between consumer and consumer by involving a third party that has provided online marketplace in carrying out transactional activities [31].

In 2022, Iprice Insight Map of E-commerce stated that there are several types of e-commerce in Indonesia. The top ten e-commerce sites and applications are, Tokopedia, Shopee, Lazada, Bukalapak, Blibli, Orami, Ralali, Zalora, Klik Indomaret, and JD ID. Tokopedia was the e-commerce site/application with the highest number of monthly visitors, reaching a staggering 158,346,667 people [32].

In line with its development, e-commerce which was initially focused on selling various physical products such as books, electronics, and clothes has now expanded into various sectors, including travel (booking plane tickets and hotels), foods and beverages (food delivery), entertainment (streaming music and film), etc. Even so, the existence of e-commerce still faces various challenges, such as the challenge of increasing safety in transactions, handling logistic and delivery issues, as well as increasing consumer protection [33].

2.3. Cybercrime

Cybercrime is a form of crime that is carried out through illegal access, such as illegal transmissions or data manipulation for certain goals, including creating disturbances and seeking financial gain. Such crimes may be carried out by individuals or groups of people [34]. Data from reports in 2021 stated that cybercrime can happen due to several factors: 53% of them happened due to system failure, 39% of them happened due to human error, 3% of them happened due to natural phenomena, and the rest, i.e., 5% of them happened due to malicious actions [35].

Cybercrime is also known as cyber sabotage and extortion. It is carried out by injecting computer viruses or certain computer programs that may make computer data and programs unusable. They may not work as how they should. Thus, they may be controlled according to the perpetrators' desires, [36]. Some of the most common forms of cyber-attacks are the attacks of destructive software (malware), personal data theft (phishing), the attack to access with ransom (ransomware), password hacking (dictionary attack), denial of service attack (DOS), and data theft from the database (structured query language injection) [37].

The emergence of e-commerce which fully utilizes the internet as its activity platform opens doors to various threats of cybercrimes. Some forms of cybercrimes that are most popularly found in e-commerce are phishing, data forgery, and carding or fraud of payment using credit cards [14].

Phishing is a term that refers to various cybercrimes that are carried out by sending a link to internet users in an effort to steal personal information such as banking details, Personal Identification Number (PIN) codes, as well as social media information [38]. Meanwhile, data forgery is an effort to illegally forge or copy e-commerce user data with the aim of bringing losses to other parties for one's personal benefit [39].

Previous research by Batmetan found that of the 30 who served as research samples, 78% of them chose to use e-commerce. Then, 80% of the people who chose to use e-commerce stated that in several marketplaces, there are frequent cases of online scams or frauds [12]. This shows that some people still have concerns about using e-commerce.

3. Research Method

This research employed the juridical normative approach with the statute approach and conceptual approach. The legal materials used in this research comprised primary and secondary legal materials [40]. The primary legal materials consisted of Law No. 11 of 2008 on Electronic Information and Transaction, which was amended into Law No. 19 of 2016 was amended into Law No. 1 of 2024 on Electronic Information and Transaction; Law No. 27 of 2022 on Personal Data Protection; Governmental Regulation No. 71 of 2019 on Electronic System Establisher; and Governmental Regulation No. 80 of 2019 on Trade Through Electronic Systems.

Then, the secondary legal materials that were used in this research included legal journals, legal books, as well as articles on websites that were relevant to the researched topic. This research was doctrinal legal research with a normative characteristic. In essence, it was an activity where researchers reviewed the internal aspects of the positive law to resolve its issues. The authors employed descriptive qualitative analysis with deductive logic [41].

4. Results

Information technology and electronic transactions have brought significant changes to various aspects of life. They have become a basis for the development of the digital economy by facilitating various activities, such as communication, trade, to online financial transactions. These technological developments do not only bring great impacts to various sectors, but they also present other challenges related to data security and privacy [42].

