JSH
Jurnal Smart Hukum
https://ejournal.ipinternasional.com/index.php/jsh
Open Access Journal
by Inovasi Pratama Internasional. Ltd
Member of Crossref
ISSN. 2961-841X

Analysis of Cybercrime as a Negative Impact of Technological and Internet Development in Indonesia Based on Law Number 19 of 2016 from a Criminal Law Perspective (Judge's Decision Study No. 569/Pid.sus/2022/PN.Btm)

Albi Ternando[1*)], Dany Dwianggara[1)], Rahman[1)], Rona Indara[1)], Orid Tatiana[1)]

[1)] *Faculty of Law, Universitas Adiwangsa Jambi, Indonesia*
Correspondance Authors: albyternando@gmail.com
DOI: https://doi.org/10.55299/jsh.v4i1.1473
Article history: *Received June 02, 2025: Revised July 10, 2025: Accepted July 30, 2025*

Abstract

The rapid development of information and communication technology has brought significant benefits to society, but on the other hand, it has also given rise to various threats, including cybercrime. In Indonesia, the increase in cybercrime cases, such as skimming, has caused major economic losses and threatened the stability of digital security. This study focuses on the factors causing the increase in cybercrime and efforts to prevent it. The research method used is a normative legal approach through a literature review that studies related laws and regulations, including Law No. 11 of 2008 concerning Information and Electronic Transactions which was updated in 2016. The results of the study indicate that the main causes of cybercrime include weak network security, low digital literacy of the community, and limitations in law enforcement. This study recommends strengthening regulations, increasing human resource capacity, and implementing technology-based prevention policies as solutions to combat cybercrime. This study is expected to be a reference for policy makers and legal practitioners in dealing with cybercrime problems in Indonesia effectively.

Keywords: *Cybercrime, Digital Security, Law Enforcement*

INTRODUCTION

We are now in an era known as the information technology era. This era began with the emergence of a new technology called the computer. Globalization has driven the birth of the information technology era. This phenomenon of rapid information technology development has spread throughout the world. Not only developed countries but also developing countries have spurred the development of information technology in their respective societies, thus ensuring that information technology plays a vital role in the progress of a nation (Marufah, Rahmat, & Widana, 2020).

As global societal needs evolve, information technology plays a crucial role, both now and in the future. It is believed to bring significant benefits and importance to countries worldwide. There are at least two reasons why information technology is considered so crucial in spurring global economic growth. First, information technology drives demand for information technology products, such as computers, modems, internet networking tools, and so on (Hartati, Karyono, & Karno Sabowo, 2022). Second, it facilitates business transactions, especially financial transactions, among other activities (Tri Bagus Prabowo & Rezya Agnesica Sihaloho, 2023).

Information technology has successfully spurred and triggered changes in the social and economic order of society, shifting from conventional transactions and interactions to electronic transactions and socialization, which are considered more effective and efficient. As a result of these developments, information technology has gradually transformed societal behavior and human civilization globally. Furthermore, the development of information technology has made the world borderless and has caused significant social change to occur at a rapid pace.

The development of information technology today has become a double-edged sword. While it contributes to improving human welfare, progress, and civilization, it also serves as an effective means for committing unlawful acts. With the emergence of these unlawful acts, the scope of the law must be expanded to encompass them.

This gave birth to a new legal regime known as cyber law or telematics law. Cyber law is internationally used to refer to laws related to the use of information and communication technology. Similarly, telematics law embodies the convergence of telecommunications law, media law, and informatics law. Other terms used include information technology law, virtual world law, and cyberspace law (Hoffman, 2021).

The development of information technology is very rapid, especially in terms of computer development, where initially computers appeared in the form of mainframe computers in a very large room in the 1950s until the end of the 1970s. Currently, on every desk we often find Personal Computers (PCs), where these PCs are smaller after the development of computers from mainframe computers to personal computers. There are many computer developments from year to year where there are now Laptops or Notebooks that can be carried anywhere according to the needs of the user. Today the size of laptops or notebooks is getting smaller and smaller, even certain brands of cellphones can also function as mini laptops (Tri Bagus Prabowo & Rezya Agnesica Sihaloho, 2023). In its development, computers have given rise to something new in our lives, namely the Internet (Diniyya, Aulia, & Wahyudi, 2021). The Internet has become very important for people throughout the world. Businesspeople, government officials, and many people around the world use the internet as part of their national and international business activities, as well as in their daily personal lives. People are becoming increasingly comfortable with the internet, becoming accustomed to it and becoming uncomfortable when their access is disrupted (Tarisa Auliya Ramadhani, Fajaryanto Cobantoro, & Sugianti, 2024).

It is clear that globalization has two consequences or meanings. On the one hand, it has given birth to a "borderless world," fostering competitive advantages, where cross-continental factors such as technology, education, management, and capital are increasingly playing a role. On the other hand, globalization has generated backlashes such as nationalism and tribal or regional revival movements, as global cultural interactions have a broad cultural impact, resulting in both profit and loss. For developing countries, especially Indonesia, facing globalization, the issue is no longer one of accepting or rejecting its presence, but rather how to utilize it positively to maximize benefits and reduce its negative impact to minimize losses (Lee, Holt, Burruss, & Bossler, 2021). The Indonesian nation cannot escape globalization. This era of globalization is marked by the emergence of a global community with shared universal values. Several issues in this era of globalization exist, such as democratization, human rights, the environment, the use of international standards, and intellectual property rights (Nasrullah, 2022).

