CONSENSUS
JURNAL ILMU HUKUM
https://consensus.stihpada.ac.id/
E-ISSN: 2962-2395
Volume 3 Nomor 2 November 2024 Page : 73-82
Alamat:
Jl. Kol. H. Animan Achyad (d/h. Jl. Sukabangun II) KM. 6,5 No. 1610
Kelurahan: Sukabangun. Kecamatan: Sukarami, Palembang.
Telp & Fax: 0711-418873/email: jurnalconsensus@gmail.com

Cybercrime Regulations In Indonesia

Haura Adietyana
Sekolah Tinggi Ilmu Hukum Sumpah Pemuda, E-mail: hauraadiet@gmail.com

Abstract
In today's world, technology is getting better. Computers, AI, and robots are getting more advanced. It makes things easier for people. People can shop, bank, send emails, study, and more online. Some people use technology to commit crimes. Cyber crime includes unauthorized access to computer systems, illegal content, data forgery, cyber espionage, cyber sabotage, infringement of privacy, carding, phishing, defacing, and cyber talking.

Keywords: Cybercrime, AI, Robots.

INTRODUCTION

This era of globalization has brought us great changes in our lives. As stated by Wijaya and Arifin (2020) As a continuation of a state characterised by interconnectedness, border blurring, and the growth of technology and information, globalisation is the act that is changing the nature of the global environment (Wijaya, M. R., & Arifin, R, 2020:63-74). It has a huge impact on many sectors. Basically, globalization started at the beginning of the 20th century, when theelectronic devices and transportation underwent major changes and it becomes more sophisticated. That major changes happened in order to accelerate the trade (cross good and services) among nations.

Now we are in the era of revolution industry 5.0. Revolution itself occurs in many areas of human existence, including industry, culture, education, technology, and technology systems, among others. Leng et. al (2012) explained that Industry 5.0 is a prime example of the value of humanistic care and recognises the evolution towards a symbiotic ecosystem by fusing the subjectivity of humans and intelligence with the efficacy, artificial intelligence, and accuracy of machines in industrial output (Leng et al, 2022:279-295). Technological advancements, particularly in the fields of communication and transportation, are regarded as locomotives that aid in the acceleration of the globalization process in various sectors of life. In this era, we can do anything electronically such as, e-banking, e-commerce, e-money, e-learning, etc. With the advancement of technology and internet, we can do anything from anywhere, with just one click.

Indeed, this massive revolution has a positive side which it makes people easier to running errands.This massive revolution certainly has the positive side of making it easier for people to run their affairs. But on the other hand, the revolution has resulted in an increase in the number of crimes that can be committed using technology. Many individuals have misused the development of technology as a means that should make it easier for people to communicate, transact, and conduct business. But in the other side, revolution has resulted in an increase in the number of cybercrimes that can be committed.

Darrel C Menthe (1997) stated that everyone interact in cyberspace in two ways, either they send information or retrieve information. the uploader and the downloader are two different parties in cyberspace under the law (Menthe, 1997:69). The uploader stores information in cyberspace, and the downloader retrieves it at a later date. Neither party

needs to know the other's identity. He also has three theories about cyberspace; (1) The Theory of the Uploader and the Downloader means a state may restrict, within its own territorial limits, uploading and downloading actions that it deems may be detrimental to its interests, (2) The Theory of Law of The Server means that the server on which server are physically located, i.e. where they are recorded as electronic data, (3) The Theory of International Spaces means that cyberspace is regarded as the fourth space. The analogy is found not in physical similarity, but in international nature, namely the sovereign quality (Menthe, 2004).

Cybercrime itself is defined as criminal actions related to the use of modern information technology, such as computer and network technological advances (Zhang, 2012:422-437) (Zhang et al. 2012). It is undeniable that every type of crime is unavoidable. Moreover, cybercrime is a kind of crime that doesn't have a physical form. It can be hard to detect, which means that it takes time for it to be found and, in most cases, cannot be recognized at all. For example, many people are unaware that they have had their computer or network hacked or assaulted., it is because cybercrime is not restricted by physical access limitations.

