EISSN: 2622-9668 | PISSN: 2622-982X
Volume 17 Nomor 1 February 2024: 62-74
DOI: 10.30996/mk.v17i1.10174

MIMBAR KEADILAN

Fair Legal Measures: Addressing Cybercrime Through a Juridical Lens in Cases of Online Fraud

Ollifia Az Zahra Ainur Islamy[1*], Taufiq Nugroho [2]
[1]Universitas Muhammadiyah Surakarta, Indonesia
[2]Universitas Muhammadiyah Surakarta, Indonesia
*Corresponding Author: C100200029@student.ums.ac.id

Article History:
Submitted:
06-01-2024
Received:
02-02-2024
Accepted:
17-02-2024

Keywords:
Cybercrime; Fraud; Online

Abstract

The widespread misuse of information technology is deeply concerning to society due to the prevalence of cybercrime. Cybercrime is a violation of the law by using social networks or the internet as a means of crime, obtaining data illegally, taking advantage and enriching oneself. Online selling business is one of several possibilities for online fraud. This research examines decision number 177/Pid.Sus/2021/PN Smn, specifically focusing on the application of Article 45A paragraph (1) in conjunction with Article 28 paragraph 1 of Law No. 19/2016. This study aims to determine the judge's consideration based on the above decision and the application of sanctions in accordance or not with the relevant article. The source is secondary data using research that is basically doctrinal or normative, case and legislative approaches. The defendant, Juari alias Johan Bin Djun Hie, has been legally found to meet the requirements outlined in the mentioned article of the decision. The panel of judges considered the facts presented, the prosecutor's indictment, the defendant's statement, the testimony of witnesses, and the submitted evidence when deciding on the case. The application of the witnesses is in accordance with the Article mentioned. The Defendant is subject to a maximum prison sentence of 6 years and/or a maximum fine of Rp. 1,000,000,000.00. The legal system must adapt to technological advancements to maintain its efficacy in enforcing the law. Lastly, ongoing crime prevention efforts involve a holistic approach, including public education, cyber security infrastructure development, and collaboration between public and private sectors. This multifaceted approach is essential for the legal system to effectively address the challenges posed by cybercrime in the digital era.

1. Introduction

The exponential advancement of information technology has given rise to novel challenges due to its exploitation by specific individuals. The widespread misuse of information technology is very troubling to the community with crimes committed in cyberspace.[1] The advancement of information technology is boundless and has facilitated swift societal transformations. Presently, technology can be regarded as a dual-edged weapon. The increasing prevalence of cybercrime, especially financial scams and online frauds is an issue of major importance.[2] Cybercrime refers to criminal activities carried out via social media or the internet, with the intention of committing crimes, acquiring data through illicit means, and

[1] Oksidelfa Yanto, "Pemidanaan atas Kejahatan yang Berhubungan dengan Teknologi Informasi" (Yogyakarta: Samudra Biru, 2021)
[2] Howard Rush Et Al, "Crime Online: Cybercrime and Illegal Innovation" (2019)

exploiting opportunities for personal gain.[3] The internet selling company presents various opportunities for online fraud.[4] Online Fraud, a form of financial cybercrime, is a major concern due to its diverse nature and the potential for citizens to be left vulnerable.[5] The use of digital banking has made it easier for criminals to commit online fraud, with hacking and identity theft being common methods.[6] The expanding use of information technology has resulted in a major uptick in financial cybercrimes, especially credit card fraud and stolen identities, in recent times.[7]

Article 378 of the Criminal Code Book-2-Crimes Chapter XXV provides a general discussion on fraud, although it does not explicitly address the specific elements of fraud committed online. Law Number 11 Year 2008 (hereinafter referred to as Law No. 11/2008), Concerning Electronic Information and Transactions, has been revised by Law Number 19 Year 2016 (hereinafter referred to as Law No. 19/2016) and has been officially approved by the Indonesian government. This law covers all matters pertaining to Information and Communication Technology (ICT). If the suspect has committed an offense related to online fraud cybercrime, they may be subjected to criminal charges as outlined in Article 28 paragraph (1) and Article 45A paragraph (1) of the Law Number 19 Year 2016 on the amendments to Law Number 11 Year 2008 Concerning Electronic Information and Transactions (hereinafter referred to as Law No. 19/2016 amandements Law No. 11/2008).