As what is written in Article 1 clause (3) of the Third Amendment of the Republic of Indonesia's 1945 Constitution, Indonesia is a legal state. Therefore, its activities, including those related to information technology and electronic transactions, are based on the law. The law regulates electronic information and transactions, which is stipulated in Law No. 11 of 2008 on Electronic Information and Transaction which was amended with Law No. 19 of 2016 that was then amended into Law No. 1 of 2024 on Electronic Information and Transaction [43].

The second amendment of the Law on Electronic Information and Transaction, i.e., Law No. 1 of 2024 aimed to protect Indonesia's digital realm, making it clean, healthy, ethical, productive, and just. Thus, information technology and electronic transactions need to be regulated by providing legal certainty and justice. It must protect the public interest from any disturbances that may lead to the misuse of electronic information, electronic documents, information technology, and/or electronic transactions that may disturb public order. These changes also bring clarity to the emergence of multi-interpretations and controversies in society. Such changes aimed to manifest justice in society and legal certainty.

Changes in the Law on Electronic Information and Transaction related to cybercrimes in e-commerce include [44]:

1. Changes in existing articles to refine Law No. 19 of 2019 to provide legal certainty and societal protection in the digital realm, i.e., Article 17 on electronic transactions, by adding stipulations on the obligations of electronic system establishers to maintain the safety of electronic information and personal data. Articles 27, 27 A, 27 B, 28, 29, and 36 stipulate prohibited actions to rediscuss and clarify articles that are deemed multi-interpretable, adding several prohibited actions and strengthening criminal sanctions. Then, Article 40 regulates the government's role in forming the National Policy Board of Personal Data Protection.
2. The addition of a new article, namely Article 13 A on digital identity is used in establishing digital-based electronic certification, which is electronic data that can be used to electronically identify a person. The application of this article is hoped to increase the security and reliability of electronic certification because digital identity can be used to make sure that the person filing for an electronic certification proposal is the real person, rather than artificial intelligence. Thus, this can be used to prevent the misuse of identity and fraud. Articles 16 A and 16 B regulate child protection. These articles regulate the obligation of electronic system establishers to provide protection to children who use or access the electronic system. Therefore, electronic system establishers must provide information on the minimum age of children that can use or access their service products. It must provide a mechanism for verifying child users as well as a mechanism for reporting the misuse of products, services, or features that violate or may potentially violate children's rights. The addition of these articles aims to provide protection to children in the digital realm, filter dangerous content, and prevent the misuse of children in the digital realm. Article 18A stipulates international electronic contracts, i.e., contracts that are electronically carried out between parties in different countries. This article aims to give legal certainty and safety for electronic system users and electronic system establishers in carrying out international electronic transactions. Article 40 A regulates the government's role in encouraging the creation of a just, accountable, safe, and innovative digital ecosystem. The role of the government includes carrying out education to society and introducing them to responsible use of the digital realm; developing policies and regulations that support a better creation of the digital realm; and carrying out monitoring and law enforcement against the violation of the Law on Electronic Information and Transaction.

5. Discussion

The application of the Electronic Information and Transaction Law which becomes the legal protection over electronic transaction encompasses several things, such as the aspect of data security, consumer protection, and the use of social media in transactions [45]. In the Electronic Information and Transaction Law, "the principle of legal certainty" is the legal basis where the use of information technology and electronic transactions and anything that supports its application is legally acknowledged within and outside of the court [7].

Implementing regulations of the Electronic Information and Transaction Law that provide protection against cybercrimes in e-commerce businesses are Governmental Regulation No. 71 of 2019 on Electronic System Establisher and Governmental Regulation No. 80 of 2019 on Trade Through Electronic Systems. Governmental Regulation No. 71 of 2019 on Electronic System Establisher contains stipulations on the protection against cybercrimes in e-commerce businesses as follows:

Article 14 clauses (1) to (6) states that electronic system establishers must implement the principle of personal data protection in processing personal data. Article 24 clauses (1) to (4) states that electronic system establishers must have and carry out procedures and facilities in securing electronic systems to prevent and handle threats and attacks that cause disturbances, failure, and harm. Article 31 stipulates that electronic system establishers are obliged to protect their users and society in general from the losses that are caused by the electronic system it established. Article 51 states that electronic system establishers must have electronic certificates. Article 74 states that feasibility certificates aim to protect consumers in electronic transactions and as a guarantee that business owners have fulfilled the criteria determined by the Feasibility Certificate Institution.