Someone with advanced knowledge of computer operation, such as an operator, programmer, analyst, or cashier could perpetrate a cybercrime (Ismail, 2009). They have the ability to corrupt data, steal it, and utilize it illegally. Sutarman (2007) on his book entitled "Cyber Crime Modus Operandi dan Penanggulangannya*"* stated that the rapid growth of communication technology such as telephones, smartphones, and other communication tools, alongside the advancement of technological innovation in computers, is one of the primary factors pushing the development of cybercrime (Sutarman et al, 2007). These are types of cybercrime; (1) Unauthorized Access to Computer Systems and Services, (2) Illegal Contents, (3) Data Forgery, (4) Cyber Spionage, (5) Cyber Sabotage and Extortion, (6) Offence Against Intellectual Property, (7) Infringements of Privacy, (8) Cyber Terrorism, (9) Cyber Pornography, (10) Cyber Harassment, (11) Cyber Stalking, (12) Hacking, (13) Carding (credit card fraud) (Handayani, 2013).

From the report of National Cyber Security Index (NCSI), security index score in Indonesia is 38,96 out of 100 in 2022. This indicates that Indonesia is placed 83rd out of 160 countries worldwide and third lowest among the G20 (Liputan6.com, March 26 2023, accessed on October 31, 2023). Since the January 1st to December 22nd 2022, based on the data in E-MP Coaching and Operations Department Criminal Investigation Agency of Indonesia National Police (E-MP Robinopsnal Bareskrim Polri) showed that the police had cracked down on 8.831 cybercrime cases (https://pusiknas.polri.go.id/, accessed on October 31, 2023). People who take advantage of technological advancement may have been damaged as a result of the rapid growth of cybercrime. Therefore, the government must offer highly competent law enforcement experts, such as police officers, prosecutors, and judges, who are highly trained in technology, in order to secure the safety of the victim. Furthermore, the government requires a law that tightly regulates, so that victims can be protected and perpetrators may be punished appropriately to reduce that kind of crime.

PROBLEMS

In this era of massive technology development, such as the development of AI (Artificial Intelligence), robots, and many other stuff has created many conveniences in carrying out daily activities. But in the other side, the more advance the technology, the more crime that can be committed using technology, and that kind of crime called cybercrime. Furthermore, cybercrime has no physical form, so it will be hard to trace down the casebecause the perpetrators can easily disappear without a trace. Indeed, anyone can commit this crime from anywhere and everywhere with just an internet connection. Regarding to this issue, the government needs law that can protect the victim and punish the perpetrators. Also, the legal officers need to master technology so that this kind of case can be prosecuted properly.

DISCUSSIONS

1. Industry 5.0 Era

The term "industry 5.0" refers to a concept that depicts the next phase of industrialisation and focusses on human-machine cooperation in the production process.. It goes beyond efficiency and production objectives to emphasize worker well-being and the societal value of the industry. Industry 5.0 intends to leverage new technology to give prosperity beyond jobs and development while remaining mindful of the planet's production constraints. It contributes to the Industry 4.0 approach by applying research and innovation to create a more sustainable, human-centered, and resilient industry (Forbes, https://www.forbes.com/, accessed on November 2nd 2023).

In Industry 5.0 there must be some challenges that will be faced by people (Alojaiman, 2023:1318). First, people must learn many new things such as working with robots or machines. someone with good skills in operating and programming the machine will be needed in the future. Second, this technological advancement is inexpensive, so the investment would be necessary. company needs a huge amount of money to provide a training session for the employee. If money doesn't pose an issue, the speed of change will be. Furthermore, People who are unable to adjust to these huge changes in technology might be falling behind. Indeed, industry 5.0 aims to create a harmonious working space where humans and machines work together to improve efficiency, personalize products, and contribute to the overall well-being of society. While still in its early stages, Industry 5.0 possesses the possibility to cause major changes in the manufacturing sector.

2. Cybercrime

Cybercrime is defined as any crime that involves the use of a machine, a computer network, or a networked device. Individuals or groups can perpetrate it, and it may threaten someone's security or finances. Cybercriminals or hackers are the most common offenders of cybercrime, and they frequently want financial gain. However, cybercrime can also be motivated by political or personal reasons. Some examples of cybercrime are: Identity theft, Malware, Ransomware, and Business email compromise (BEC) scams.

First, Identity theft takes place when criminals exploit private data, which might include an individual's Social Security number or credit card number, to conduct purchases or open accounts (Lucas Coll, 2022, https://www.usnews.com/360-reviews/privacy/what-is-cybercrime). Second, malware is a harmful software that can be secretly placed on

someone's device in order to steal personal information and password. Third, ransomware occurs when cybercriminals seize control of a person's or company's devices and demand a ransom. Fourth, Business email compromise (BEC) scamsare scams which take advantage of knowing that a lot of people transact business via email, so they can be financially harmful (FBI, https://www.fbi.gov/investigate/cyber, accessed on October 28th 2023).