Technology itself is neither good nor evil, and blaming it is like blaming an iceberg for sinking the Titanic. Technological advancements and the development of transportation and communication systems, resulting in interdependence between nations, have resulted in the world shrinking, transforming it into a global village. No part of the globe is free from observation and monitoring. We have been, or are being, spoiled by technological products, as we can easily visit other parts of the world and establish global communication, or socialize with others, find new partners, and even learn how to become terrorists, become members of mafia networks, or become part of organized crime (Fadilah, Aranggraeni, & Putri, 2021).

The development of computer, telecommunications, and information technology has driven the growth of internet transactions worldwide. Global companies are increasingly utilizing the internet, such as Shell, Amco, Ford, General Motors, and Sony Corp. Meanwhile, online transactions are growing in various sectors, which has led to the emergence of the term e-banking in financial transactions, and in investment, e-commerce has begun to operate in large numbers (Rawat, AJAGBE, & OKI, 2022). The rapid development in the use of internet services has in fact had a negative impact in the form of criminal acts and violations, which then gave rise to the term Cyber Crime (Nurpadillah, 2021).

The emergence of new crimes as a result of the development of technological currents in the world through globalization is also growing rapidly like the rapid development of technology itself, including data manipulation, espionage, sabotage, provocation, money laundering, hacking, software theft, online fraud and various other types. Even the government does not have sufficient capacity to keep up with these crimes via the internet, making it difficult to control them. With the emergence of several cases of cybercrime in Indonesia, it has become a threat to the stability of national security and order with a fairly high escalation. The government and its apparatus have not been able to keep up with the techniques of crime committed with computer technology, especially on the internet and the internet (internet). Cyber unlawful acts are very difficult to overcome by relying on conventional positive law, because talking about crime cannot be separated from five (5) interrelated factors: the perpetrator of the crime, the victim of the crime, the social reaction to the crime and the law. Law is indeed an important instrument in preventing and overcoming crime. However, creating legal provisions for a legal field that is changing very quickly, such as information technology, is not easy. This is where laws (regulations) often appear to quickly become outdated when they regulate areas undergoing rapid change, creating a situation that appears to be experiencing a legal vacuum. This legal vacuum appears to be occurring in the case of internet crime, or cybercrime (Marufah et al., 2020).

In fact, in the case of cybercrime, there is no legal vacuum. This occurs when interpretative methods recognized in legal science are used, and this is what law enforcement officials should adhere to when dealing with new-dimensional acts that are not specifically regulated by law. The problem becomes different if the political decision to define cybercrime in separate legislation outside the Criminal Code or other special laws. Unfortunately, in this matter of interpretation, judges have not agreed on the categories of certain acts. Therefore, it is crucial to develop judges' understanding of information technology so that the interpretation of forms of cybercrime within the articles of the Criminal Code or other laws is not confusing. To address the above, careful legislative action is clearly needed, keeping in mind one thing: legislation should not be stunned by developments in information technology, resulting in overlegislating regulations, which in turn will have negative impacts, both in other legal fields and in the socio-economic sphere (Pambudi, Budiman, Rahayu, Sukanto, & Hendrayani, 2023) .

Before the enactment of Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), there were two opinions regarding the need for a law regulating cybercrime, including:

First, there's the group that argues that, to date, there's no legislation governing cybercrime, making it extremely difficult for law enforcement to prosecute perpetrators if cybercrime occurs. This argument is reinforced by the large number of cybercrime cases that our judicial system has failed to resolve. The problem stems from the difficulty in finding articles that can be used as the basis for prosecution in court.

Second, there are those who believe there is no legal vacuum. They believe that, even though there is no specific law regulating cybercrime, law enforcement can utilize existing laws. Implementing this requires the courage of judges to explore existing laws by creating legal provisions (jurisprudence) as the basis for court decisions (Anugrah, 1 ✉, & Sidi, 2024).

However, in April 2008, the government passed Law Number 11 of 2008 concerning Electronic Information and Transactions. This law regulates the criminalization of several criminal acts that were previously not criminal through several breakthroughs and expansions in terms of principles and criminal sanctions. In addition, this law also regulates procedures and evidence that have been expanded, namely the inclusion of new evidence related to electronic media. Law Number 11 of 2008 concerning Electronic Information and Transactions is reviewed from the perspective of criminal policy, generally in terms of the formulation of criminal acts, the formulation of criminal sanctions, and the procedures or mechanisms of the criminal justice system. Reviewing the issue of criminalization policy in this law is the most strategic stage in the overall planning process of the functionalization of criminal law or the process of criminal law enforcement in combating cybercrime.

One example of a case that occurred in Batam in 2022, a Foreign Citizen (WNA) with the initials VT (the perpetrator) together with three other people (initials AG, JP, AND CC) installed a skimming device on a Bank Riau Kepri ATM machine by committing a crime intentionally and without rights or against the law by accessing computers and/or electronic systems belonging to other people in any way with the aim of obtaining Electronic Information and/or Electronic Documents which resulted in losses for other people (Zuhdi & Mulawarman, 2021).

VT was assisted by JP and CC using an ATM whose data used data from skimming. VT began to make transactions/withdrawals of money belonging to Bank Riau Kepri customers, they made withdrawals and transfers of money for approximately 78 (seventy-eight) customers who had been taken/moved/withdrawn/sent by VT in the amount of approximately Rp. 1,121,450,000 (one billion one hundred twenty-one million four hundred and fifty thousand rupiah), with the money from VT's actions, VT immediately sent it to the Permata Bank account and the Cryptocurrency account managed by AG, and from the results of his actions, VT received a portion of AG that was still left after being used to meet daily needs of approximately Rp. 211,000,000 (two hundred and eleven million rupiah), 1000 euros in euro money, so that the total loss experienced by Bank Riau Kepri was approximately Rp. 1,121,450,000 (one billion one hundred twenty-one million four hundred and fifty thousand rupiah).