Article 94 states that the government has the role to protect public interests from all types of disturbances as impacts of the misuse of Information technology and electronic transactions that disturb public order. Article 100 clause (1) regulates administrative sanctions for violators of the stipulations in this Governmental Regulation in the forms of (2): written warning; administrative fines; temporary termination; access severance; and/or being exempted from the list; (3) administrative sanctions are imposed by the Minister according to the stipulations of legal regulations; (4) the imposition of administrative sanctions as aforementioned in clause (2) letter c and letter d is carried out through coordination with the leaders of the related Ministry or institution; (5) the imposition of administrative sanctions as aforementioned in clause (2) and clause (3) does not eliminate criminal and civil liability.

Governmental Regulation No. 80 of 2019 on Trade Through Electronic Systems provides protection against cybercrime, starting from Article 3 which regulates the principles in implementing trade through electronic systems (e-commerce). These principles are good faith, carefulness, transparency, trust, accountability, balance, justice, and healthiness.

Article 13 stipulates the obligations of e-commerce applications/websites, namely:

1. Providing clear, correct, and honest information on the identity of the legal subject that is supported by valid data or documents; provide information on the condition and guarantee of the offered goods and/or services including electronic systems and their characteristics, functions, and roles in that transaction; and fulfil the stipulations on advertising ethics according to the legal regulations.
2. Providing clear, correct, and honest information as aforementioned in clause (1) which at least encompasses information truthfulness and accuracy; accordance between the advertised information and the physical condition of the items; feasibility of the consumption of such goods and/or services; the legality of the goods and/or services; and the quality, price, and accessibility of the goods and/or services.

Article 14 states that domestic and/or foreign Trade Through Electronic Systems must use electronic systems that are certified with an electronic systems feasibility certificate according to the legal regulations.

Article 24 clause (1) states that domestic and/or foreign Trade Through Electronic Systems must maintain the electronic systems, making sure that they are safe, feasible, and responsible. They must build the public's trust towards their established system. Therefore, (2) it must provide an electronic system security that encompasses prevention and handling procedures and systems against threats and attacks that cause disturbances, failure, and harm. (3) electronic system security may encompass security from the aspect of domestic and/or foreign Trade Through Electronic Systems' computer system or aspect of the communication network that is used and established by other parties.

Article 25 clause (1) states that domestic and/or foreign Trade Through Electronic Systems must keep the Trade Through Electronic Systems' data and information that are related to financial transactions for at least 10 (ten) years and data that are not related financial transactions for at least 5 (five) years since the data and information obtainment; and (2) the aforementioned data and information in clause (1) must at least contain information on customers; electronic offers and electronic demands; electronic confirmation, payment confirmation; goods delivery status; trade complaints and disputes; electronic contracts; and the type of goods and/or services sold.

Article 26 states that business owners must protect consumer rights according to the stipulations of legal regulations in the consumer protection sector and comply with stipulations of legal regulations in the business competition sector.

Article 27 clause (1) stipulates that business owners must provide complaint services for consumers; and (2) complaint services as stipulated in clause (1) must at least contain complaint contact address and phone number; procedures of consumer complaint; complaint follow-up mechanisms; officers that are competent in processing complaint services; and the period needed to resolve a complaint.

Article 59 clause (1) states that business owners must keep personal data according to the standard of personal data protection or the appropriate business practices according to the development; (2) the standard of personal data protection; (3) in the case where owners of the personal data state exit, unsubscribe, or stop from using Trade Through Electronic Systems' services and facilities, the personal data owners have the right to ask business owners to eradicate all of their personal data; and (4) under the request of the personal data owners, business owners must eradicate all of their personal data in the system they manage.