Cybercrime can be difficult to combat because it often involves cross-border attacks and the use of the internet to target people from various locations. Cybercriminals can also use the internet to magnify the scale of harm done. To protect oneself from cybercrime, it is important to take the right security measures, be alert and aware when connected, and avoid clicking on links in spam emails or unfamiliar websites. Individuals, corporations, and society as a whole can all suffer as a result of cybercrime. Cybercrime can result in monetary damage and theft of identity for individual, along with the reputational harm and legal consequences for businesses, individual may suffer financial losses. Phishing, hacking, and malware are commonly used by attackers to obtain someone's banking data, such as credit card numbers, passwords, and other banking personal information. Money may be lost as a result of illicit transaction, which can be hard to recover. Next, is identity theft. Identity theft happens when hackers take personal data, especially a Social Security number or a debit or credit card number, and subsequently use it to make purchases or start new accounts. Furthermore, it may cause emotional distress. Cyberbullying and harassment can cause persons emotional pain and injury.

Next, cybercrime has a huge impact towards business. A cyberattack may result in the loss of financial assets, intellectual properties, and information regarding customers, all of which can be expensive to recover. Due to the financial consequences of cybercrime, some businesses may even be forced to close.It may also harm a company's reputation, leading to a loss of client trust and loyalty. Next, Businesses who fail to protect their customers' data may face legal ramifications such as fines and litigation. Also, cybercrime can disrupt a company's day-to-day operations, resulting in lost income and significant brand reputation damage. Cybercrime not only has it impact on individuals and business, but the impact of it may also happened on society. First, Cybercrime can have a huge economic impact, resulting in financial losses for individuals, corporations, and governments. The cost of fixing system damage, recovering lost data, and avoiding future assaults can be considerable. It may also have an effect on customer trust in online transactions, reducing the adoption of digital platforms. Second, cybercriminals can target government organizations and essential infrastructure, cybercrime can constitute a threat to national security.

3. Types of cybercrime

1. Unauthorized Access To Computer System And Service

Unauthorized access to or infiltration of a computer network system without the owner's consent or agreement may lead to this criminal action (Ketaren, 2016:35-42). The motivations vary and include sabotage, data theft, and so forth.

2. Illegal Contents

This type of crime can be committed through the transfer of information, data, or other material onto the internet concerning something that is false, unethical, illegal, or

disrupts public order. Common instances of this kind of crime includes sexually explicit material, the dissemination of false information, and political violations committed in cyberspace.

3. Data Forgery

Falsifying data on critical information published as documents on the internet is a felony. The target of this crime is the important documents that belongs to e-commerce (Putra, & Sutabri, 2023:11-20).

4. Cyber Espionage

A crime committed by infiltrating the victim's computer network system and using the internet network to spy on them. This type of crime is typically committed against company competitors whose records or information are kept in a digital system.

5. Cyber Sabotage and Extortion

This felony is perpetrated by interfering with, damaging, or destroying data, computer programs, or computer network systems linked to the internet. Usually, a computer virus or specialized software is used to commit this crime, rendering the network system or computer program data unusable, malfunctioning, or, no longer functioning as the offender intends. This type of crime is also known as cyberterrorism.

6. Offence Against Intellectual Property

This crime targets IPR (intellectual property rights) held by third parties on the internet. Copying the web appearance of a certain site, for example, or publicizing trade secrets that are someone else's trade secrets.

7. Infringements of Privacy

This offense is committed against a person's highly intimate and confidential information. The crime is recorded on a computer. It can inflict material or immaterial damage if it is known to others, such as ATM PIN numbers, credit card numbers, and so on.

8. Carding

Carding is a type of crime that steeling someone's credit card number and it being used for online transaction. The perpetrators usually got the data by buying it from spamming networkhttps.

9. Phising

This crime usually attract the internet users to give their personal data (username and password) on a defaced website. Those personal data is use to get someone's e-banking data, so that the perpetrators could get the whole access to the bank account of the victim. Phishing is typically carried out through spoofing e-mails or instant chats, and it frequently encourages people to enter information on a false website that appears and feels very identical to the real one.

10. Defacing

Similarly with hacking, defacing focused on the display changes of the website. Some defacing acts are done for pleasure, to demonstrate one's ability to write programs, some actions are taken to steal information and sell it to outside parties.

11. Cyberstalking

The perpetrator will do a harassment to their victim using e-mail and done repeatedly. It is like a terror that addressed to someone, and it could happened because the easiness in making an e-mail address without the actual profile.