Because it fulfills all the elements of a crime, VT has been legally and convincingly proven guilty of committing the crime of "Without the Right to Access Electronic Systems Belonging to Other People in Any Way with the Aim of Obtaining Electronic Information and Electronic Documents that Cause Losses to Other People" and was sentenced to 7 (seven) years in prison and a fine of Rp. 5,000,000,000 (five billion rupiah) with the provision that if the fine is not paid it will be replaced with 6 (six) months in prison.

RESEARCH METHODS

1. Research Specifications

The approach used in this research is normative juridical research. Using Ronald Dworkin's term, this type of research is also called doctrinal research, which analyzes laws, both those written in books and those decided by judges through court proceedings (Rai, Heryadi, & Kamaluddin, 2022). This research utilizes literature and document studies as the primary sources.

2. Research Data Sources

The main data in this research are:

a. Primary data, namely laws and regulations regarding criminal liability committed by children, including Law Number 11 of 2012 concerning the Juvenile Justice System, Law 35 of 2014 concerning Child Protection and other laws and regulations relating to criminal liability committed by children.

b. Secondary data, namely materials that provide explanations regarding primary law, such as research results, the work of legal experts and other documents related to criminal responsibility for children.
c. Tertiary data, namely supporting legal materials that provide guidance and explanations for primary legal materials and secondary legal materials such as general dictionaries, legal dictionaries, magazines/journals or newspapers as long as they contain information relevant to this research (Rai et al., 2022).

3. Data Collection Techniques

In connection with the problems in this research, data collection will be carried out through literature studies, collected through literature studies, namely by studying the provisions of legislation regarding criminal liability committed by children and other laws and regulations relevant to the research material (PADILA, 2020).

4. Data Analysis

After all data was obtained through library research, it was examined to determine its validity. Then, the data was grouped into similar data. Qualitative data was interpreted legally, logically, and systematically using the inductive method.

The inductive method means drawing from developing generalizations and looking at regulations that apply generally, even though they are not absolutely certain, but are used as a legal basis in applying criminal responsibility to children (Setiantoro, Putri, Novitarani, & Njatrijani, 2018).

By using the inductive method, we will obtain a consensus on how criminal responsibility for children actually occurs. The results of this discussion and analysis are expected to yield conclusions that provide answers to the research questions.

RESULTS AND DISCUSSION

A. Factors Causing the Development of Cybercrime

The advancement of information technology can be marked by the increasing use of the internet, the increasing use of the internet can have a positive impact but the negative impacts due to technological advances are numerous and often become criminal. According to Didik M. Arief Mansur and Elisatris Gultom, cyber crime was born due to the lack of ability or knowledge of law enforcement officers in handling cyber cases (Wibawa, 2020).

Information technology and its initiating operators are closely linked; the two cannot be separated. Human resources in information technology play a crucial role in controlling a tool. Will the tool be used as a means of benevolence to achieve human welfare, or will it be criminalized and thus undermine the interests of the state and society? Technology, as a result of human discovery and development, is then utilized for the betterment of humanity, but on the other hand, it can bring disaster to humanity due to deviations. In Indonesia, the resources for managing information technology are sufficient, but the human resources to produce or create this technology are still lacking. The causes are various, including a lack of research personnel and insufficient research funding, or perhaps a lack of attention and appreciation for research. Consequently, human resources in Indonesia are mostly users, and their numbers are quite large.

With the advent of technology as a means to achieve goals, including the internet as a means of communication, a new cyber community has emerged sociologically: a community of internet addicts who communicate with each other and exchange ideas based on the principles of freedom and balance among these addicts or cyber maniacs. This community represents a new social phenomenon and is highly strategic to consider, as it offers numerous lessons to be learned. From ignorance to knowledge, those who know become increasingly intelligent, while those who are intelligent become increasingly

sophisticated. Technological developments and the pace of societal development are quickly and accurately known, allowing them to exchange ideas and cross-check with each other.

Unlimited internet access. Nowadays, the internet is no longer a rare thing, as everyone uses it. Using the internet provides us with the convenience of unlimited access to anything. This convenience is a major factor in some individuals' ease of committing cybercrime. Computer user negligence is one of the main causes of computer crime. As we know, people who use the internet always enter all their important data online. This makes it easier for some individuals to commit crimes.

It's easy to do, with minimal security risks and no need for sophisticated equipment. This is a driving factor in cybercrime. Like us, the internet is a tool we can easily use without the need for specialized equipment. However, the primary driver of internet crime is the difficulty of tracking down those who abuse its capabilities (ESTER, 2022).

The perpetrators are generally intelligent, inquisitive, and passionate about computer technology. This is a difficult factor to avoid, as the advantages or intelligence possessed by individuals accessing the internet in this day and age are often misused for profit. Therefore, it's difficult to avoid.

Weak network security systems. As we know, most internet users prioritize design, neglecting security. This weak network security system creates a significant loophole for certain individuals to commit crimes.

Lack of public awareness: The public and law enforcement currently still place a significant emphasis on conventional crime. In reality, computer criminals continue to commit crimes. This is due to a lack of public awareness of deeper internet usage.