Article 80 clause (1) states that business owners that violate the stipulations are imposed with administrative sanctions by the Minister; and (2) these administrative sanctions may be in the form of a written warning; being inserted into the list of prioritized monitoring; blacklisted; having its domestic and/or foreign Trade Through Electronic Systems' services temporarily blocked by the authorized related institutions; and/or the revocation of its business permit.

The Indonesian material cyber law in the forms of legal regulations above has not truly protected Trade Through Electronic System business actors if its law enforcement is still weak, especially considering that the sanctions stipulated in these regulations are only administrative ones. These sanctions only apply to electronic system establishers and trade through electronic system/e-commerce actors. Perpetrators of cybercrime in the forms of the attack of destructive software (malware), personal data theft (phishing), the attack to access with ransom (ransomware), password hacking (dictionary attack), etc. that are forms of disturbances in the electronic system (intrusion) are not touched by these laws.

The second amendment to the Law on Electronic Information and Transaction, namely Law No. 1 of 2024 has the spirit to make the e-commerce climate in Indonesia grow for a betterment. Therefore, it needs to immediately establish intensive and massive education for society, including e-commerce actors and electronic system establishers. It must also be followed by changes in its implementing regulations. Thus, Governmental Regulation No. 71 of 2019 on Electronic System Establisher and Governmental Regulation No. 80 of 2019 on Trade Through Electronic Systems needs to immediately be amended.

The suboptimum protection against cybercrimes in e-commerce businesses may lead e-commerce business actors (both business owners and consumers) to refrain from undergoing transactions due to their distrust over security in these electronic transactions. Their trust fades due to cases of personal data privacy leakage. Trust as a social capital in e-commerce businesses is crucial, as without it, e-commerce will not exist.

The protection against cybercrimes in the form of electronic system disturbance (system interference) may only be obtained in Law No. 27 of 2022 on Personal Data Protection. Unfortunately, its law enforcement is still suboptimum, especially in its formal process to prove such crimes.

6. Conclusion

From the perspective of the Electronic Information and Transaction Law in Indonesia, Cybercrimes that are a form of disturbance in the electronic system (system interference) in e-commerce transactions still cannot optimally be prevented and handled. This leads to the fading trust of consumers as a social capital among e-commerce actors. This may inhibit the state's economic growth in general and especially the growth of e-commerce.

Amendments to the Electronic Information and Transaction Law as the legal basis to this must be followed by changes in its implementing regulations. This is so that changes in these regulations to bring legal certainty and protection to society as well as create a safe, accountable, just, and innovative digital ecosystem for everyone may be achieved.

Acknowledgement:

This research funded by DRTPM DIKTI Ministry of Education Republic of Indonesia with contract 108/E5/PG.02.00/PL/2024, Contract 007/LL.6/PB/AL/04/2024 and 196.73/A.3-III/LRI/VI/2024

Copyright:

