YURISDIKSI
Jurnal Wacana Hukum dan Sains
Universitas Merdeka Surabaya

E-Commerce as a Source of Cyber Crime

Reda Manthovani
Faculty of Law, Pancasila University, Jakarta, Indonesia
E-mail:redamanthovani@univpancasila.ac.id

ABSTRACT

E-commerce is a type of electronic business mechanism that focuses on individual-based business transactions using the internet (digital network-based technology) as a medium for exchanging goods or services between two institutions (B to B) and institutions to direct consumers (B to C). The aim of this research is the effectiveness and efficiency of electronic transaction law in Indonesia. The research method used is normative juridical with a statutory approach using primary and secondary legal sources, the results show that crimes committed through online networks are either online auction fraud, check fraud, credit card fraud, trust fraud, identity fraud, pornography. children, and others cannot be dealt with firmly so that these actions can damage the business climate. So it could be said that our legal system has not been effective in preventing cyber crime.

.

Keywords: E-Commerce, Cyber Crime, Criminal Law, Indonesian Criminal Code, Extraordinary Crimes.

1. INTRODUCTION

The ease of transactions makes the state of the business world like a "double-edged sword". On the one hand, it makes it easier for people to meet the needs of the community. On the other hand, many crimes occur in cyberspace as an excess of information technology developments that are exploited by irresponsible parties. We can easily find digital platform providers in bridging electronic transactions - Online buying and selling sites such as Lazada, Zalora, Bukalapak, blibli.com, Tokopedia, etc. are sites that sell various types of goods for people's daily needs.

Based on Ifrani's research, M. Yasir Said, the regulations on cybercrime prevention issued by the OJK have not been effective in anticipating crimes in Fin-Tech P2P Lending because there is no preventive protocol. The existence of the legal umbrella becomes an instrument in providing legal certainty for the parties involved in it, It must be realized that crime occurs not only in the real world but also in virtual world transactions, for this, we need a legal substance in the form of written rules driven by a phenomenon in cybercrime, for this reason, the law must be responsive to the dynamics of the business world so that it can protect the interests of the people. (Ifrani & Said, 2020)

Meanwhile, in the research of Made Wisnu Adi Saputra, I Wayan Gde Wiryawan, Kt. Sukawati Lanang P. Perbawa stated that the causative factor of cybercrime is unlawful acts for personal or group interests which are carried out through threats to victims. Negligence and creating conditions that support the occurrence of crime (opportunity), so we need a rule of law that can anticipate every cybercrime because not all criminal acts in cyber can be subject to sanctions in the Criminal Code and the ITE Law so that a legal reform is needed by sociological

aspects which developed in the era of globalization where jurisdiction and also forms of cybercrime activities have become cross-border transactions. (S. et al., 2021)

Previous research conducted by Hendy Sumadi (2016) criminal acts of cybercrime often occur because of regulatory support and the structure of law enforcement and the culture of a society are still weak, therefore it is very natural that cybercrimes continue to increase over time. Given the rampant cases of cybercrime or cybercrime, it is necessary to have serious handling by law enforcement officials. Because of enforce that the legal structure factor plays a very important role in preventing cybercrime whether pre-emptive, preventive, or repressive. (Januri et al., 2022)

The novelty of this study is that the authors examine the effectiveness of enforcing regulations related to cybercrime in Indonesia. Therefore, crimes on the internet in conducting electronic commerce do not become more widespread and continue to occur. Regulations related to electronic trading crimes must be realized and realized immediately so that people who frequently carry out electronic trading transactions can be protected and have a legal basis that can be used as a reference. In Indonesia, regulations related to electronic information technology have been regulated in Law No. 11 of 2008 and Law No. 19 of 2016 concerning changes to Law No. 11 of 2008 concerning Information and Electronic Transactions.

The development of the internet has led to the formation of a new world which is commonly called cyberspace. In this virtual world, every individual has the right and ability to interact with other individuals without any restrictions that can prevent them. So perfect globalization has occurred in cyberspace that connects all digital communities. Of all aspects of human life affected by the presence of the Internet, the business sector is the sector most affected by developments in information technology and telecommunications and is the fastest growing. Through e-commerce, for the first time, all people on earth have the same opportunities and opportunities to be able to compete and succeed in doing business in cyberspace.

