Volume 6 Number 1 (2024)
January-June 2024
Page: 163-180

E-ISSN: 2686-4819
P-ISSN: 2686-1607
DOI: 10.37680/almanhaj.v6i1.4910

AL-MANHAJ
Jurnal Hukum dan Pranata Sosial Islam

Analysis of Cybercrime Potential in E-Commerce Buying and Selling Transactions

Evi Elisanti[1], Ariy Khaerudin[2], Amir Junaidi[3], Hanuring Ayu Ardhani Putri[4], M. Muhtarom [5]

[1] Universitas Islam Batik Surakarta, Indonesia; evielisanti@gmail.com
[2] Universitas Islam Batik Surakarta, Indonesia; ari. khaerudin@gmail.com
[3] Universitas Islam Batik Surakarta, Indonesia; amirjunaidi@uniba.ac.id
[4] Universitas Islam Batik Surakarta, Indonesia; Haruringayu@gmail.com
[5] Universitas Islam Batik Surakarta, Indonesia; mmmuhtarom@gmail.com

Received: 14/02/2024 Revised: 20/04/2024 Accepted: 16/05/2024

Abstract

The research aims to analyze the potential for cybercrime in e-commerce buying and selling transactions. The research method used is normative juridical. The type of primary data is interviews and discussions related to e-commerce, and secondary data is library literature. Data collection techniques used literature studies, interviews, observation, and documentation. The data analysis technique is descriptive qualitative which is used in the form of an interactive analysis model. The research results show that the potential for cybercrime in e-commerce buying and selling transactions has increased significantly, including minimal knowledge, waste of money, being tempted by fake gifts, high levels of unemployment and poverty, and less strict government security policies. Forms of cybercrime in e-commerce include hacking, identity theft, data breach, phishing, spamming, pharming, pretexting, qui pro quo, and contacting the victim directly. Specific solutions are needed to overcome the cybercrime problem of e-commerce buying and selling, namely Backup, Use of SSL Certificates, Firewall, E-Commerce Security Plugin, Multilayer security, User and Staff Education. The conclusion of this research is that the potential for cybercrime in e-commerce buying and selling transactions has increased significantly so it is very necessary to prevent specific solutions in resolving cybercrime problems in e-commerce buying and selling transactions.

Keywords Analysis; Cybercrime; Transactions; E-commerce

Corresponding Author
Evi Elisanti
Universitas Islam Batik Surakarta, Indonesia; evielisantil@gmail.com

1. INTRODUCTION

Cybercrime, often known as computer crime, is the use of computers for criminal purposes, such as fraud, trafficking in child pornography and intellectual property, identity theft, and privacy violations. As computers become increasingly important in commerce, entertainment, and government, cybercrime, especially via the internet, is increasing. increased significantly (Harahap et al., 2022). The internet has become a breeding ground for various criminal activities and techniques (Wibowo, 2016) Different types of cybercrime can be classified into three groups. First, the Internet facilitates the

establishment and maintenance of cybercrime markets. The internet also provides a venue for cyber-fraud activities. Third, the Internet has become a breeding ground for cybercriminal communities (Fianyi, 2016)

Based on facts on the ground, the cases above related to data leaks are evidence of weak Internet cyber security in Indonesia. According to National CyberSecurity Index (NCSI) data, Indonesia is ranked 83rd out of 160 countries in cyber security. Indonesia scored 38.96 points on the Cyber Security Index and 46.84 points on the Development or Digital Development Level. Indonesia is ranked 6th out of 10 countries in the Southeast Asia Cyber Security Index. Neighboring country Malaysia is in first place with 79.22 points. Another nearby country, Singapore, ranked second in cyber security with a score of 71.43.

The activity of using the Internet for business transactions is called Electronic Commerce (E-Commerce). E-commerce which involves the use of the Internet and the World Wide Web to sell products and services to consumers, occurs between business organizations and consumers. E-commerce technology is a business method that makes electronic products around online business transactions, which provides the opportunity to create person-to-person relationships with customers regardless of time and place (Ummiyati & Anggono, 2020)

The scope of e-commerce according to the World Trade Organization (WTO) includes the fields of production, distribution, marketing, sales and delivery of goods or services via electronic means, while the OECD (Organization for Economic Cooperation and Development) explains that e-commerce is e-commerce. -commerce is a transaction based on the processing and transmission of electronic data. Apart from these two international institutions. The Alliance for Global Business, a leading trade association, defines e-commerce as all value transactions involving the transfer of information, products, services, or payments via electronic networks as a medium. Meanwhile, e-commerce from ECEG Australia (Electronic Commerce Expert Group) is "Electronic commerce is a broad concept that includes every commercial transaction carried out via electronic means and includes means such as fax, telex, EDI, Internet and telephone" (Lubis, 2022)

E-commerce is the result of advances in information and technology that change traditional business practices from face-to-face interactions between sellers, business people, and buyers, to virtual interactions between business people and consumers in cyberspace. This development can be seen from the rise of online shops that use the internet as a medium for buying and selling goods or services with business or individual customers, as well as the use of digital technology in bartering methods for goods, services, information, etc. (Putri et al., 2023)