© 2024 by the authors. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

References

- [1] B. Parker, "Evolution and Revolution: From International Business to Globalization," in *Managing Organizations: Current Issues*. Los Angeles, Washington DC, and Toronto: SAGE Publications Ltd, 2012. doi: 10.4135/9781446218563.
- [2] W. R. Jati, "Memahami Globalisasi sebagai Evolusi Kapitalisme (Understanding Globalization as the Evolution of Capitalism)," *Jurnal Global dan Strategis (Global and Strategic Journal)*, vol. 7, no. 2, pp. 241–258, 2013, [Online]. Available: <https://journal.unair.ac.id/JGS@memahami-globalisasi-sebagai-evolusi-kapitalisme-article-6326-media-23-category-8.html>
- [3] T. Mustajibah and A. Trilaksana, "Dinamika E-Commerce di Indonesia Tahun 1999-2015 (Dynamics of E-Commerce in Indonesia 1999-2015)," *Jurnal Pendidikan Sejarah (Journal of History Education)*, vol. 10, 2021, [Online]. Available: <https://ejournal.unesa.ac.id/index.php/avatara/article/view/40965>
- [4] M. Ikhsan and M. Hasan, "Analisis Dampak Penggunaan E-Commerce dalam Meningkatkan Omzet Penjualan Usaha Mikro Kecil Menengah di Kota Makassar (Analysis of the Impacts of e-Commerce Usage in Increasing the Sales Income of MSMEs in Makassar City)," *Journal of Economic Education and Entrepreneurship Studies*, vol. 1, no. 1, 2020, doi: 10.26858/je3s.v1i1.18112.
- [5] F. Hidranto, "Bisnis E-Commerce Semakin Gurih (E-Commerce Business is Increasingly Savvy)," *Portal Informasi Indonesia (Indonesian Information Portal)*. [Online]. Available: <https://www.indonesia.go.id/kategori/indonesia-dalam-angka/2534/bisnis-e-commerce-semakin-gurih>
- [6] M. A. Rizaty, "Transaksi E-Commerce Indonesia Diproyeksikan Capai Rp 403 Triliun pada 2021 (Indonesian E-Commerce Transactions are Projected to Reach IDR 403 Trillion in 2021)," *Katadata*. [Online]. Available: <https://databoks.katadata.co.id/datapublish/2021/11/25/transaksi-e-commerce-indonesia-diproyeksikan-capai-rp-403-triliun-pada-2021>
- [7] E. Santoso, "Opportunities and Challenges: E-Commerce in Indonesia from a Legal Perspective," *Jurnal Penelitian Hukum De Jure (Journal of De Jure Legal Research)*, vol. 22, no. 3, p. 395, 2022, doi: 10.30641/dejure.2022.V22.395-410.
- [8] A. L. Kusumatriana, K. Amri, L. Angraini, T. Sutarsih, and V. C. Wulandari, *Statistik e-commerce 2022-2023 (E-Commerce Statistics of 2022-2023)*. Jakarta: Badan Pusat Statistik, 2023. [Online]. Available: <https://www.bps.go.id/id/publication/2023/09/18/f3b02f2b6706e104ea9d5b74/statistik-e-commerce-2022-2023.html>
- [9] E. F. Santika, "ECDB: Proyeksi Pertumbuhan e-Commerce Indonesia Tertinggi Sedunia pada 2024 (ECDB: Indonesia's e-Commerce Growth Projection is Highest in the World in 2024)," *Katadata*. [Online]. Available: <https://databoks.katadata.co.id/datapublish/2024/04/29/ecdb-proyeksi-pertumbuhan-e-commerce-indonesia-tertinggi-sedunia-pada-2024>
- [10] F. Arif, "35 Data Statistik E-commerce Indonesia di Tahun 2024 (35 Indonesian E-commerce Statistics Data in 2024)," *Semnesia*. [Online]. Available: <https://semnesia.com/blog/data-statistik-e-commerce-indonesia/>
- [11] R. Nafi'ah, "Pelanggaran Data dan Pencurian Identitas pada E-Commerce (Data Breach and Identity Theft in E-Commerce)," *Cybersecurity dan Forensik Digital (Cyber Security and Digital Forensics)*, vol. 3, no. 1, pp. 7–13, 2020, doi: 10.14421/csecurity.2020.3.1.1980.
- [12] A. P. Kehista, A. Fauzi, A. Tamara, I. Putri, N. A. Fauziah, S. Klarissa, V. B. Damayanti, "Analisis Keamanan Data Pribadi pada Pengguna E-Commerce: Ancaman, Risiko, Strategi Kemanan (Literature Review) (Security Analysis of Personal Data on E-Commerce Users: Threats, Risks, Security Strategies (Literature Review))," *Jurnal Ilmu Manajemen Terapan (Journal of Applied Management Science)*, vol. 4, no. 5, 2023, doi: 10.31933/jimt.v4i5.1541.
- [13] P. A. Baiq, "Perlindungan Hukum terhadap Data Pribadi dalam Transaksi E-Commerce: Perspektif Hukum Islam dan Hukum Positif (Legal Protection of Personal Data in E-Commerce Transactions: Islamic Law and Positive Law Perspectives)," *Diktum: Jurnal Syariah dan Hukum (Sharia and Law Journal)*, vol. 19, 2021, doi: 10.35905/diktum.v19i2.2463.
- [14] S. Mulyani, S. Suparno, and R. M. Sukmariningsih, "Regulations and Compliance in Electronic Commerce Taxation Policies: Addressing Cybersecurity Challenges in the Digital Economy," *International Journal of Cyber Criminology*, vol. 17, no. 2, pp. 133–146, 2023, [Online]. Available: <https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/194>
- [15] H. Nurhayati and Wolff, "E-commerce in Indonesia: Statistics and Facts," *Statista*. [Online]. Available: <https://www.statista.com/topics/5742/e-commerce-in-indonesia/#editorsPicks>