E-commerce is a type of electronic business mechanism that focuses on individual-based business transactions using the internet (digital network-based technology) as a medium for exchanging goods or services between two institutions (business to business) and direct consumers (business to business). consumers), bypassing the limitations of space and time that have been dominant. In this era of increasingly fierce competition in the current era of globalization, the real competition lies in how a company can utilize e-commerce to improve performance and existence in its core business. With e-commerce applications, relations between companies and other external entities (suppliers, distributors, partners, consumers) can be carried out more quickly, intensively, and inexpensively compared to the application of conventional management principles (door-to-door, one-to-one). So, e-commerce is not just a mechanism for selling goods or services through Internet media, but also a business transformation that changes the perspective of

companies in carrying out their business activities. Building and implementing an e-commerce system is not an instant process, but a transformation of business strategies and systems that continues to evolve in line with company and technology developments. The existence of crime on the internet, especially in conducting electronic commerce, can cause anxiety in society. (Maskun et al., 2020)

Because the occurrence of internet crimes cannot be seen directly by people who carry out electronic transactions, these crimes can only be accepted indirectly and require valid evidence to be disclosed. Therefore, in conducting electronic transactions, good trust is needed between parties who want to buy goods or services from these electronic transactions. However, as someone who purchases goods through an online store, you cannot know or guess whether the seller can be trusted or not. So as a buyer, you have to be wiser and more vigilant when making transactions in e-commerce.

Crimes committed by perpetrators in digital-based transactions can be subject to criminal responsibility if they fulfill the elements that are alleged to be based on their mistakes. Barda Nawawi Arief in Arif Bayuaji, Rehnalemken Ginting said that the value of justice is something that must be considered in determining whether the perpetrator is guilty or not based on the principles of legality and legal certainty - because the purpose of punishment is law enforcement, conflict resolution and community protection as well as restoring balance in community life. (Bayuaji & Ginting, 2020).Based on the background above, the authors aim to determine and analyze the effectiveness and efficiency of electronic transaction law in Indonesia and its prevention.

2. RESEARCH METHODS

The research method used in this writing is normative juridical legal research or research that is doctrinal (Wijaya, 2022), namely legal research conducted by examining library materials consisting of primary legal materials, secondary legal materials, and tertiary legal materials with collection techniques in the form of one in the library. types of quantitative and descriptive approaches to analysis through interpretation from legal sources such as Law Number 19 of 2016 concerning ITE, Criminal Code, and Criminal Procedure Code and secondary legal materials in the form of books, research results related to electronic transactions, and cybercrime. In the next stage, conclusions are drawn. The statutory approach (statute approach) is carried out by reviewing all laws and regulations related to the legal issues under study, (Marzuki, 2019) especially Law No. 11 of 2008 and Law No. 19 of 2016 concerning changes to Law No. 11 of 2008 concerning Information and Electronic Transactions. In addition, research was also conducted by looking at how deep the empirical practice of legalization is in the Ministry of Law and Human Rights and the Ministry of Foreign Affairs. (Dewi & Fahrial, 2021)

3. RESULTS AND DISCUSSION

The increasingly extreme acceleration of technology is the material cause of continuous changes in all interactions and activities of the information society. The Internet is a symbol of the forerunner of the global community. The internet makes the world round as if it were only as wide as a moringa-leaf. The information age is characterized by very high information accessibility. In the current era, information is the main commodity that is traded, so various networks and information companies have sprung up that will trade various network facilities and various information databases about various things that can be accessed by users and customers. There is a legal vacuum, especially in dealing with criminal acts of cyber-terrorism, as well as cyber transactions that involve cross jurisdictions. (Januri et al., 2022)