The Internet is a worldwide computer network. Economically, it is recognized that using the Internet is very urgent/important to speed up business transactions, but using the internet also requires

extra caution. This is transnationally synonymous with the word "internet business". E-commerce is the practice of conducting business through the use of computer networks, such as the internet, involving consumers, producers, service providers, and intermediaries (Santoso, 2022)

E-commerce is the practice of distributing, buying, selling, and marketing goods and services via the internet. Electronic commerce is very dependent on the existence of the Internet as the main medium for carrying out transactions therein (Azizah et al., 2021) The ease and speed that E-commerce provides in online transactions makes many people prefer to transact online compared to regular or offline transactions (Yadi et al., 2022)The number of internet users in Indonesia continues to increase from year to year, which has a very pronounced impact on the progress of e-commerce in Indonesia (Hanim, 2011)

Based on data on the development of E-Commerce transactions in Indonesia in 2018-2022. Indonesian people enjoy business development in the form of e-commerce, online shopping using various applications, buying and selling shopping sites operating in Indonesia. The development of e-commerce in Indonesia is growing rapidly. According to the 2021 Bank Indonesia Annual Report, E-commerce transactions in 2018 amounted to IDR 106 trillion, E-commerce transactions in 2019 amounted to IDR 206 trillion, and E-commerce transactions in 2020 amounted to IDR 266 trillion. E-commerce transactions for digital banking payments in 2021 will amount to IDR 403 trillion. E-commerce transactions in Indonesia will continue to increase in 2022 with a value reaching IDR 530 trillion or growing 31.4% yoy.

As e-commerce transactions increase, more cybercrime is susceptible to emerging. The factors causing cybercrime in e-commerce transactions are unlawful acts for personal or group interests carried out through threats to victims (Sumadinata, 2023)Negligence and creating conditions that support the occurrence of crime (opportunity), then legal certainty is needed that can anticipate every cybercrime because not all criminal acts in cyberspace can be subject to sanctions in the Criminal Code and the ITE Law so that they can obtain legal sanctions (Harahap et al., 2022). In fact, in the field, many problems befall consumers when making transactions in e-commerce because it often happens that the goods/products ordered are different from the actual goods in terms of size, color, type, and quality of the goods. goods, from the conditions experienced by consumers based on consumer law (Rahayu et al., 2021)Law Number 8 of 1999 concerning Consumer Protection states that anyone can file a civil suit with the District Court, and Law Number 11 of 2008 as amended by Law Number 19 of 2016 concerning ITE (Haryani Putri & Endang Hadrian, 2022)

Previous research conducted by Rahayu et al., (2021) stated that cybercrime is very detrimental to users, such as losing a lot of time, financial loss, or data loss. This was responded to by respondents with a score of 86.2%. User trust in e-commerce due to this crime has decreased. Respondents' responses with a score of 73.8% indicate that e-commerce users do not trust e-commerce. Another solution taken

by e-commerce is to increase legal protection for e-commerce users. Users need this protection; a score of 90.9% indicates a response that users need clearer and firmer legal protection to follow up on criminal acts in transactions on e-commerce applications to feel safe in the transaction process.

According to Fadila, a 2021 research study stated that the lack of legal awareness of the community itself is one of the strong factors in the occurrence of cybercrime in e-commerce buying and selling. This factor can be seen from fraud victims who do not understand cybercrime itself, and victims who do not want to report the crime to the authorities. so that the victim's too much trust in what the perpetrator offers and their lack of caution results in the victim being easily victimized or made a victim by the perpetrator which indirectly becomes a "supporting factor" for the perpetrator who has the opportunity to commit cybercrime (Rohmat et al., 2024).

Research studies according to Sumadi (2016) state that cybercrime often occurs because regulatory support and the structure of law enforcement as well as the culture of a society are still weak, therefore it is very natural that cybercrime continues to increase from time to time. Considering the rise in cases of cybercrime, it is necessary to handle it seriously by law enforcement officials. Therefore, law plays a very important role in preventing cybercrime, whether pre-emptive, preventive, or repressive. Law enforcement, conflict. resolution and protection of society and restoration of balance in community life.

The research aims to analyze the potential for cybercrime in E-commerce platform buying and selling transactions. A deeper analysis of the factors that cause cybercrime in e-commerce and identification of more specific solutions to overcome this problem. The relevance of the research topic on potential cybercrime in e-commerce buying and selling transactions is in accordance with current needs. The phenomena of cybercrime problems include minimal knowledge, waste of blood, being tempted by fake gifts, high levels of unemployment and poverty and less firm government security policies. The importance of analyzing potential cybercrime such as hacking, identity theft, data breach, phishing, spamming, pharming, Pretexting, Qui pro quo in the context of cybercrime as well as providing specific solutions to various problems related to potential cybercrime in electronic buying and selling transactions. Based on the above background, the researchers conducted research with the title "Analysis of Cyber Crime Potential in E-Commerce Buying and Selling Transactions"

2. METHOD

This research method uses normative juridical (Sonata, 2015)The type of primary data is interviews and discussions related to e-commerce, and secondary data is library literature. Data collection techniques used literature studies, interviews, observation, and documentation. This normative juridical research analyzes the supremacy of law, so the objects studied are regulatory documents and library literature. The object of this research is a regulation in Law Number 8 of 1999 concerning