4. Cybercrime cases

1. Ransomware

On May 2023, a group of hacker named Lockbit from Rusia claimed that they has disabled the server of Bank Syariah Indonesia (BSI) (Cloudeka, https://www.cloudeka.id/id/berita/web-sec/contoh-kasus-cyber-crime/, accessed on October 14th 2023). Because of this accident, the customers are unable to access their Mobile Banking. Besides, Bank Syariah Indonesia also lost their 1,5 TB of their customer and employee private data. Furthermore, Lockbit threatened Bank Syariah Indonesia that they would sell those data to the dark web if BSI cannot give them a sum of money. This kind of crime known as ransomware.

2. Hoax News

The initial of EJA (38), sent a hoax news to his/her client e-mail about five banks that are in liquidity distress. According to reports, the EJA received verbatim information from brokers regarding a number of banks liquidity distress. EJA sent that news to his/her client with the company's domain and this information has spread beyondand is believed that it may cause in a rush or chaos.

3. Pornography

A content creator named Dea posted a content that contain pornography on a platform called "Onlyfans". Dea is a suspect for violating Article 27 paragraph (1) in conjunction with Article 45 paragraph (1) of Law Number 19 of 2016 concerning ITE and/or Article 4 paragraph (1) in conjunction with Article 29 and/or Article 4 paragraph (2) in conjunction with Article 30 and/or Article 8 Jo Article 34 and/or Article 9 Jo Article 35 and/or Article 10 Jo Article 36 Law Number 44 of 2008 concerning Pornography (CNN Indonesia, https://www.cnnindonesia.com/nasional, accessed on October 28 2023).

4. Defamation

Omni International Hospital reported a crime committed by PritaMulyasari to the police. Mulyasari made an e-mail about her experience while being treated at the emergency room. At first, Mulyasariwas sentenced to pay material damages of 161 million as for the material losses and 100 million for immaterial losses (Detik news, https://news.detik.com/berita/, accessed on October 28 20223). But then, after judicial review, Mulyasari declared not guilty.

5. Email Scams (Phising)

Fraud using this media has even been linked to the international mafia. This email scams also known as phising. Based on CNBC Indonesia, Indonesia being the country which has the most phising case with 208.238 cases in 2022 (CNBC Indonesia, https://www.cnbcindonesia.com/, accessed on October 28 2023).Someone would ask for assistance in "receiving" money from a completed project or for other reasons related to the bank account of the possible victim. The enticement is that the victim will receive 30% of the money, which is worth billions of rupiah. Several reports eventually revealed,

however, that they initially had to transmit roughly 0.1 percent of the amount of money belonging to the victim to the person who committed the fraud. Finally, despite being sent, the promised funds were not received. As a pure act of crime, this offense has a cybercrime motive.

6. Cyber Vandalism

The occurrence of changes in the KPU *(KomisiPemilihanUmum)*website. On April 17 2004, Dani Hermansyah vandalized the website by replacing the names of current parties at www.kpu.go.ig with fruit names (DungaAshola, https://dungaashola.wordpress.com/, accessed on October 28 2023). As a result, the public lost faith in the democratic process that was taking place at the moment. It is not impossible that the numbers of voters recorded on the website are not secure and can be modified by changing the names of the parties on the website. This offense is committed by altering the appearance and content of the website. As a pure act of crime, the motivation for this offense falls under cybercrime.

7. Distributed Denial of Service

Denial of Service (DoS) and Distributed DoS (DDos) attack is to take control of the government's electronic base using virus attack (Sirohi, 2015). This is not a stealing, eavesdropping, or data falsification attack. However, due to the loss of service, the target is nolonger able to supply services, resulting in a financial loss. This criminal behaviour is carried out by causing a service or service to fail. As a pure act of crime, the motivation for this offense falls under cybercrime.

5. Cyberspace Law

The scope of the internet is vast and limitless. Therefore, Jonathan Rosenoer (1997) categorizes the scope of cyberlaw into: (1) Trademark, (2) Copyright, (3) Illegal Access, (4) Hate Speech, Hacking, (5) Defamation, (6) Duty Care, (7) Electronic Contract, (8) Pornography, (9) Hacking, (10) Regulation Internet Resource, (11) Procedural Issues (Jurisdiction,Investigation, Evidence), (12) Robbery, E-Commerce, (13) Viruses, (14) E-Government, (15) Consumer Protection, (16) Criminal Liability, and (17) Privacy (Rosenoer, 1997). In Indonesia itself, the scope of cyberlaw distinguished into two: (1) Public Law includes Juridiction, Online Activity Ethics, Consumer Protection, Antitrust, Fair Competition, Taxation, Regulatory Body, Data Protection and Cyber Crimes, and (2) Private Law includes Insurance, E–Commerce, Domain Name, Cyber Contract, Intellectual Property Right (IPR).