As technology advances and cybercrime evolves, it evolves into various new types of crimes with new modus operandi. Cybercrime continues to evolve, from the more commonly known, such as hacking, cracking, and carding, to more specific ones, such as: probes (attempts to gain access to a system); scans (large-scale probes); account compromise (illegal account use); root compromise (account compromise with privileges for the intruder); denial of service (DoS) (causing the network to malfunction due to traffic overload); domain name misuse, and others. Technological developments have significantly contributed to improving human welfare, progress, and civilization, but they also have unavoidable negative impacts, such as the theft of bank customer funds through ATM card duplication, better known as skimming (Putra, 2022) .

Skimming is one of the many types of cybercrime. Both on a small scale and on a global scale, the victim's account is typically controlled by the magnetic stripe system on an ATM card, without legal or official authorization. This system should only be controlled by the authorized bank. Cybercriminals possess considerable technological expertise, making this type of crime extremely difficult to eradicate completely because they are difficult to track.

As a result of technological advancements, almost everyone now has an electronic transaction card, from rural to urban residents. Surveys show that most people's wallets contain a plastic card called an ATM (Automated Teller Machine). It's surprising to see the increasing number of ATM hacks, often targeting customers of leading banks, resulting in significant losses totaling billions.

ATM machine hacking using skimming technique is one of the types of crime that carries out its actions, namely damaging the system, by spreading the system, by transferring data using the system, and illegally deleting data regarding the data owned by the victim sent to an ATM owned by the perpetrator who has been planned in advance, then the data and money in the victim's ATM will act to the perpetrator's account. This shows that the perpetrator already has a fairly high level of technological knowledge that is used to commit a crime.

Skimming is a crime that occurs through computers or computer LAN networks and is a serious threat today. By properly utilizing this technology, which is based on computer systems or a means of communication in this global era, we can be seen virtually, making us the victims (Oktaviani, Hermawan, & Utami, 2024).

ATM thefts are often caused by the negligence of the cardholder. In ATM skimming, the victim is unknowingly videotaped while entering their PIN, and the magnetic strip is also recorded using a

special device. This type of theft, which uses skimming as a method, causes significant losses to many parties, even to the point of the government spending state funds. In other words, the effects we experience from the collapse and destruction of a bank are not limited to that institution; many other parties are affected, and other banks experience similar effects related to the financial and payment systems.

Skimming is the act of stealing credit or debit card information by illegally copying the information contained on the card's magnetic strip, where this strip is a wide black line on the back of the debit card, which functions more or less like a cassette tape or ferromagnetic material that can be used to store customer data.

The process of duplicating customer data to a new debit card can also be done using more sophisticated techniques, where the creation of this fake debit card can be done in three ways, namely:

1. The altered card method is carried out by using an original electronic card whose data has been changed. This method is carried out by heating the relief on the electronic card (re-embossed) and then filling it with the customer's personal data (re-encoded).
2. The total counterfeit method, which is the creation of an electronic card that is completely fake, and this method requires the perpetrator to print a card that is similar to the original electronic card by including images, logos, and numbers so that it looks like the original electronic card, the creation of which involves an embossing and encoding process.
3. The white plastic card method is the creation of electronic cards using plain white plastic cards, where this method only involves the encoding process because the fake card is only made by involving data without falsifying the physical card.

One example of a case that occurred in Batam in 2022, a Foreign Citizen (WNA) with the initials VT (the perpetrator) together with three other people (initials AG, JP, AND CC) installed a skimming device on a Bank Riau Kepri ATM machine by committing a crime intentionally and without rights or against the law by accessing computers and/or electronic systems belonging to other people in any way with the aim of obtaining Electronic Information and/or Electronic Documents that result in losses for other people (Kirana, Abbas, & Rustan, 2021).

Starting from VT arriving in Batam City in October 2021, previously meeting with AG they were fellow Bulgarian citizens living in Bali, then VT wanted to borrow money from AG because VT wanted to live in Indonesia. AG only wanted to lend money to VT if VT was willing to do skimming work. The definition of skimming is placing a tool in an ATM machine for the purpose of obtaining data from an ATM card in the form of a PIN code and banking data on the ATM itself, then VT learned to skimming from AG just a few days after that the defendant went to Batam City and at that time had been given banking data by AG through sendspace.com to then the banking data was entered into a blank card which the defendant would later use to withdraw money at an ATM in Batam City, in addition, AG has also sent the tools that VT will use to do the skimming to CC's home address in Royal Grande Batam City.

VT asked CC to create a savings account and make an ATM which was then used by VT to try by covering the chip section using tape whether it could still enter and be read by the ATM machine, and if it could eat the ATM machine would be installed with a skimming machine. Then AG told VT to cook a skimming device using a hidden camera on the number cover on the ATM machine which functions to record the ATM PIN pressed by the Customers who use the ATM card on the ATM machine, then the skimming insert device or commonly called a black machine copies the data, or with the term iron metal, the skimming devices were then installed by VT at the ATM belonging to Bank Riau Kepri accompanied by CC and JP installing the skimming device. Installing the skimming device, VT wore dark clothes with the help of JP, namely covering it with his body so as not to be seen by CCTV and people around the ATM room. After installing the skimming device, they then left the ATM location where the device had been installed.