Consumer Protection stating that anyone can file a civil suit with the District Court, and Law Number 11 of 2008 as amended by Law Number 19 of 2016 concerning ITE and Bibliographic literature includes books, journal articles related to the potential for cybercrime in e-commerce buying and selling transactions. In carrying out this research, the author used several research approaches in the field of science so that the research focused on solving the following problems. specified scope. The approach in this research consists of a statutory approach and a conceptual approach. The legal approach according to the law is carried out by examining statutory regulations. The legal approach in the law is used to examine provisions or regulations that are relevant to cybercrime crimes. Regarding the conceptual approach, it is carried out based on legal principles obtained from the views of legal experts or other legal doctrines without deviating from existing regulations. This approach is necessary because there are no regulations that regulate it. The application of a conceptual approach is to look for definitions of cyber crime found in law books and other legal journal articles. All data collected is analyzed through interpretation techniques and then explained about the cases studied with the provisions of relevant laws and regulations. (Muhaimin, 2020).

3. FINDINGS AND DISCUSSION

The methodology in this research is normative juridical. The data used is relevant and the analysis method is appropriate. The research steps and tools used to collect data are 1) collecting primary data, interviews and direct discussions with sources related to e-commerce. 2) collecting secondary data on library literature, namely Law Number 8 of 1999 concerning Consumer Protection which states that anyone can file a civil lawsuit with the District Court, and Law Number 11 of 2008 as amended by Law Number 19 of 2016 about ITE and literature including books, journal articles related to the potential for cybercrime in e-commerce buying and selling transactions. 3) Carry out data collection techniques using literature studies, interviews, observation and documentation. 4) The data analysis technique, namely descriptive qualitative, is used in the form of an interactive analysis model, namely all the data collected is analyzed and interpreted, and then the explanation and conclusions are explained.

Among the many cases of personal data leakage in Indonesia, the one that has attracted the most public attention is the data leak case experienced by e-commerce, namely Tokopedia, 20 on March 2020, where hackers managed to hack almost all of their accounts and succeeded in taking their data. The perpetrator managed to steal around 91 million user data and more than 7 million merchant data from the platform. The hacked information, such as names, email addresses and user passwords, was then sold for around US$ 5,000 or the equivalent of IDR 74.5 million at an exchange rate of IDR 14,900/US$.

The use of e-commerce applications is not balanced with the application of high and accurate security technology and the very vulnerability of e-commerce applications to criminal activities,

requires innovation at the security level. to protect and prevent crime. prevalence of crime, fraud by employees, and cybercrime (Hans Schulte-Nölke et al., 2020)As a result of the outbreak of the virus which causes e-commerce applications to malfunction and results in material and immaterial losses for consumers, the cyber/cyber world workforce is the culprit for the extreme discomfort experienced by consumers when carrying out online business transactions. This will erode public trust in e-commerce applications (Apau et al., 2019)

Although it is widely recognized that the use of e-commerce can increase productivity, efficiency and cost savings, which in turn can encourage competition in the business sector, considering the elements that influence the growth and development of e-commerce, including:

a) E-commerce can reach more customers/consumers continuously/simultaneously
b) E-commerce can promote seller/business actor innovation precisely and accurately
c) E-commerce can create/produce high-efficiency, cheap/low-cost, and informative
d) International, intergalactic, and 24 -hour E-commerce.

In e-commerce transactions, the following parties are involved:

a) Sellers are business actors who are run as individuals or business entities
b) Consumers/buyers are people who use the services of business actors, both individually and corporately.
c) The acquirer is the collection intermediary.
d) The issuer is a credit card company/corporation consisting of banks and non-bank financial institutions (Dharma et al., 2013)

Even though the payment system used in e-commerce is as follows:

a) Electronic money such as tokens, net cash, visa cash, e-cash, millicent, cybercoin, and wordpay.
b) Banking debits such as Bank internet payment systems (BPIPS), FSTC electronic checks.
c) Credit systems such as Paylater
d) IT Digital money
e) cyber money
f) first virtual
g) Net Chat
h) E-gold

Apart from that, there are several characteristics of cybercrime, where the action is carried out in data space in cyberspace without permission or in a way that violates the law and is unethical:

a) Equipment connected to the Internet application network is used in the action.
b) Behavior that results in material or immaterial losses
c) National and international (Wijoseno & Widhiyaastuti, 2023)

Based on their actions, we must understand several categories of cybe crime:

a) System Unauthorized access to computers and services, namely when criminals (hackers) illegally gain access or infiltrate a computer network system without the owner's consent or with the aim of stealing. facts or information that are confidential and sensitive (Rahayu et al., 2021)
b) Content that violates the law, such as crimes committed by entering information or data into internet applications that are incorrect or false, unethical and formal illegally, or disturbing public order by slandering other people and degrading their dignity.
c) Data falsification, namely the criminal act of falsifying important documents or data recorded in unscripted documents via the internet network, is aimed at e-commerce documents and is carried out with the intention of gaining profit from this criminal act (Suharto & Kurniawan, 2020)
d) Cyber espionage, a crime involving illegal entry into a computer network system to conduct spying operations, is usually targeted at competitors in the e-commerce industry.
e) By interfering with, deleting, or destroying data on computer programs connected to the internet network, cyber sabotage and cyber extortion, crimes like this, are carried out.
f) Intellectual property infringement, also known as IPR, is a type of crime that involves violating the rights of others by illegally copying the web pages of their websites, which contain private information about their trading activities (Ramli, 2004)
g) Violation of privacy: this crime targets a person's personal information or data which is stored in the form of personal data and if discovered by other people, can cause both material and immaterial losses to the victim, such as credit card numbers and ATM PINs.
h) Carding is a criminal act that involves the use of computer technology to carry out credit card transactions for other people or parties, which harms other people both materially and intangibly (Kusumaningtyas, 2019)