To punish the perpetrators of cybercrime, the House of Representatives together with the President of the Republic of Indonesia issued the Electronic Information and Transaction (EIT) Law Number 11 of 2008 as follows:

Considering:

1. that the process of national development is sustainable and should always be sensitive to the changing dynamics among the populace;
2. that because of the globalization of information, Indonesia is now a part of the information community worldwide; as a result, regulations governing the organization of electronic information and transactions must be made at the national level in order to promote the intellectual development of the populace

and ensure that information technology is developed in an efficient, distributive, and widespread manner across all societal levels;

3. that the extremely quick growth and advancement of information technology has influenced how people live their lives in a variety of ways, which has directly led to the creation of new legal acts;
4. that, in accordance with laws and regulations that serve the interests of the country, information technology use and usage must be continuously developed to promote, preserve, and deepen national union and unity;
5. that in order to attain public wealth, the use of information technology is crucial to national commerce and economic growth;
6. that in order to ensure that information technology usage is carried out securely and prevent its misuse while taking into account the social and cultural values of Indonesian society, the government must support the development of information technology through the infrastructure of law and its regulation;
7. that a law pertaining to electronic information and transactions must be made in light of the consideration as indicated by points a, b, c, d, e, and f.

Furthermore, President of the Republic of Indonesia together with the House of Representatives has decided to enact Electronic Information and Transaction (EIT) Law Number 11 of 2008 as follows:

1. Chap. I : General Provisions
2. Chap. II : Principles and Objectives
3. Chap. III : Electronic Information, Records, and Signatures
4. Chap. IV : Provision of Electronic Certification and Electronic Systems
5. Chap. V : Electronic Transactions
6. Chap. VI : Domain Names, Intellectual Property Rights and Protection of Privacy Rights
7. Chap. VII : Prohibited Acts
8. Chap. VIII : Dispute Resolution
9. Chap. IX : Role of the Government and Role of the Public
10. Chap X : Investigation
11. Chap. XI : Penal Provisions
12. Chap. XII : Transitional Provisions
13. Chap. XIII : Concluding Provisions

There are several article changes on the Law Number 11 of 2008 which are regulated on Law Number 19 of2016.

Considering:

a. that in order to guarantee recognition and respect for the rights and freedoms of others and to fulfill fair demands in accordance with considerations of security and public order in a democratic society, it is necessary to amend Law Number 11 of 2008 concerning Electronic Information and Transactions (EIT) in order to realize justice, public order, and legal certainty;

b. that based on the considerations referred to in letter a, it is necessary to form a Law on the Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions.

Furthermore, President of The Republic of Indonesiawith The House of Representativehas decided to enact Law number 19 of 2016 that consist of two articles. The changes were made to article 1, article 5, article 26, article 27, article 31, article 40, article 43, article 45, article 45A and article 45B.Besides, there are some articles in the Criminal Code of Indonesia that usually used by the law enforcement officer to punish the perpetrators, there are Article 167 of the Indonesia Criminal Code, Article 406 Paragraph (1) of the Indonesia Criminal Code, Article 282 of the Indonesia Criminal Code, Article 378 of the Indonesia Criminal Code, Article 112 of the Indonesia Criminal Code, Article 362 of the Indonesia Criminal Code,Article 311 of the Indonesia Criminal Code, and Article 372 of the Indonesia Criminal Code.

6. Cybercrime Prevention

With the rise of cybercrime cases in Indonesia, there is a need for countermeasures. Penal policy and non-penal policy could be used in the action of cybercrime prevention (Hatta, 2010). Penal policy is the policy that uses criminal sanctions in order to solve the cybercrime cases. According to Bunga (2019) penal policy can be done by three ways and they are, criminalization of behaviours in the law which includes cybercrime, the national legal requirements need to be aligned with international law in countering cybercrime, and enforcing the law with strict criminal sanctions for the perpetrators to create a sense of deterrence (Bunga, 2019:1-15).