After several days, VT returned to the ATM that had installed the skimming device and then in the ATM, approximately 100 (one hundred) customer data had been installed, then VT sent the data

to AG via sendspace.com which would later be processed by AG, after the data was processed, the data was sent back by AG to VT to be input into the magnetic stripes card using an EDC (Electronic Data Capture) machine along with its software, namely MSRX6 to read and write the data that VT would input and upload to the magnetic stripes card that VT used, namely the Alfamart card and then with the card it became an ATM card that could be used to make transactions/withdraw money;

VT was assisted by JP and CC using an ATM whose data used data from skimming. VT began to make transactions/withdrawals of money belonging to Bank Riau Kepri customers, they made withdrawals and transfers of money for approximately 78 (seventy-eight) customers who had been taken/moved/withdrawn/sent by VT in the amount of approximately Rp. 1,121,450,000 (one billion one hundred twenty-one million four hundred and fifty thousand rupiah), with the money from VT's actions, VT immediately sent it to the Permata Bank account and the Cryptocurrency account managed by AG, and from the results of his actions, VT received a portion of AG that was still left after being used to meet daily needs of approximately Rp. 211,000,000 (two hundred and eleven million rupiah), 1000 euros in euro money, so that the total loss experienced by Bank Riau Kepri was approximately Rp. 1,121,450,000 (one billion one hundred twenty-one million four hundred and fifty thousand rupiah).

Because it fulfills all the elements of a criminal act, VT has been legally and convincingly proven guilty of committing the crime of "Without the Right to Access Electronic Systems Belonging to Others in Any Way with the Aim of Obtaining Electronic Information and Electronic Documents that Cause Losses to Others" and was sentenced to imprisonment for 7 (seven) years and a fine of IDR 5,000,000,000 (five billion rupiah) with the provision that if the fine is not paid it will be replaced with imprisonment for 6 (six) months (Ni Luh Gede Yogi Arthani, 2021).

The application of the article to the perpetrator of the crime of skimming, namely that it can be imposed in Article 30 paragraph (2) of the ITE Law states that, "Any person who intentionally and without rights or criminal acts accesses a computer and/or digital structure in any way with the aim of obtaining Electronic Information and/or Electronic Documents. This method is that every act can be punished if it has fulfilled the criminal elements contained in the accused article, namely:

1. Details of the intentional error
2. Unlawful elements, especially without rights or against the law
3. Action elements access by any means
4. Elements of objects, namely computers and/or electronic systems
5. The motive is to obtain electronic information and/or electronic documents.

As for criminal responsibility, it is the foundation of the broad understanding of error. There are three conditions regarding criminal responsibility, namely as follows:

a. The possibility of determining one's will regarding an action
b. Know the true meaning of the action
c. Awareness that it is prohibited in society.

The definition of error has a sign as something reprehensible (verwijtbaarheid) which in essence does not prevent (vermijdbaarheid) unlawful behavior (der wederrechtelijke gedraging). The essence of not preventing unlawful behavior (vermijdbaarheid der wederrechtelijke gedraging) in the formulation of positive law, there means having intent and negligence that leads to unlawful nature (wederrechtelijkheid) and the ability to be responsible (toerekenbaarheid).

Negligence is the mental attitude of a person who creates a prohibited situation, the perpetrator does not oppose the prohibition, the perpetrator does not want it, where in practice there are various formulations of negligence as a condition for a crime, namely:

1) No guesswork, which is required by law.
2) Not Avoiding Prohibitions
3) Lack of caution
4) Taking little or no precautions
5) Negligent, carrying out actions that result in prohibited things

Reasons for expungement of criminal offenses can be divided into two, namely reasons for expungement of criminal offenses which are forgiving reasons and secondly reasons for expungement of criminal offenses which are justification reasons. Reasons for expungement of criminal offenses which are forgiving reasons are reasons that eliminate the mistakes made by the perpetrator or defendant, because these reasons concern the perpetrator's mistakes, then these reasons for expungement of criminal offenses only apply to the perpetrator or defendant personally. Reasons for justification are reasons that eliminate the unlawful nature of their actions, because these reasons for expungement of criminal offenses concern actions, then these reasons apply to all people who commit these actions.

B. Efforts to Combat Cybercrime

Indonesia in making laws in the field of cybercrime apparently uses the 'umbrella provision' model so that the provisions of cybercrime are not in separate legislation, but are regulated generally in Law No. 11 of 2008 concerning Electronic Information and Transactions which has been amended by Law No. 19 of 2016 (Aritonang, Lasmana, & Kurnia, 2019).

Efforts to combat cybercrime crimes in Law Number 11 of 2008 concerning Information and Electronic Technology as amended by Law No. 19 of 2016 are contained in Chapter VII entitled "Prohibited Acts", regulated from Article 27 to Article 37. Chapter VII of Law Number 11 of 2008 concerning Information and Electronic Technology as amended by Law No. 19 of 2016 essentially contains the formulation of criminal acts as contained in the Council of Europe Cyber Crime Convention, hereinafter referred to as the Cyber Crime Convention (CC) which was signed in Budapest on November 23, 2001, namely:

Article 27:

(1) Any person who intentionally and without authority distributes and/or transmits and/or makes accessible electronic information and/or electronic documents that contain content that violates morality.
(2) Any person who intentionally and without authority distributes and/or transmits and/or makes accessible electronic information and/or electronic documents containing gambling content.
(3) Any person who intentionally and without authority distributes and/or transmits and/or makes accessible electronic information and/or electronic documents that contain insulting and/or defamatory content.
(4) Any person who intentionally and without authority distributes and/or transmits and/or makes accessible electronic information and/or electronic documents containing blackmail and/or threats.

Regarding Article 27 paragraph (3) of Law No. 11 of 2008, Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 states that:

1. To avoid multiple interpretations of the provisions prohibiting the distribution, transmission and/or making accessible of Electronic Information containing insults and/or defamation, the following 3 (three) changes have been made:
   d. Adding an explanation of the term 'distributing, transmitting and/or making accessible Electronic Information'
   e. Confirming that the provision is a complaint offense, not a general offense
   f. Emphasizing that the criminal elements in the provisions refer to the provisions on defamation and slander as regulated in the Criminal Code.
2. Reducing the criminal threat for insults and/or defamation from a maximum of 6 (six) years' imprisonment to 4 (four) years and/or a fine from a maximum of IDR 1 billion to a maximum of IDR 750 million.