- [16] N. Wilson, K. Keni, P. Henriette, and P. Tan, "The Role of Perceived Usefulness and Perceived Ease-of-Use Toward Satisfaction and Trust which Influence Computer Consumers' Loyalty in China," *Gadjah Mada International Journal of Business*, vol. 23, no. 3, pp. 262–294, 2021, doi: 10.22146/gamaijb.32106.
- [17] B. Ko, "A Comparative Study of Consumer Trust in Major Digital Trade Agreements," *Journal of International Trade and Commerce*, vol. 17, no. 3, pp. 147–165, 2021, doi: 10.16980/jitc.17.3.202106.147.
- [18] Y. L. Fista, A. Machmud, and S. Suartini, "Perlindungan Hukum Konsumen Dalam Transaksi E-commerce Ditinjau dari Perspektif Undang-Undang Perlindungan Konsumen (Consumer Legal Protection in E-commerce Transactions Viewed from the Perspective of Consumer Protection Law)," *Binamulia Hukum (Binamulia Law)*, vol. 12, no. 1, pp. 177–189, 2023, doi: 10.37893/jbh.v12i1.599.
- [19] R. Suhargon, A. Dermawan, T. Hidayah, and S. Asahan, "Urgensi UU ITE Dalam Menjalankan Peran Aktif Kedudukan Hukum Bisnis di Indonesia (The Urgency of the ITE Law in Carrying Out an Active Role in the Legal Position of Business in Indonesia)," *Journal of Science and Social Research*, vol. 7, no. 1, 2024, [Online]. Available: <https://jurnal.goretanpena.com/index.php/JSSR/search/authors/view?firstName=Rahmat&middleName=&lastName=Suhargon&affiliation=Sekolah Tinggi Ilmu Ekonomi Muhammadiyah Asahan&country=ID>
- [20] M. Anggusti, "Cybercrime Change Consumers' Purchase Intention in Indonesia: A Moderating Role of Corporate Social Responsibility and Business Law," *International Journal of Cyber Criminology*, vol. 16, no. 1, 2022, [Online]. Available: <https://cybercrimejournal.com/manuscript/index.php/cybercrimejournal/article/view/74>
- [21] J. Allan and E. Persson, "Social capital and trust for inclusion in school and society," *Education, Citizenship and Social Justice*, vol. 15, no. 2, 2018, doi: 10.1177/1746197918801001.
- [22] F. Fukuyama, *Trust: Kebijakan Sosial dan Penciptaan Kemakmuran (Trust: Social Policy and Prosperity Creation)*. Yogyakarta: Penerbit Al-Qalam, 2010. [Online]. Available: <https://opac.perpusnas.go.id/DetailOpac.aspx?id=1221823>
- [23] V. D. Hasmi and Z. Roshia, "Pengaruh Experiential Marketing, Trust dan Customer Satisfaction Terhadap Customer Loyalty pada Online Shop Shopee di Kota Padang (The Influence of Experiential Marketing, Trust and Customer Satisfaction on Customer Loyalty in the Shopee Online Shop in Padang City)," *Kumpulan Executive Summary Mahasiswa Program Studi Manajemen Wisuda Ke-74 Tahun 2020 (Collection of Executive Summary of 74th Graduation Management Study Program Students in 2020)*, vol. 17, no. 2, 2020, [Online]. Available: <https://ejurnal.bunghatta.ac.id/index.php/JFEK/article/view/17742>
- [24] N. Dulfar, A. McKernan, and J. Kriewaldt, "Article Undermining teachers' social capital: a question of trust, professionalism, and empowerment," *British Journal of Sociology of Education*, vol. 44, no. 3, pp. 418–434, 2023, doi: 10.1080/01425692.2023.2179018.