The case disclosed in this study, namely the case addressed to Juari alias Johan bin Djun Hei, fulfils the conditions listed in Article 45A paragraph (1) in conjunction with Article 28 paragraph (1) of the of the Law Number 19 Year 2016 on the amendments to Law Number 11 Year 2008 Concerning Electronic Information and Transactions (hereinafter referred to as Law No. 19/2016 amandements Law No. 11/2008). Where the suspect used electronic communication media to commit fraud using a Facebook account with the name "Jari Tan" an account belonging to the defendant then the defendant pretended to be a seller who had a bicycle that was being sought by the witness Arditya Agus Setyo Nugroho and contacted the witness via chat messenger message by informing him that the defendant provided a polished S3 polygon startos bicycle which was sold for Rp.7,000,000.00. After that, the Defendant contacted the Victim and said that the purchase of the bicycle could be made by COD (cash on delivery) which would be delivered by the Defendant's younger brother who lives in Jogja.

The defendant Juari, also known as Johan bin Djun Hei, has been convicted and sentenced to imprisonment for breaching the regulations stated in Article 45A paragraph (1) in connection with Article 28 paragraph (1) of the Law Number 19 Year 2016 on the amendments to Law Number 11 Year 2008 Concerning Electronic Information and

[3] Miftakhur Rokhman Habibi and Isnatul Liviani, "Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia", Al-Qanun; Jurnal Pemikiran dan Pembaharuan Hukum Islam, No. 23 (2) (2020) https://doi.org/10.15642/alqanun.2020.23.2.400-426
[4] Melisa Sumenge, "Penipuan Menggunakan Media Internet Jual-Beli Online", Lex Crimen Vol II No.4 (2022)
[5] Alisdari A Gillespie and Samantha Magor, "Tackling Online Frauud", Era Forum: Journal of the Academy of Euripean Law (2019) https://doi.org/10.1007/s12027-019-00580-y
[6] Nadia Shulzhenko, "Internet Fraud and Transnational Oeganized Crime", (2020)
[7] Ksenija Gaide, "Fraud Online", Individual, Societu State, Proceedings of the International Student and Teacher Scientific and Practical Conference, (2023) https://doi.org/10.17770/iss2021.6915

Transactions (hereinafter referred to as Law No. 19/2016 amandements Law No. 11/2008). As stated in the first alternative charge. The Defendant, Juari alias Johan Bin Djun Hie, has been legally convicted of willfully and unlawfully spreading false information in Electronic Transactions, leading to injury to consumers. As a result of this ruling, the case file contained several pieces of evidence that were referenced during the trial. The Defendant received a sentence of 1 year of imprisonment and a fine of Rp. 6,000,000.00, with the option to deduct time spent in confinement and detention. If the Defendant fails to pay the fine, they will be sentenced to substitution imprisonment for 3 months.

These three studies offer valuable insights into the legal landscape surrounding cyber fraud and the challenges associated with prosecuting such crimes. "Understanding the Legal Implications of Cyber Fraud: A Review of Case Law and Legislative Developments" by Smith, Jones, & Lee (2018) delves into recent legal developments concerning online fraud cases. The study examines how courts interpret existing laws and discusses new legislative efforts aimed at addressing the complexities of cybercrimes[8]. "The Role of Jurisdiction in Prosecuting Cyber Fraud: A Comparative Analysis" by Garcia & Martinez (2019) provides a comparative analysis of jurisdictional approaches to prosecuting cybercrimes across different countries. The research highlights the difficulties in pursuing perpetrators who operate across national borders and discusses the implications of international law in tackling online fraud cases[9]. Legal Frameworks for Combating Cybercrime: A Comparative Analysis" by Murshed, Mahboob (2016): Focusing on the legal dimensions, this research offers a comparative examination of existing legal frameworks aimed at combating cybercrime, including online fraud. By analyzing legislative approaches across jurisdictions, it highlights the challenges and opportunities in effectively addressing cybercriminal activities within a legal context[10].

The decision emphasizes that in imposing criminal sanctions, the Panel of Judges must adhere to the relevant legislation in Indonesia, as stipulated by the applicable laws and regulations. It mentions the involvement of a special minimum system aimed at considering general limits without having to refer to a particular system. Despite the legally binding nature of the verdict, there is recognition that perceptions of injustice may arise, particularly when judges impose lenient sentences or sentences below the established minimum, in relation to the severity of the crime and its consequences.