A term that refers to criminal activity with a computer or computer network as a tool, target, or place of crime. These include online auction fraud, check fraud, credit card fraud, trust fraud, identity fraud, child pornography, etc. Cybercrime as a crime in this case is the illegal use of computers. Cybercrime is very difficult to identify because almost every day there are crimes with new motives. Cybercrime is also usually carried out only as a support for criminal acts in the real world, for example selling illegal drugs as a promotional medium using cyber facilities such as websites. (Maskun et al., 2020)

Classification of Cyber Crime is as follows: (Smariti, 2017)

1. Cyber piracy is the use of computer technology to reprint software or information and distribute that information or software through computer networks.
2. Cybertrespass is the use of computer technology to enhance access to an organization's or individual's computer systems and password-protected websites.
3. Cyber vandalism is the use of computer technology to create programs that interfere with the transmission of electronic information and destroy data on the computer.
4. Cybercrime is a pure crime: Where a person commits a crime intentionally, for example, theft, or anarchic acts, against an information system or computer system.
5. Cybercrime as a gray crime: Where this crime is not clear whether it is a crime or not because it commits a burglary but does not damage, steal, or commit anarchic actions against information systems or computer systems.
6. Cybercrimes that attack individuals. Crimes committed against other people with the motive of revenge or fad aiming to damage one's good name, for example: pornography, cyberstalking, and others.
7. Cybercrimes that attack copyright (proprietary rights): Crimes committed against someone's creation with the motive of copying, marketing, or modifying it for personal/public interest or material/non-material purposes.

8. Cybercrimes against the government: Crimes committed with government objects with the motive of committing terror, piracy, or undermining security.
9. Unauthorized Access to Computer Systems and Services Crime committed by entering/infiltrating a computer network system illegally, without permission. Usually, the criminals (hackers) do this to sabotage or steal important information.
10. Illegal Content. Entering data or information on the internet about something untrue, or unethical, and can be considered as breaking the law or disturbing public order is a crime. An example is the loading of hoaxes or slander news that will damage the dignity of other parties.
11. Data Falsification It is a crime to falsify data on important documents that are stored as unscripted documents via the Internet.
12. Cyber Espionage is a crime that utilizes the internet network to carry out espionage activities against other parties, by entering the computer network system of the intended party.
13. Cyber Sabotage and Extortion This crime is carried out by disrupting, destroying, or destroying data, computer programs, or computer network systems connected to the internet.
14. Intellectual Property Violation This crime is directed against Intellectual Property Rights owned by other parties on the Internet. For example, imitating the display on a web page of a site belonging to someone else illegally, broadcasting information on the internet that turns out to be someone else's trade secret, and so on.
15. Violation of Privacy This crime is usually directed against a person's personal information stored in a personal data form that is computerized, which if known by another person can harm the victim materially or immaterially, such as credit card numbers, ATM PINs, and hidden defects. or disease etc.
16. Cracking is a crime using computer technology that is carried out to undermine the security system of a computer system and usually commits theft, and anarchic acts once it gains access. Usually, we often misinterpret hackers and crackers where hackers themselves are synonymous with negative actions, even though hackers are people who like to program and believe that information is something very valuable and some can be published and confidential.
17. Carding Is a crime that uses computer technology to carry out transactions using other people's credit cards so that it can harm that person both materially and immaterially.
18. Cybercrime attacks individuals (Against Person) with this type of activity, the target of the attack is aimed at individuals or individuals who have certain characteristics or criteria

according to the purpose of the attack. Examples: pornography, Cyberstalking, Cyber-Tress pass.

19. Cybercrime attacks Cyber property that is carried out to interfere with or attack the property rights of others. Some examples of these crimes include unauthorized computer access through cyberspace, illegal possession of electronic information/information theft, carding, cybersquatting, piracy, data falsification, and others.
20. Cybercrime Against the Government (Again Government) Cybercrime Against the Government is committed with the specific aim of attacking the government. Such activity is for example Cyber Terrorism as an act that threatens the government, including breaking into official sites, government sites, or the military.