Regarding paragraph (4), it is stated in Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning ITE that 'the criminal threat for sending electronic information containing

threats of violence or intimidation is a maximum prison sentence of 12 (twelve) years to a maximum of 4 (four) years and/or a maximum fine of IDR 2 billion to a maximum of IDR 750 million.

Article 28:

(1) Any person who intentionally and without authority spreads false and misleading news that results in consumer losses in electronic transactions.
(2) Any person who intentionally and without right disseminates information aimed at causing hatred or hostility towards individuals and/or certain community groups based on ethnicity, religion, race and inter-group relations (SARA).

Article 29:

"Any person who intentionally and without authority sends electronic information and/or electronic documents containing threats of violence or intimidation directed at a person"

Article 30:

(1) Any person who intentionally and without authority or against the law accesses another person's computer and/or electronic system in any way.
(2) Any person who intentionally and without authority or against the law accesses a computer and/or electronic system in any way with the aim of obtaining electronic information and/or electronic documents.
(3) Any person who intentionally and without authority or against the law accesses a computer and/or electronic system in any way by violating, breaking through, exceeding or breaking through the security system.

Article 31:

(1) Any person who intentionally and without authority or against the law carries out interception or tapping of electronic information and/or electronic documents in a computer and/or certain electronic system belonging to another person.
(2) Any person who intentionally and without authority or against the law intercepts the transmission of electronic information and/or documents that are not public from, to, and within a particular computer and/or electronic system belonging to another person, whether this does not cause any changes or causes changes, removal, and/or termination of electronic information and/or electronic documents that are being transmitted.

Article 32:

(1) Any person who intentionally and without authority or against the law in any way changes, adds, reduces, transmits, damages, removes, moves, hides electronic information and/or electronic documents belonging to another person or the public.
(2) Any person who intentionally and without authority or against the law in any way moves or transfers electronic information and/or electronic documents to the electronic system of another person who is not authorized.

Article 33:

"Any person who intentionally and without authority or against the law carries out any action that results in disruption of the electronic system and/or causes the electronic system to not work as it should."

Article 34:

“Any person who intentionally and without rights or against the law produces, sells, procures for use, imports, distributes, provides, or owns:

a) computer hardware or software designed or specifically developed to facilitate acts as referred to in Articles 27 to 33;
b) computer passwords, access codes, or similar things that are intended to enable electronic systems to be accessed with the aim of facilitating acts as referred to in Articles 27 to 33.

Article 35:

"Any person who intentionally and without authority or against the law manipulates, creates, changes, removes, destroys electronic information and/or electronic documents with the aim of making the electronic information and/or electronic documents appear to be authentic data."

Article 36:

"Any person who intentionally and without rights or against the law carries out an act as referred to in Articles 27 to 34 which results in loss to another person."

Article 37:

"Any person who intentionally carries out prohibited acts as referred to in Articles 27 to 36 outside the territory of Indonesia against electronic systems located within the jurisdiction of Indonesia."

The criminal acts as mentioned above (Article 27 to Article 37) are punishable by imprisonment (maximum ranging from 6 (six) years to 12 (twelve) years) and/or a fine (maximum ranging from Rp. 600,000,000.00 (six hundred million rupiah) to Rp. 12,000,000,000.00 (twelve billion rupiah).

In addition, the prison sentence can be increased by one third of the main sentence if:

a. criminal acts as referred to in Article 27 paragraph (1) concerning morality or sexual exploitation of children;
b. the criminal acts mentioned in Articles 30 to 37 are directed against computers and/or electronic systems as well as electronic information and/or electronic documents which belong to the government and/or are used for public interest;
c. The criminal acts mentioned in Articles 30 to 37 are directed against computers and/or electronic systems and electronic information belonging to the government and/or strategic bodies, including but not limited to defense institutions, central banks, banking, finance, international institutions and aviation authorities.
d. the crimes mentioned in Articles 27 to 37 are committed by corporations.

Articles concerning criminal provisions are regulated in Articles 45 to 52. From the provisions contained in Law No. 11 of 2008 concerning Information and Information Technology, which has been amended by Law No. 19 of 2016, it can be seen that the scope that has been put forward is not much different from what has been regulated in legislation in other countries.

Currently, the regulation used as the legal basis for cybercrime cases is Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE). The existence of this ITE Law is expected to protect the public who use information technology in Indonesia, this is important considering the number of internet technology users is increasing from year to year. The increasing use of the internet on the one hand provides many conveniences for humans in carrying out their activities, on the other hand makes it easier for certain parties to commit criminal acts, this technological advancement also affects people's lifestyles and mindsets, in fact, currently many crimes occur using information technology. The phenomenon of cybercrime which is growing rapidly and does not recognize territorial boundaries must be watched out for because this crime is somewhat different from other crimes in general (Dhillon, Herman, & Syafryadin, 2020).

The use of Information Technology plays an important role in trade and national economic growth to realize public welfare, that the government needs to support the development of Information Technology through legal infrastructure and its regulations so that the use of Information Technology is carried out safely to prevent its misuse by paying attention to the religious and socio-cultural values of Indonesian society. In the provisions of Article 4 paragraph (2) of the ITE Law it is stated that the Government protects the public interest from all types of disturbances as a result of the misuse of Electronic Information and Electronic Transactions that disrupt public order, in accordance with the provisions of the Laws and Regulations.