We often see e-commerce fraud everywhere, namely on social media, via cellphone numbers, or in person. Typically, cybercriminals pretend to be legitimate e-commerce groups and then deliver fake products using special lures that lure victims with their personal data and money. Cybercrime often involves fraudulent tricks against its victims (Rantesalu, 2022)But what is the objective factor of e-commerce fraud. Based on literature studies, the factors that cause fraud in e-commerce are as follows:

a) User knowledge factor is minimal

The entire community needs to be educated to understand the dangers of online transaction fraud. Everyone is required to be clever at using digital in the era of globalization Society 5.0. Socialization to the public is needed to understand and be wary of digital transaction fraud. With this socialization movement, the public knows the motives for online transaction fraud.

b) User data leak

User data leaks are usually caused by user error. To prevent personal data from being leaked, you must not provide personal data such as ID Card/KTP, SIM, account number, verification code or other personal information. If our personal data is shared or distributed, it can be used by bad people to carry out illegal activities. Apart from that, data breaches can also be caused by hackers and data hackers. People who can do this are those who know the technology but are not good at using it positively. Hackers use our data through online links/sites. Therefore, if you receive a link or email that you are not sure about, do not open it because it could be a trap for the hanker to carry out his actions (Artikov, 2021).

c) Users are tempted by fake prizes

Few people understand online transaction fraud, but there are still those who fall for fraud cases. Users are tempted by millions of rupiah in prizes, discounted goods, and other luxuries. Users are tempted by fake prizes. For example, if the user needs money, fraudsters promote prize offers of tens of millions through easy terms. We must be wise regarding our actions in dealing with it, even though in difficult conditions we must think logically and rationally (Suharto & Kurniawan, 2020).

d) Unemployment and poverty rates are high

Some people have a short mind to commit crimes because job opportunities are limited and competition is tight. Online transaction fraudsters carry out their actions using false promises. The government's concern and attention are really needed to act against online transaction fraud. Increase employment opportunities thereby reducing the poverty rate, along with reducing online transaction fraud.

e) The security system and lack of firm government policy

Indonesia's e-commerce security system is not safe, an example of the Tokopedia application data leak case. Government policies are less firm, giving cybercriminals opportunities. The Law and the Minister of Communication and Information oversee the security of e-commerce transactions in Indonesia. However, the policy has not been completely successful, as evidenced by the fact that there are still many cases of e-commerce fraud. To reduce the number of fraudulent e-commerce transactions, it is our right as citizens to report cases like this to the authorities (Fauzi & Primasari, 2016) Cybercrime uses various methods to obtain victims' personal data in their operations. Some frauds in e-commerce transactions include the following:

a. Phishing is an act of fraud in which files with fictitious links are sent via email by cybercriminals. Cybercrime will trick its victims into believing that the link provided is an official E-commerce platform link, requiring them to enter personal information to claim the promised prize. This is the most widely used phishing method (Suharto & Kurniawan, 2020)

b. Pharming is a deceptive cyber crime scheme in which victims are tricked into visiting fake websites by redirecting them from legitimate websites. Therefore, victims will enter a site that they believe is a legitimate website and will fill in personal information or any other data that may be required by cybercrime through a fake website without hesitation (Kusumaningtyas, 2019)
c. Pretexting is a cyber crime that carries out fraudulent actions asking for the victim's personal data by disguising themselves as the name of a certain e-commerce. Cybercrime will acknowledge requests for victims' personal data to facilitate e-commerce access. Cybercriminals can easily use victims' personal data for their own personal interests.
d. Quid Pro Quo is a fraud carried out by cybercrime by persuading the victim to offer a gift in the form of money or other valuables on the condition that the victim provide his/her personal data first. The perpetrator will then profit from the personal data information, and although this will not happen, the promised reward will be processed. because cyber crime victims are tricked into providing their personal information.
e. Contacting Victims, this scam is most successful, this is the action that is most often avoided. The prize will be sent directly to the account number if the cybercriminal contacts the victim's telephone number or WhatsApp number and then pretends to come from an online shop that offers prizes on condition that they only provide the account number. Cybercriminals talk like official e-commerce parties, use standard language similar to e-commerce services in general, and repeatedly persuade and convince victims until they are incited. This action is most successful in most cases. It is recommended to just turn it off and not continue if an unknown number appears claiming to be from an e-commerce party offering prizes to prevent fraud. Cybercrime has methods and strategies to convince and persuade victims until they believe (Kusumaningtyas, 2019)

Meanwhile, the following procedures are usually followed in cybercrime:

a) Collect and evaluate data and information on the computer network and target operating system.
b) Accessing a target's computer network or infiltrating it against its rights.
c) Seeking greater and more technologically advanced access to a computer system than the target or victim's access
d) Add a back door or remove all traces.