Electronic commerce is divided into 2 types: (Utama et al., 2021) first, Business-to-customer (B2C) Trading via electronic networks relating to transactions between companies and end users of products. Business to Customer (B2C) Strategy through Electronic Networks: Digital Products, certain products and services can be delivered to consumers directly via the Internet. Examples of digital products such as songs, films, and software. Products and services can be consumed immediately after download. Physical Products, namely certain products and services that cannot be directly consumed via the internet, but must be delivered to consumers. Sales orders and payments can be received via the internet after which they are sent to the buyer. Virtual vs. Hybrid Sales, Virtual Sellers are sales made by companies that do not have physical stores. Hybrid selling is selling by a company that has a physical store and also has a Web page to make the sale. Second, business to business (B2B) Trading via electronic networks relating to transactions between companies that do not involve end users. Involve a few people The people involved are highly trained in the use of information systems and familiar with business processes. The people involved are highly trained in the use of information systems and familiar with business processes.

In recent decades, there has been a lot of forgery of business-related letters and documents. The act of counterfeiting the letter has damaged the business climate in Indonesia. The Criminal Code does have a special chapter, namely Chapter XII which criminalizes the act of forging letters, but these provisions are still very general. Currently, fake letters and documents can be in the form of electronic documents sent or stored in electronic archives of government agencies institutions, companies, or individuals. Indonesia should have special criminal provisions related to the forgery of letters or documents by distinguishing the types of fake letters or documents that are *lex specialists* outside the Criminal Code. Another crime that falls into the category of cybercrime in business crime is Cyber Fraud, which is a crime committed by fraud via the internet, one of which is by committing a crime first, namely stealing other people's credit card numbers by hacking or

breaking into sites on inside. Internet. Cases related to cybercrime in business crimes rarely reach court, this is because there is still debate about regulations related to these crimes. (Smariti, 2017)

Specifically regarding Law Number 11 of 2008 concerning the Internet and Electronic Transactions, which until now, although it was passed on April 21, 2008, has not yet issued a Government Regulation as an explanation and complement to the implementation of the Law. In addition, many of these incidents were not reported by the public to the police so the cybercrimes that occurred were only like the wind and suffered by the victims.

Fundamental problems in e-commerce include: (Maskun et al., 2020) see (Mawarni Fatma, 2022) see (Kamran & Maskun, 2021) First, in cyberspace, virtualization is the main concept that underlies the form and structure of a company. In virtual companies, physical assets are omitted whenever possible. Customers around the world do not transact with institutions through physical transactions involving buildings, people, and other tangible objects, but only transact via electronic sites. With only $35 a year (to order a domain address), a company can be established and offer its services or products to various countries, without having to be burdened with various administrative matters. The application of cyber law articles that complicate the establishment of a company will reduce the intention of new players to establish virtual companies, which means it will sluggish the industry in cyberspace.

Second, the applied business model tends to eliminate all forms of mediation. This is possible because, through the internet, individuals can easily make transactions with other individuals (or between companies) quickly. This phenomenon is a simple form of a free market where both parties who transact consciously exchange services or products with risks that are realized together. The application of cyber law articles that reduce the maximum profit that has been obtained by both parties in the transaction will result in a reduction in the frequency and volume of business on the internet.

Third, the boundaries between producers and consumers are blurred. The term that is developing is "prosumer" because the business model that exists in cyberspace allows someone to be both a producer and a consumer (such as membership in American Online, E-Groups, Geocities, etc.). The application of cyber law articles based on conventional economic systems (such as supply and demand law) will hinder the growth of various business models that have been the main attraction and advantage of cyberspace.

Fourth, the fact that virtual companies cannot run all their businesses, but must cooperate with various other virtual companies (such as merchants, content providers, technology vendors, etc.). This resulted in inter-company dependence on the Internet being very high. Application of cyber law market articles that make it easier for a company to go out of business will result in the downfall of the business of several other companies that depend on it.

Fifth, the main resource that is needed in the process of creating products and services is knowledge. Because knowledge is attached to human resources (elements of creativity, intellect, emotionality, etc.), knows no national boundaries, and is easily exchanged and communicated, all forms of protection are irrelevant and effective. The application of cyber law articles that limit and restrain individuals from using or exchanging their knowledge will have an impact on reducing the types of products or services that may be created.