Responding to the demands and challenges of global communication via the Internet, the Law is expected to be able to answer all legal issues related to global technological developments and be anticipatory towards all existing problems, including the negative impacts of internet misuse which will ultimately cause losses for its users (Ismanto, Gunarto, & Wahyuningsih, 2021).

Maintaining and protecting technology users requires cooperation and commitment from all parties, given that information technology, especially the internet, has become a tool for building an information-based society. The existence of laws governing cybercrime is expected to protect and provide a sense of security for those who use technology as a platform for conducting transactions and conducting economic activities (Koto, 2021). Taking action against those who abuse technological developments requires qualified human resources with the ability and expertise in the technology field (Dudin, Zasko, Frolova, Pavlova, & Rusakova, 2018) . Law enforcement is influenced by at least several factors, namely the legal regulations themselves or laws, the implementing apparatus of these regulations, namely law enforcement officers, and the legal culture itself, namely the community itself, which is the target of the law.

CONCLUSION

1. The development of cybercrime in Indonesia is influenced by several key factors, including rapid advances in information technology, weak network security systems, and the limited capabilities of law enforcement officials in handling cybercrime cases. Other factors include a lack of public understanding of the dangers of cybercrime and the misuse of technological capabilities by certain individuals for personal gain, which is often difficult to detect. Furthermore, easy, unlimited internet access has opened up greater opportunities for certain individuals to commit cybercrime.
2. Efforts to combat cybercrime by means of penalties, namely in addition to being regulated in articles in the Criminal Code such as Article 362 concerning Theft, Article 378 concerning Fraud and Article 263 concerning Identity Forgery with the threat of existing penalties, also by implementing Law No. 11 of 2008 which was amended by Law No. 19 of 2016 concerning ITE, especially in Articles 27 to 37 concerning Prohibited Acts and in Articles 45 to 52 concerning the threat of imprisonment by imposing the threat of a maximum prison sentence of 12 (twelve) years and a maximum fine of Rp. 2,000,000,000.00 (two billion rupiah).

Suggestion

3. To reduce the development of cybercrime, it is recommended that the government and relevant institutions improve the quality of human resources in the field of cybersecurity, both for law enforcement and the general public. Training and education on information technology and cybersecurity need to be encouraged to raise awareness and skills in preventing and mitigating cyber threats. Furthermore, improvements to network security systems and revisions to cybercrime laws are also needed to keep pace with rapid technological developments.
4. Cybercrime must be punished with severe penalties and large fines. The threat of a cumulative penalty, consisting of imprisonment and a fine, must be imposed to deter perpetrators from repeating their crimes. Furthermore, the government needs to further develop and improve the human resources and technology of a dedicated cybercrime team to track down perpetrators of cybercrime so that they no longer have the freedom to commit their crimes.

REFERENCES

Anugrah, K., 1✉, P., & Sidi, R. (2024). Penegakan Hukum Terhadap Remaja Sebagai Pelaku Tindak Pidana Perundungan Media Sosial Di Dunia Siber. *Innovative: Journal Of Social Science Research*, *4*, 801–811.

Aritonang, I. R., Lasmana, S., & Kurnia, D. (2019). The Analysis Of Skimming And Scanning Technique To Improve Students In Teaching Reading Comprehension. *Project (Professional Journal Of English Education)*, *1*(2), 101. Https://Doi.Org/10.22460/Project.V1i2.P101-106

Dhillon, B. P. S., Herman, H., & Syafryadin, S. (2020). The Effect Of Skimming Method To Improve Students' Ability In Reading Comprehension On Narrative Text. *Linguists : Journal Of Linguistics And Language Teaching*, *6*(1), 77. Https://Doi.Org/10.29300/Ling.V6i1.2991

Diniyya, A. A., Aulia, M., & Wahyudi, R. (2021). Financial Technology Regulation In Malaysia And Indonesia: A Comparative Study. *Ihtifaz: Journal Of Islamic Economics, Finance, And Banking*, *3*(2), 67. Https://Doi.Org/10.12928/Ijiefb.V3i2.2703

Dudin, M. N., Zasko, V. N., Frolova, E. E., Pavlova, N. G., & Rusakova, E. P. (2018). Mitigation Of Cyber Risks In The Field Of Electronic Payments: Organizational And Legal Measures. *Journal Of Advanced Research In Law And Economics*, *9*(1 (31)), 78–88.

Ester, E. L. I. (2022). *Perlindungan Hukum Bagi Investor Asing Dari Kerugian Non Komersial Di Indonesia*. Https://Doi.Org/Http://Digilib.Unila.Ac.Id/Id/Eprint/63646

Fadilah, A., Aranggraeni, R., & Putri, S. R. (2021). Eksistensi Keamanan Siber Terhadap Tindakan Cyberstalking Dalam Sistem Pertanggungjawaban Pidana Cybercrime. *Syntax Literate: Jurnal Ilmiah Indonesia*, *6*(4), 1555.

Hartati, S., Karyono, H., & Karno Sabowo, H. (2022). Implementation Of The Law On Information And Electronic Transactions And Pancasila Law Enforcement Related To Cybercrimes In Indonesia. *International Journal Of Educational Research & Social Sciences*, *3*(1), 425–436. Https://Doi.Org/10.51601/Ijersc.V3i1.290

Hoffman, P. (2021). Countering The Corrupt: The What, Who, Where, Why And How-To Of Countering Corruption. In *Countering The Corrupt: The What, Who, Where, Why And How-To Of Countering Corruption: Hoffman, Paul*. Cape Town, South Africa: Siber Ink.