Committing fraud in online transactions is illegal. The law enforcement process is hampered by cybercrime for several reasons, including:

a) Due to limited space and the unclear identity of the perpetrator, investigators need time to arrest the perpetrator.
b) Collecting evidence considering that online transactions are regulated in the Criminal Code (lex generalis) and additional evidence permitted in the ITE Law (lex specialist) (Rahmanto, 2019)

c) The facilities and infrastructure (sophisticated equipment) available to investigators are not utilized optimally in gathering information and finding criminals.
d) Citizen's awareness. Many people still don't know the correct way to carry out online transactions to avoid fraud by cybercriminals. People want to make transactions quickly and easily, but are deceived by promises of big profits when all that is offered is a series of lies. For example, there have been cases of binomo, farehnheit, and similar crimes where the public seemed to be hypnotized by the luxury cars displayed by the suspect, even though the real aim was to attract the attention of the victims and persuade them to invest their money in his business. without first verifying whether the business is truly registered or just a fake business (Fadhila, 2021)

The following types of fraud often occur in e-commerce transactions:

a) Incompatibility of products/goods obtained by consumers with what they requested.
b) Use of fictitious business actors or consumers or use of fake identities.
c) Discounts or fake sales rates offered by commercial actors (Fadhila, 2021)

This crime of fraud is defined as the dissemination of false or misleading information regarding product advertising or consumer identity which results in material and immaterial losses for both consumers/buyers and business actors/sellers. Based on this, if there is a legal problem then the provisions of Article 45 A paragraph 1 of the ITE Law apply criminal law with a maximum penalty of six years in prison and/or a maximum fine of one billion rupiah, then firstly the ITE ma and technical investigations still refer to rule B PK.

Likewise, if legal problems arise in e-commerce transactions, civil legal action must refer to the ITE Law in conjunction with the Consumer Protection Law in conjunction with the Trade Law which also regulates procedures for selling online. Then the solution must look at the choice of law or choice of law, which law is agreed upon or is subject to which law is the law in the business actor's country or uses international law. For the convenience of both parties, e-commerce transactions should be carried out with a written agreement/contract that is approved and signed by the parties. If the contract has been agreed upon, formal legal rights and obligations arise between the parties making the agreement, whether using litigation or non-litigation legal processes (alternative dispute resolution).

Law Number 11 of 2008 which was later revised/updated to become Law Number 19 of 2016 concerning ITE functions as the legal basis for controlling cyber crime. Criminal law provisions are regulated in Articles 27 to 35 which explain the form and nature of the offense (Ks et al., 2022) The law then regulates criminal threats in Articles 45 to 52, with details of each article as follows:

Regarding the offense of disseminating, disseminating or transferring unauthorized material.

a) Article 27 paragraph 1 of the Constitution contains regulations relating to morality.
b) Article 27 paragraph 2 regulates gambling

c) Article 27 paragraph 3 of the Constitution regulates slander and defamation.
d) In Article 27 paragraph 4, threats of extortion are prohibited.
e) Article 28 paragraph 1 regulates fake news, misleading news and fraud.
f) Article 28 paragraph 2 SARA regulates incitement to hatred.
g) Article 29 of the Constitution regulates the threat of domestic violence.
h) Article 30 of the Constitution regulates unauthorized access.
i) Article 31 paragraph 1 regulates illegal wiretapping and wiretapping.

Crimes involving interference or interference

a) Intervention with confidential data based on article 32
b) System disruption as intended in Article 33
c) Providing resources for activities prohibited under article 34
d) Relation of Article 35 to Manipulation or Falsification of Information
e) Weighing - Article 52,

Considering Criminal Threats.

a. The investigation as intended in Article 42 must be carried out in accordance with the criminal provisions/provisions regulated in this law and the terms/conditions of the criminal procedural law.
b. Evidence for investigation, prosecution and trial as regulated in Article 44 is amended in accordance with the law or ius constitum, namely (lex generalis), and is equipped with electronic evidence which is regulated in the requirements of this Law as a special provision (lex specialist) .
c. Articles 45 to 52, which regulate criminal threats posed by cybercrime, provide for the most severe penalties without setting a minimum period.

If we look at the comparison of cybercrime laws in Singapore and Malaysia from neighboring countries, it turns out that the publication, and distribution of illegal content using the internet, computers and technology is not considered part of cybercrime. In Singapore, cybercrime includes the Computer Misuse Act which prohibits certain types of cybercrime such as unauthorized access, disclosure of secrets, destruction or damage to computer systems or electronic data, and computer fraud. Similarly in Malaysia, the Computer Crimes Act covers essentially the same offenses as Singapore's Computer Misuse Act. Both countries do not have special provisions regarding freedom of expression such as online defamation and hatred because these violations are covered by the standard Criminal Code.