Meanwhile, non-penal policy is extrajudicial countermeasures which means, a prevention ways by educating or providing socialization for people to not commit to cybercrime and how to not be the victim of cybercrime. Bunga (2019) stated that create laws other than criminal law which promote efforts to avoid cybercrime by educating or giving some kind of socialization for people such as not to put or share their personal information (full name, address, identity card number, and so on) in the internet and/or other cyberspaces, government should have a collaboration with the private sector to establish a cybersecurity system, and last but not least, considering that cybercrime is a worldwide crime so forming the institutional networks with an international collaboration to prevent cybercrime both national and international level is necessary.

CONCLUSIONS

In the globalized world, technology is developing rapidly. As technology advances, people can do more with just a click. But this also makes it easier for criminals to commit cybercrime. Cybercrime is a type of crime that happens online. It is hard to detect because it has no physical form. There are many types of cybercrime, including hacking, data theft, and online fraud. The Prevention Act has two parts: penal policy and non-penal policy. Penal policy uses criminal sanctions to solve cybercrime cases. It requires strict laws and legal officers who understand technology to prosecute perpetrators. Non-penal policy is an extrajudicial act of prevention. The government can educate people about not sharing personal data online and about not committing crimes online.

REFERENCES

Rosenoer, J. (1997). *CyberLaw: The law of the Internet*. Springer Science & Business Media.

Sirohi, M. N. (2015). *Cyber Terrorism and Information Warfare*. Vij Books India Pvt Ltd.

Sutarman, H., Widiana, I. G., & Amin, I. (2007). *Cyber crime: modus operandi dan penanggulangannya*. LaksBangPressindo.

Bunga, D. (2019). Politik hokum pidana terhadap penanggulangan cybercrime. *Jurnal Legislasi Indonesia*, *16* (1), 1-15.

Handayani, P. (2013). Penegakan hokum terhadap kejahatan teknologi informasi (Cyber Crime). *Jurnal Dimensi*, *2*(2).

Hatta, M. (2010). *Kebijakan politik kriminal: Penegakan hokum dalam rangka penanggulangan kejahatan*. Pustaka Pelajar.

Ismail, D. E. (2009). Cyber Crime di Indonesia. *Jurnal INOVASI*, *6*(3)

Ketaren, E. (2016). Cybercrime, cyber space, dan cyber law. *Jurnal Times*, *5*(2), 35-42.

Leng, J., Sha, W., Wang, B., Zheng, P., Zhuang, C., Liu, Q., ... & Wang, L. (2022). Industry 5.0: Prospect and retrospect. Journal of Manufacturing Systems, 65,279-295.

Menthe, D. C. (1997). *Jurisdiction in cyberspace: A theory of international spaces*. Mich. Telecomm. & Tech. L. Rev., 4, 69.

Putra, Y. A., & Sutabri, T. (2023). Analisis penyadapan pada aplikasi whatsapp dengan menggunakan metode sinkronisasi data. *Blantika: Multidisciplinary Journal*, *2*(1), 11-20.

Wijaya, M. R., & Arifin, R. (2020). Cyber Crime in International Legal Instrument: How Indonesia and International deal with this crime?. *IJCLS (Indonesian Journal of Criminal Law Studies)*, *5*(1), 63-74.

Cloudeka, https://www.cloudeka.id/id/berita/web-sec/contoh-kasus-cyber-crime/, accessed on October 14th 2023

CNBC Indonesia, https://www.cnbcindonesia.com/tech/20230320091926-37-423069/pencuri-uang-online-bertebaran-di-ri-jangan-lakukan-ini, accessed on October 28 2023.

CNN Indonesia, https://www.cnnindonesia.com/nasional/20220328125649-12-776970/jadi-tersangka-dea-onlyfans-dijerat-uu-ite-dan-pornografi, accessed on October 28 2023.

Detik news, https://news.detik.com/berita/d-2023887/ini-dia-kronologi-prita-mencari-keadilan, accessed on October 28 20223

DungaAshola, https://dungaashola.wordpress.com/cybercrime/hacker-dan-cracker/, accessed on October 28 2023.

Forbes, https://www.forbes.com/sites/jeroenkraaijenbrink/2022/05/24/what-is-industry-50-and-how-it-will-radically-change-your-business-strategy/, accessed on November 2nd2023.

Liputan6.com,March 26 2023, https://www.liputan6.com/bisnis/read/5243523/keamanan-siber-indonesia-peringkat-3-terbawah-di-g20-ego-sektoral-kronis-jadi-biang-keladinya?page=2, accessed on October 31, 2023.

Pusiknas Bareskrim Polri, https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat, accessed on October 31, 202