Ismanto, H., Gunarto, G., & Wahyuningsih, S. E. (2021). The Juridical Formulation Of Hate Speech Cyber Crime And Its Law Enforcement Implementation. *Law Development Journal*, *3*(4), 710–718.

Kirana, A. R. A., Abbas, I., & Rustan, M. (2021). Analisis Perlindungan Hukum Terhadap Konsumen Terkait Penjualan Barang Bermerek Palsu Melalui Transaksi Online Ditinjau Berdasarkan Hukum Perdata. *Qawanin Jurnal Ilmu Hukum*, *2*(1).

Koto, I. (2021). Cyber Crime According To The Ite Law. *International Journal Reglement & Society (Ijrs*, *2*(2), 103–110. Https://Doi.Org/10.55357/Ijrs.V2i2.124

Lee, J. R., Holt, T. J., Burruss, G. W., & Bossler, A. M. (2021). Examining English And Welsh Detectives' Views Of Online Crime. *International Criminal Justice Review*, *31*(1), 20–39. Https://Doi.Org/10.1177/1057567719846224

Marufah, N., Rahmat, H. K., & Widana, I. D. K. K. (2020). Degradasi Moral Sebagai Dampak Kejahatan Siber Pada Generasi Millenial Di Indonesia. *Nusantara: Jurnal Ilmu Pengetahuan Sosial*, *7*(1), 191–201. Https://Doi.Org/Http://Dx.Doi.Org/10.31604/Jips.V7i1.2020.191-201

Nasrullah, R. (2022). *Teori Dan Riset Media Siber (Cybermedia)*. Prenada Media.

Ni Luh Gede Yogi Arthani, K. A. S. (2021). Jauan Kriminologi Terhadap Kejahatan Skimming Melalui Atm Di Polda Bali. *Jurnal Hukum Mahasiswa*, *1*(1), 109–128. Https://Doi.Org/10.36733/Jhm.V1i1.2581

Nurpadillah, V. (2021). *Kontribus Sastra Siber Terhadap Pembelajaran Menulis Teks Sastra Bagi Mahasiswa Prodi Tadris Bahasa Indonesia*.

Oktaviani, N. I., Hermawan, R. P., & Utami, C. R. (2024). Tinjauan Hukum Terhadap Perlindungan Konsumen Dalam Layanan Shopee Pay Later. *Jurnal Ilmiah Penelitian Mahasiswa*, *2*(6), 1–10.

Https://Doi.Org/Https://Doi.Org/10.61722/Jipm.V2i6.481

Padila, R. (2020). *Perlindungan Hukum Bagi Konsumen Terhadap Pembatalan Transaksi Oleh Aplikasi Belanja Online Dalam Perspektif Hukum Islam Dan*.

Pambudi, R., Budiman, A., Rahayu, A. W., Sukanto, A. N. R., & Hendrayani, Y. (2023). Dampak Etika Siber Jejaring Sosial Pada Pembentukan Karakter Pada Generasi Z. *Jurnal Syntax Imperatif: Jurnal Ilmu Sosial Dan Pendidikan*, *4*(3), 289–300.

Putra, E. A. (2022). *Analisis Yuridis Perlindungan Hukum Terhadap Penanaman Modal Asing Di Provinsi Riau*. Universitas Islam Riau. Https://Doi.Org/Http://Repository.Uir.Ac.Id/Id/Eprint/16736

Rai, I. N. A. S., Heryadi, D., & Kamaluddin, A. (2022). The Role Of Indonesia To Create Security And Resilience In Cyber Spaces [Peran Indonesia Dalam Membentuk Keamanan Dan Ketahanan Di Ruang Siber]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *13*(1), 43–66.

Rawat, R., Ajagbe, S. A., & Oki, O. A. (2022, Mei 24). *Techniques For Predicting Dark Web Events Focused On The Delivery Of Illicit Products And Ordered Crime*. Https://Doi.Org/10.21203/Rs.3.Rs-1665267/V1

Setiantoro, A., Putri, F. D., Novitarani, A., & Njatrijani, R. (2018). Urgensi Perlindungan Hukum Konsumen Dan Penyelesaian Sengketa E-Commerce Di Era Masyarakat Ekonomi Asean. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, *7*(1), 1–17.

Tarisa Auliya Ramadhani, Fajaryanto Cobantoro, A., & Sugianti, S. (2024). Implementasi Algoritma Advanced Encryption Standard 128 Untuk Pengamanan Database Sistem Registrasi Pasien. *Jurnal Informatika Polinema*, *10*(4), 521–526. Https://Doi.Org/10.33795/Jip.V10i4.5619

Tri Bagus Prabowo, & Rezya Agnesica Sihaloho. (2023). Analisis Ketergantungan Indonesia Pada Teknologi Asing Dalam Sektor Energi Dan Dampaknya Pada Keamanan Nasional. *Jurnal Lemhannas Ri*, *11*(1), 72–82. Https://Doi.Org/10.55960/Jlri.V11i1.426

Wibawa, D. (2020). *Jurnalisme Warga Perlindungan, Pertanggungjawaban Etika Dan Hukum*. Cv. Mimbar Pustaka. Opgehaal Van Https://Etheses.Uinsgd.Ac.Id/Id/Eprint/33206

Zuhdi, N. M., & Mulawarman, M. (2021). Pengaruh Perundungan Siber Di Media Sosial Dan Bystander Terhadap Regulasi Emosi Remaja Se-Kabupaten Pemalang. *Jurnal Al-Taujih : Bingkai Bimbingan Dan Konseling Islami*, *7*(2), 118–127. Https://Doi.Org/10.15548/Atj.V7i2.3121