- [25] Y. A. Rizki, F. Dharma, Y. Amelia, and T. J. Prasetyo, "Factors Affecting Trust and Interest in Transactions by Indonesian MSME Sellers in E-Commerce," *Journal of Indonesian Economy and Business*, Vol. 38, No. 1, pp. 19–42, 2023, doi: 10.22146/jieb.v38i1.4394.
- [26] N. Wilson, "Trust Vs Satisfaction: Which One is More Important in Mediating the Impact of Website Quality Towards Customer Loyalty in The Indonesian E-Commerce Industry?" *Proceedings of the International Conference on Management, Accounting, and Economy (ICMAE)*. Jakarta: Atlantis Press, 2020. doi: 10.2991/aebmr.k.200915.003.
- [27] M. Soleimani, "Buyers' trust and mistrust in e-commerce platforms: a synthesizing literature review," *Information Systems and e-Business Management*, vol. 20, no. 1, pp. 57–78, 2022, [Online]. Available: <https://link.springer.com/article/10.1007/s10257-021-00545-0>
- [28] V. Jain, B. Malviya, and S. Arya, "An Overview of Electronic Commerce (e-Commerce)," *Journal of Contemporary Issues in Business and Government*, vol. 27, no. 3, pp. 665–670, 2021, doi: 10.47750/cibg.2021.27.03.090.
- [29] M. Mahdikhani and B. Yazdani, "Transformational leadership and service quality in e-commerce businesses: The role of trust and team performance," *International Journal of Law and Management*, vol. 62, no. 1, pp. 23–46, 2020, doi: 10.1108/IJLMA-12-2018-0290.
- [30] A. Maulana, I. Kurniawan, and A. Riyansyah, "The Effect Of E-Commerce Trust, Site Loyalty, And E-Commerce Satisfaction on Purchasing Behavior," *Jurnal Manajemen (Management Journal)*, vol. 27, no. 2, pp. 362–380, 2023, doi: 10.24912/jm.v27i2.1329.
- [31] K. Y. Prasetyo, A. Basith, F. Damayanti, M. W. Utami, R. F. Abdillah, and K. Sofyan, "Pengaruh E-Commerce terhadap Tindak Kejahatan Siber di Era Milenium untuk Generasi Milenial (The Influence of E-Commerce on Cyber Crime in the Millennium Era for the Millennial Generation)," *Journal of Education and Technology*, vol. 1, no. 2, 2021, [Online]. Available: <https://jurnalilmiah.org/journal/index.php/jet/article/view/58>
- [32] Ipricegroup, "The Map of E-commerce in Indonesia," *Iprice Insight*. Accessed: Jul. 09, 2024. [Online]. Available: <https://iprice.co.id/insights/mapofecommerce/en/>
- [33] H. Setiawan, M. Ghufroon, and D. A. Mochtar, "Perlindungan Data Pribadi Konsumen Dalam Transaksi E-Commerce Menurut Peraturan Perundang-Undangan Di Indonesia (Legal Protection of Consumer Personal Data in E-Commerce According to Laws dan Regulations in Indonesia)," *Merdeka Law Journal*, vol. 1, no. 2, 2020, [Online]. Available: <https://jurnal.unmer.ac.id/index.php/mlj/article/view/5496>
- [34] S. Ariyaningsih, A. A. Andrianto, A. S. Kusuma, and R. A. Prastyanti, "Korelasi Kejahatan Siber dengan Percepatan Digitalisasi di Indonesia (Correlation of Cyber Crime with the Acceleration of Digitalization in Indonesia)," *Justitia: Jurnal Ilmu Hukum (Journal of Legal Sciences)*, vol. 1, no. 1, 2023, doi: 10.56457/jjih.v1i1.38.
- [35] R. N. Rohmah, "Upaya Membangun Kesadaran Keamanan Siber pada Konsumen E-commerce di Indonesia (Efforts to Build Cyber Security Awareness among E-commerce Consumers in Indonesia)," *Cendekia Niaga (Commerce Scholar)*, vol. 6, no. 1, pp. 1–11, 2022, doi: 10.52391/jcn.v6i1.629.