The development of technology now provides new nuances in the field of evidence in court so that the evidence presented at trial is not only limited to physical evidence as regulated in the Criminal Procedure Code which includes documentary evidence or witness evidence, but also documentary evidence or witness evidence. has also extended to the use of physical evidence. Evidence in the form

of digital documents in the form of discs (CS, VCD, DVC) or other evidence in the form of writing on social media and other electronic evidence (Dharma et al., 2013)

The birth of the ITE Law is little progress in responding to and overcoming the current rise in cyber crime, especially in the law enforcement process. If we look at Article 1 paragraph (1) of the ITE Law, it is stated that electronic information is one or a collection of electronic data, including but not limited to written information. , sounds, images, maps, photo designs, electronic data intercharge (EDI), electronic mail (electronic mail, telegram, telex, telecopy or similar, letters, signs, numbers, access codes, symbols or processed perforations that have meaning or can be understood by those who can understand it (Sumiyati, 2018)

In Article 1 point (4) of the ITE Law, it is stated that any electronic information that is created, forwarded, sent, received, or stored in analog, digital, electromagnetic, optical, or similar form can be seen, displayed and/or heard via a computer or electronic system. , including but not limited to writing, letters, images, maps, designs, photos or the like, letters, numbers, access codes, symbols, or perforations that have meaning or significance that can be understood by people who are able to understand them (Rahmanto, 2019)

From the meaning of Article 1 paragraphs 1 and 4 of the ITE Law, there are differences between electronic information and electronic documents which form the basis of both, namely:

a) In principle, electronic information can be distinguished but cannot be separated from electronic documents.
b) Electronic information is data or a collection of data in various forms
c) Electronic documents are containers or packages of electronic information
d) For example, if we are talking about a music file in mp3 form, then all the information or music that comes out of that file is electronic information, while the document from that file is mp3.

If we look again at the comparison between the Criminal Code, specifically articles 310, 311, and the ITE Law, it turns out that the criminal threat of the ITE Law is higher than the Criminal Code. Changes to the legal regulatory framework related to ITE from Law Number 11 of 2008 which was amended/enacted into Law Number 19 of 2016 are contained in the provisions of articles: 1, 26, 31, 40, 43, and 45 paragraphs (A) and (B) which the same and does not apply the threat of a minimum sentence (Rahmanto, 2019)

Apart from knowing the government policies, laws, and regulations that regulate cases of e-commerce fraud, society as a whole must also be smart in facing the increasingly growing era of globalization and digitalization. We don't have to rely completely on government policies, to take the risk of becoming the next victim. Because, in general, fraudsters never hesitate to commit crimes. As an intelligent citizen, you must be alert to respond, seek clear information, and be able to report to the

authorities any losses caused by fraud. Several steps to prevent fraudulent transactions are as follows: a) Choose an e-commerce platform that is official and has been supervised by the OJK, b) Pay attention whether the verification code has a blue tick, c) Do not share confidential verification codes, d) Must read the information and transaction process carefully, e) Always act in good faith when making transactions, f) Pay according to the nominal value stated in the application, g) Be wise in responding to fraud cases, h) Read the latest news about the latest fraud motives, i) Don't immediately believe and be tempted by gifts given for free, j) always be careful when making transactions (Silalahi et al., 2022)

More specific solutions to overcome the problem of cybercrime in E-commerce:

1. Backups.

Backup is a basic principle of security mechanisms that must be implemented in all technology, especially in the world of e-commerce. If data is lost, this will have fatal consequences, especially in terms of trust in all stakeholders, and of course it will be very detrimental. Lost data is also accompanied by reduced hope that the data will be returned. Therefore, backup is a simple step that will be very useful and important in the future.

2. Use of SSL Certificates.

SSL or secure socket layer is a protocol for data encryption, and is used as a standard when the data exchange process between client & server occurs safely (Adobe Communications Team, 2022). SSL is a security standard that is recognized and has been proven to secure online transactions, including e-commerce. If compared to HTTPS, it is a protocol in browsers for safer communication, then on the other hand, SSL is an encryption protocol used by HTTPS for the data encryption process.

3. Firewalls.

With a firewall, configurations can be made regarding what traffic regulations are allowed to enter and exit. With a server that has a firewall installed, the server will only allow traffic that is trusted and in accordance with existing regulations.

4. E-Commerce Security Plugin.

Security protection from various types of attacks such as bots and formjacking as well as various other cyber attacks. Some security plugin products will automatically patch or update regularly. The plugin will work by warding off and preventing malicious requests from entering the web server.

5. Multilayer security.

Mechanism for adding security methods when entering a system. If the first layer is successfully hacked, then the next hacker must break into the next layer, and so on. Multilayer security makes it difficult for hackers to break into system security if there is more than one layer.

6. User and Staff Education.

Security gaps often occur not in terms of security on the web server but in e-commerce users themselves. Users are sometimes easily influenced to click on dangerous links or use common and easy-to-guess passwords. Education for e-commerce users can be done by displaying information on preventing phishing attacks and the use of weak passwords via the website homepage. Education can also be spread via SMS or other instant messaging applications. E-commerce companies must also have clear and firm policies in taking action if crimes occur within the internal environment. When an employee leaves or resigns, the company is obliged to revoke all access to that employee. Apart from that, both users and e-commerce service providers must always be alert and always monitor if suspicious transactions occur.

The multi-stakeholder perspective considers including the government, business actors, and consumers, to obtain a more holistic and comprehensive understanding of where all parties are involved and also how to present it using various methods that can mutually support the problem and its solution. This review will go into depth into how collaboration between various stakeholders including government, business actors, consumers can strengthen the implementation and monitoring of e-commerce problems, solutions and regulations. Challenges in E-commerce can be overcome by focusing on effective collaboration between various stakeholders. Stakeholder collaboration is key in solving problems, and designing regulations that reflect the needs and dynamics of the rapidly developing E-Commerce industry.