From the five main principles above, it can be seen that the formulation and development of cyber law must be carried out with extra care. Cyberspace is the only business arena today that has implemented the concept of the free market and globalization of information almost perfectly. The existence of cyber law is needed not only to protect consumer rights or enforce fair business rules but also to prevent "chaos" in cyberspace. Because after all the chaos in the virtual world will have a direct impact on human life in the real world.

Juridical Review Regulations in Indonesia regarding Internet crimes in electronic trading transactions. Online business which is increasingly favored by internet users both as consumers and owners of online business sites will give rise to a lot of fraud. With the increasing number of frauds that will or have occurred, legal protection is needed for both consumers and owners of honest online buying and selling sites. Online business in Indonesia has not been specifically regulated by law. There are no procedures, transaction terms, establishment requirements, taxes to be paid, or other matters governing this activity. However, to minimize crime in online business, the government has made the Electronic Information and Transaction Law (UU ITE) Number 11 of 2008. In the ITE Law there are two important things, namely: (Maskun et al., 2020)

1. Recognition of electronic transactions and electronic documents within the legal framework of engagement and evidentiary law, so that legal certainty for online business can be guaranteed.
2. Classification of actions that include violations of the law related to misuse of Information Technology (IT), so that strict sanctions will be given to those who violate the ITE Law.

However, the main factors causing consumer exploitation are consumers' lack of understanding of their rights, lack of information obtained, and low online consumer knowledge of online business law. Consumer protection is regulated in Law No. 8 of 1999 concerning Consumer Protection (UU PK).

This law provides a strong legal basis for efforts to empower consumers. ITE Law Number 11 of 2008 protects consumers and obligations for business actors, namely in CHAPTER III Article 9 "Business actors offering products through electronic systems are required to provide complete and correct information relating to contract requirements, producers and products offered". The ITE Law also regulates sanctions for parties who misuse the features of online

transactions for criminal acts. Article 28 Paragraph 1 of the ITE Law states "Every person intentionally and without right spreads false and misleading news that results in consumer losses in electronic transactions". The penalty is imprisonment for a maximum of 6 years and/or a fine of up to IDR 1,000,000,000.00 (Article 45 Paragraph (2) of the ITE Law). (Maskun et al., 2020)

Furthermore, Article 36 of the ITE Law stipulates that anyone who deliberately and without rights or unlawfully commits an act as referred to in Articles 27 to 34 which causes harm to other people, is punishable by imprisonment for a maximum of 12 years and/or a fine for a maximum Rp. 12,000,000,000.00 (two billion rupiah). The losses referred to here are large or material, not immaterial. The legal basis for electronic transactions is as follows: a. Law of the Republic of Indonesia Number 8 of 1999 concerning Consumer Protection; b. Law of the Republic of Indonesia Number 11 of 2008 concerning Information and Electronic Transactions; c. Government Regulation of the Republic of Indonesia Number 82 of 2012 concerning the Implementation of Electronic Systems and Transactions.

4. CONCLUSION

In the ITE Law, some special chapters and articles give rise to new rules in the field of electronic transactions that did not exist before, namely Chapter V Article 17 to Article 22. Although the rules regarding online business are not specifically regulated in law, the provisions regarding online business are not specifically regulated in law. The existence of this article is very important to provide protection and legal certainty for online business users. Moreover, currently, the government will process the issuance of Government Regulations in the field of Electronic Transactions. In addition to clarity regarding the status of electronic transactions regulated in UU ITE No. 11 years old. 2008 with several special articles, there must be further legal protection for consumers because if studied and understood carefully, it is likely that consumers will be the most disadvantaged in this online business. Consumers must be careful in choosing an online store site and a business will run well and be big because there are many consumers. As explained in UU ITE no. 11 of 2008 Article 38 "Everyone can file a lawsuit against the party that operates the electronic system and/or uses information technology that causes harm."