- [36] S. Devinda, P. K. Rizqyta, C. Firdiani, T. Da Costa, S. S. Shifa, and Z. P. G. Chelsea, "Analysis of Information Technology Crime and Criminal Law Enforcement Policy Efforts in the Era of Globalization," *Problematika Hukum Journal (Legal Problem Journal)*, vol. 9, no. 2, pp. 74–88, 2023, [Online]. Available: <http://e-journal.president.ac.id/Presunivojs/index.php/problematika-hukum/article/view/5206/0>
- [37] T. Fadziso, U. R. Thaduri, S. Dekkati, V. K. R. Ballamudi, and H. Desamsetti, "Evolution of the Cyber Security Threat: An Overview of the Scale of Cyber Threat," *Computer Science and Engineering*, vol. 3, no. 1, pp. 1–12, 2023, doi: 10.6084/m9.figshare.24189921.v1.
- [38] D. Puspitasari and T. Sutabri, "Analisis kejahatan phising pada sektor e-commerce di marketplace Shopee (Analysis of phishing crimes in the e-commerce sector on the Shopee marketplace)," *Jurnal Digital Teknologi Informasi (Digital Journal of Information Technology)*, vol. 6, no. 2, 2023, doi: 10.32502/digital.v6i2.5653.
- [39] M. Yusuf, M. Agustantia, and S. Zulaiha, "Tindak Pidana Kejahatan Pemalsuan data (Data Forgery) dalam Bentuk Kejahatan Siber (Cyber Crime) (Crime: Data Forgery in the Form of Cyber Crime)," *Jurnal Pendidikan dan Konseling (Journal of Education and Counseling)*, vol. 4, no. 6, 2022, doi: 10.31004/jpdk.v4i6.9365.
- [40] C. B. E. Praja, B. A. Riswandi, and K. Dimiyati, "Urgensi Mediasi sebagai Alternatif Penyelesaian Sengketa Hak Cipta (The Urgency of Mediation as an Alternative to Resolving Copyright Disputes)," *Kertha Patrika*, vol. 43, no. 3, pp. 275–295, 2021, doi: 10.24843/KP.2021.v43.i03.p04.
- [41] K. Dimiyati and K. Wardiono, *Metode Penelitian Hukum (Legal Research Method)*. Surakarta: Universitas Muhammadiyah Surakarta, 2004.
- [42] A. H. Al Faraby, "Perkembangan Teknologi Informasi Dan Transaksi Elektronika (ITE) Di Indonesia (Development of Information Technology and Electronic Transactions in Indonesia)," *Meraja Journal*, vol. 7, no. 1, 2024, doi: 10.33080/mrj.v7i1.331.
- [43] S. Yuniarti, A. M. Ramli, S. D. Rosadi, and D. Budhijanto, "The New Chapter of Indonesia's Data Protection on Digital Economy Perspective," *Journal of Southwest Jiaotong University*, vol. 58, no. 3, 2023, doi: 10.35741/issn.0258-2724.58.3.9.
- [44] P. A. Dewi, "Menilik Perubahan UU ITE Nomor 1 Tahun 2024 yang Baru Saja Disahkan (Looking at the Amendments to the ITE Law Number 1 of 2024 which have just been passed)," *Mekari Sign*. [Online]. Available: <https://mekarisign.com/id/blog/perubahan-uu-ite-2024/>
- [45] A. Amahoru, A. Sadikin, F. Aziz, E. Fkun, and I. Ludin, "Social Media and Commerce: A Review Of The Indonesian Government's Efforts To Regulate Online Transactions," *Jurnal Scientia (Science Journal)*, vol. 12, no. 4, 2023, doi: 10.58471/scientia.v12i04.2095.