The government, business actors, and consumers need to unite to form balanced and progressive policies. First, the government has a crucial role in formulating effective, and adaptive regulations. By involving business actors and consumers, the government can understand in depth the challenges and opportunities faced by business actors. A transparent and participatory policy formulation process will ensure that regulations take into account various perspectives and interests. The role of business actors in this collaboration is no less important. They can provide practical insight into regulatory implementation, identify potential bottlenecks, and provide an in-depth operational perspective. Collaboration with business actors can also ensure that regulations remain relevant to the latest technological advances and business practices.

Community participation as consumers is an important element in stakeholder collaboration. They can bring a consumer perspective, highlighting consumer needs and concerns that might otherwise be overlooked. By involving the public as consumers, problems, solutions and regulations in e-commerce can become more inclusive and strengthen consumer protection. Stakeholder collaboration, if done well, can solve problems, provide solutions and create balanced E-Commerce regulations, supporting sector growth, protecting consumers, and maintaining the integrity of digital markets. Continuing dialogue

and active involvement of all parties involved is the key to resolving problems, providing specific solutions, and overcoming challenges in implementing E-Commerce regulations.

4. CONCLUSION

Based on the findings of this research, it can be concluded that cybercrime in e-commerce buying and selling transactions has increased significantly, including minimal knowledge, waste of money, being tempted by fake gifts, high levels of unemployment and poverty, and less firm government security policies. Forms of cybercrime in e-commerce include hacking, identity theft, data breach, phishing, spamming, pharming, pretexting, qui pro quo, and contacting the victim directly. Specific solutions are needed to overcome the cybercrime problem of e-commerce buying and selling, namely Backup, Use of SSL Certificates, Firewall, E-Commerce Security Plugin, Multilayer security, User and Staff Education. Suggestions require multi-stakeholder collaboration between government, business actors, and consumers to form balanced and progressive policies. The government has a crucial role in formulating effective and adaptive regulations. Stakeholder collaboration, if done well, can solve problems, provide solutions, and create balanced E-Commerce regulations, supporting sector growth, protecting consumers, and maintaining the integrity of digital markets. Continuing dialogue and active involvement of all parties involved is the key to resolving problems, providing specific solutions and overcoming challenges in implementing E-Commerce regulations.

REFERENCES

Apau, R., Koranteng, F. N., & Gyamfi, S. A. (2019). Cyber-Crime and its Effects on E-Commerce Technologies. *Journal of Information*, *5*(1), 39–59. https://doi.org/10.18488/journal.104.2019.51.39.59

Artikov, A. K. (2021). Cybercrime As a Threat To Public Safety. *Texas Journal of Multidisciplinary Studies*, *1*, 171–178. https://doi.org/10.31085/2310-8681-2021-1-204-171-178

Azizah, S. Z., Asikin, Z., & Parman, L. (2021). Implementation of E-Commerce Crime Law Enforcement at the West Nusa Tenggara Regional Police. *International Journal of Multicultural and Multireligious Understanding*, *8*(2), 7. https://doi.org/10.18415/ijmmu.v8i2.2273

Dharma, A. A. G. S. S., Sarjana, I. M., & Indrawati, A. A. S. (2013). kajian Yuridis Keabsahan Jual Beli Secara Elektronik (E-Commerce) dengan Menggunakan Kartu Kredit. *Kertha Semaya: Journal Ilmu Hukum*, 1–11.

Fadhila, A. P. (2021). Penegakan Hukum Terhadap Tindak Pidana Penipuan Berbasis Transaksi Elektronik (Legal Enforcement Against Fraudulent Acts in Electronic-Based Transactions). *Jurnal Siara Hukum*, *3*, 274–298. https://katadata.co.id/0/analisisdata/5f7c5da0cc927/kenali-maraknya-penipuan-online-saat-pandemi

Fauzi, S. N., & Primasari, L. (2016). Tindak pidana penipuan dalam transaksi di situs jual beli. *Recidiive:*

Jurnal Hukum Pidana Dan Penanggulangan Kejahatan, *7*(3), 250–261. https://jurnal.uns.ac.id/recidive/article/viewFile/40603/26760

Fianyi, I. (2016). Curbing cyber-crime and Enhancing e-commerce security with Digital Forensics. *IJCSI International Journal of Computer Science Issues, Volume 12, Issue 6, November 2015*, *12*(6), 78–85. http://arxiv.org/abs/1610.08369

Hanim, L. (2011). Pengaruh Perkembangan Teknologi Informasi Terhadap Keabsahan Perjanjian Dalam Perdagangan Secara Elektronik (E-Commerce) Di Era Globalisasi. *Jurnal Dinamika Hukum*, *11*(Edsus). https://doi.org/10.20884/1.jdh.2011.11.edsus.262

Hans Schulte-Nölke et al. (2020). The legal framework for e-commerce in the Internal Market. *Policy Department of Economic, Scientific and Quality of Life Policies*, *Study for the committee on the Internal Market and Consumer Protection*, *Policy Department for Economic, Scientific and Quality of Life Policies*, *European Parliament*.