Whereas in the development of electronic trading transactions, there must be regulations or provisions as a legal umbrella that can become a reference for the community. In conducting electronic trading transactions, there is often a lot of unrest in the community, especially public trust in producers (sellers) of goods via the Internet. Sometimes what consumers buy does not match what they see on the internet (online shop), and can be said to be an act of fraud. This is an example of a crime that occurs on the internet in electronic commerce transactions. Therefore, the role of the government is urgently needed here in regulating and making regulations or laws and

regulations that can make producers more worry and afraid of committing crimes in electronic transactions (deterrence effect). So it can be said that our legal system has not provided effectiveness in preventing cybercrimes.

REFERENCE

Bayuaji, A., & Ginting, R. (2020). Pertanggungjawaban Pidana Kejahatan Cyberbullying (Studi Putusan Nomor 97/Pid.Sus/2019/PN.SMN). *Recidive : Jurnal Hukum Pidana Dan Penanggulangan Kejahatan*, *9*(2), 98. https://doi.org/10.20961/recidive.v9i2.47397

Dewi, N. M. T., & Fahrial, R. L. (2021). Suatu Kajian Yuridis Terhadap Penggunaan Alat Bukti Elektronik dalam Kejahatan Cyber dalam Sistem Penegakan Hukum. *Jurnal Hukum Saraswati (JHS)*, *3*(2), 11–25. https://doi.org/10.36733/jhshs.v3i2.2949

Ifrani, I., & Said, M. Y. (2020). Kebijakan Kriminal Non-Penal OJK dalam Mengatasi Kejahatan Cyber Melalui Sistem Peer to Peer Lending. *Al-Adl : Jurnal Hukum*, *12*(1), 61. https://doi.org/10.31602/al-adl.v12i1.2607

Januri, Melati, D. P., & Muhadi. (2022). Upaya Kepolisian dalam Penanggulangan Kejahatan Cyber Terorganisir. *Audi Et AP : Jurnal Penelitian Hukum*, *1*(2), 94–100. https://doi.org/10.24967/jaeap.v1i02.1692

Kamran, M., & Maskun, M. (2021). Penipuan Dalam Jual Beli Online: Perspektif Hukum Telematika. *Balobe Law Journal*, *1*(1), 41. https://doi.org/10.47268/balobe.v1i1.501

Marzuki, P. M. (2019). *Penelitian hukum* (14th ed.). Jakarta.

Maskun, Achmad, Naswar, Assidiq, H., Safira, A., & Lubis, S. N. (2020). Korelasi Kejahatan Siber dan Kejahatan Agresi Dalam Perkembangan Hukum Internasional. In *Korelasi Kejahatan Siber dan Kejahatan Agresi Dalam Perkembangan Hukum Internasional*. CV. Nas Media Pustaka.

Mawarni Fatma, S. (2022). Jual Beli Online: Pada Penipuan Perspektif Hukum Telematika. *Gajah Putih Journal of Economics Review (GPJER)*, *4*(2), 1–9.

S., M. W. A., Wiryawan, I. W. G., & P., K. S. L. P. (2021). Faktor Penyebab Terjadinya Kejahatan Cyber Crime yang Dilakukan oleh Orang Asing di Bali Ditinjau dari Perspektif Kriminologi. *Jurnal Yusthima*, *1*(1), 58–70. https://doi.org/10.36733/yusthima.v1i01.2984

Smariti. (2017). Classification of cyber crime. *International Journal of Applied Research*, *3*(7), 616–625.

Utama, K. M. R. A., Umar, R., & Yudhana, A. (2021). Implementasi Metode Business To Costumer Pada Sistem Informasi Toko Kgs Rizky Motor. *RADIAL : Jurnal Peradaban Sains, Rekayasa Dan Teknologi*, *9*(2), 173–184. https://doi.org/10.37971/radial.v9i2.234

Wijaya, T. H. D. (2022). Penerapan Sanksi Sosial Sebagai Alternatif Pemidanaan Terhadap Pelaku Tindak Pidana Kejahatan Siber (Cyber Crime). *Al-Qisth Law Review*, *5*(2), 371. https://doi.org/10.24853/al-qisth.5.2.371-404