Haryani Putri, A., & Endang Hadrian. (2022). Perlindungan Hukum Bagi Korban Penipuan Jual Beli Online. *Krtha Bhayangkara*, *16*(1), 131–138. https://doi.org/10.31599/krtha.v16i1.1018

Ks, S., Ablisar, M., Mulyadi, M., & Leviza, J. (2022). Analisis Yuridis Terhadap Tindak Pidana Manipulasi Informasi Pengguna E-Commerce Menurut Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik banyak dim. *Locus: Jurnal Konsep Ilmu Hukum*, *2*(542), 42–57.

Kusumaningtyas, J. A. (2019). Analisa Pengelompokan Cyber Crime PadaPenerapan Electronic Commerce. *Jurnal Prodi Teknik Informatika UNW "Multimatrix," 11*(1), 9–19.

Lubis, F. (2022). Cyber Crime E-Commerce Business Transactions. *Journl of Sasi*, *28*(4), 589. https://doi.org/10.47268/sasi.v28i4.1068

Muhaimin, M. (2020). *Metode Penelitian Hukum*. Mataram: Mataram University Press.

Putri, J. D., Priyatna, M. R., Empy, M. N., & ... (2023). Akad E-Commerce Jual Beli Online Ditinjau dari Kompilasi Hukum Ekonomi Syariah. *Al-Muamalat: Jurnal Ilmu Hukum & Ekonomi Syariah*, *8*(2), 43–59. https://journal.iainlangsa.ac.id/index.php/muamalat/article/view/5193

Rahayu, S. K., Ruqoyah, S., Berlina, S., Pratiwi, S. B., & Saputra, H. (2021). E-commerce Dan dampaknya pada teknologi E-Commece. *Journal of Information System, Applied, Management, Accounting and Research.*, *5*(3), 632–639.

Rahmanto, T. Y. (2019). Penegakan Hukum Terhadap Tindak Pidana Penipuan Berbasis Transaksi Elektronik (Legal Enforcement Against Fraudulent Acts in Electronic-Based Transactions). *Jurnal Penelitian Hukum De Jure*, *19*(1), 31–52.

Ramli, A. M. (2004). *Ahmad M. Ramli, Cyber Law dan Haki – Dalam Sistem Hukum di Indonesia , PT Refika Aditama, Bandung, 2004. Hlm. 1. 1 1*. 1–18.

Rantesalu, H. (2022). Online Shopping Fraud Crime Commitment in East Java Regional Police Area. *Janaloka Jurnal*, *1*(2), 70–94.

Rohmat, A., Ayu, H., Putri, A., Muhtarom, M., & Fortina, A. (2024). Potential Cybercrime and Prevention in the Overseas Official Travel Approval Letter. *AL-MANHAJ Jurnal Hukum Dan Pranata Sosial Islam*, *6*(1), 87–98. https://doi.org/10.37680/almanhaj.v6i1.4674

Santoso, E. (2022). Opportunities and Challenges: E-Commerce in Indonesia from a Legal Perspective. *Jurnal Penelitian Hukum De Jure*, *22*(3), 395. https://doi.org/10.30641/dejure.2022.v22.395-410

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.

Sonata, D. L. (2015). Dualisme Penelitian Hukum Normatif dan Empiris. *Fiat Justisia Jurnal Ilmu Hukum*, *8*(1), 15–35.

Suharto, B., & Kurniawan, A. B. (2020). Tindak Pidana Cybercrime bagi Pelaku Pemalsuan Data pada Situs E-Commerce (Phising). *JHP 17 (Jurnal Hasil Penelitian)*, *5*(2), 57–61. http://jurnal.untag-sby.ac.id/index.php/jhp17

Sumadinata, W. S. (2023). Cybercrime And Global Security Threats : A Challenge In International Law. *Russian Law JournaL*, *XI*(3), 438–444.

Sumiyati. (2018). Perjanjian Belanja Online Berdasarkan Kitab Undang-Undang Hukum Perdata Dan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *Jurnal Sigma-Mu*, *Vol.10*(No.1), 1–16. https://jurnal.polban.ac.id/ojs-3.1.2/sigmamu/article/view/1173/964

Ummiyati, D., & Anggono, A. (2020). Cybercrime Behavior Mode Through E- Commerces. *International Colloquium on Forensics Accounting and Governance (ICFAG)*, *1*(1), 202–210.

Wibowo, E. A. (2016). Pemanfaatan Teknologi E-Commerce Dalam Proses Bisnis. *Journal of Equilibiria*, *1*(1), 95–108.

Wijoseno, B. A., & Widhiyaastuti, I. G. A. A. D. (2023). Jerat Pidana Terhadap Pelaku Peretas Sistem Komputer Secara Ilegal (Hacker) Dalam Perpsektif Hukum Pidana Indonesia. *Jurnal Kertha Desa*, *11*(3), 2031–2041.

Yadi, D. K., Sood, M., & Martini, D. (2022). Perlindungan Hukum Bagi Para Pihak Dalam Transaksi E-Commerce Menurut Tata Hukum Indonesia. *Commerce Law*, *2*(1). https://doi.org/10.29303/commercelaw.v2i1.1368

Yulia Santri Harahap, E., Ramadhani, N., & Manajemen, J. (2022). Cybercrime and Its Impact on E-Commerce Technology. *Jurnal Ekonomi Manajemen Akuntansi Dan Keuangan*, *3*(1), 188–192.