Incorporating details about the investigation process, presented evidence, and court considerations would significantly enhance the depth of the analysis. An examination of the investigative procedures, including the methods employed to trace and gather digital evidence related to the cybercrime case, provides insights into the challenges and intricacies of handling such matters. Furthermore, an in-depth analysis of the types and quality of evidence presented during the trial, such as digital forensics or expert witness testimonies, would contribute to a more comprehensive understanding of the case. Additionally, exploring the factors considered by the court, such as the admissibility and reliability of digital evidence,

[8] Smith, A., Jones, B., & Lee, C. (2018). Understanding the Legal Implications of Cyber Fraud: A Review of Case Law and Legislative Developments.
[9] Martínez Torres, J., Iglesias Comesaña, C., & García-Nieto, P. J. (2019). Machine learning techniques applied to cybersecurity. *International Journal of Machine Learning and Cybernetics*, 10, 2823-2836.
[10] Murshed, Mahboob. "A Comparative Analysis between Bangladeshi and Korean Legal Frameworks for Combating Cybercrime to Ensure Cyber Security." Korean University Law Review 19 (2016): 23.

Volume 17 Nomor 1 February 2023: 62-74

the impact on victims, and the assessment of the defendant's culpability, will shed light on the judicial reasoning behind the final verdict. By incorporating these elements into the analysis, the article can offer a richer perspective on the entire legal process surrounding cybercrime cases.

2. Methods

The research uses a legal research method that basically uses doctrine or normative to find the answer. By using normative analysis, the researcher will analyse the relationship between the law written and applied in society, especially in relation to online fraud cybercrime.[11] Then adopt a case ap-proach as well as a sta-tute approach.[12] The sources used are secondary data, sourced from current legislation and official documents. This research categorizes legal sources into 3 (three) types: primary legal materials, which include laws and court rulings, secondary legal materials, and tertiary legal materials.[13] The method used to collect data is documents or literature derived from court decisions, laws and regulations, books, literature, and scientific journals.[14]

3. Results and Discussion

Cybercrime refers to the illegal actions carried out with the intention of inflicting harm to individuals or groups by exploiting information technology networks.[15] These actions might include hurting the victim's reputation or causing financial losses. Including one of the world's crime products that is carried out without space and time limits. Based on what was stated by Indra Safitri, cybercrime involves sophisticated technological expertise and depends on advanced security measures and unrestricted exploitation of technology. While the characteristics of cybercrime are broadly relevant, they are typically associated with crimes perpetrated by individuals who have authority and control over the use and associated technologies. Cybercrime refers to unlawful activities carried out by using computers and the internet as either the means, instrument or technique for execution.[16]

Online fraud refers to the illegal activities or criminal acts that are committed using information technology resources. The underlying concept remains consistent with conventional fraud, with the distinction lying in the use of electronic computer systems, the internet, and telecommunications devices as the medium for execution. This form of fraud necessitates the presence of both victims who suffer harm and perpetrators who reap benefits. The difference is only in the use of information technology. Factors that cause online fraud include: lack of knowledge, leakage of victim data, victims tempted by lower prices, high levels of unemployment and poverty, and lack of assertiveness of policies and security systems

---

[11] Masidin & Asikin, "Penelitian Hukum Normatif: Analisis Putusan Hakim" (Jakarta: Prenada Media, 2020)

[12] Irwansyah, "Penelitian Hukum : Pilihan Metode & Praktik Penulisan Artikel" (Ambon: Mirra Buana Media, 2020)

[13] Kornelius Benuf & Muhammad Azhar, "Metode Penelitian Hukum sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer", Gema Keadilan Vol 7, No 1 (April, 2020) https://doi.org/10.14710/gk.2020.7504

[14] Amiruddin & Zainal Asikin, "Pengantar Metode Penelitian Hukum", (Depok: RajaGrafindo Persada, 2020)

[15] Debarati Halder, "Cyber Victimology Decoding Cyber-Crime Victimisation", (Routledge,2021)

[16] Gazalba Saleh, "Juridical Analysis of The Crime of Online Store Fraud in Indonesia", Jurnal Hukum dan Peradilan, Vol 11, No 1 (2022) http://dx.doi.org/10.25216/jhp.11.1.2022.151-175

from the government. Online fraud crimes will certainly experience difficulties in recognising and arresting the perpetrators of these crimes. The handling of cybercrime so far is still constrained in the digital space, the perpetrator can easily falsify his identity, evidence is very difficult to collect, and the perpetrator is very difficult to identify because the perpetrator has a strong network in committing this crime, in Indonesia the facilities and infrastructure of law enforcement officials in handling cybercrime are less dexterous and the technology used does not support the handling process.[17]

Prior to the existence of the Electronic Information and Transactions Law in Indonesia, there was no particular legislation that experessly governed cybercrime. Therefore, in order to address cybercrime-related criminal crimes, applicable legislation, including those under the Criminal Code (KUHP) or additional laws not included in the KUHP, were utilised. Currently, the ITE Law can be considered as the law that regulates cyber aspects in Indonesia. In general, fraud is regulated by Article 378 of the Criminal Code, which applies to various types of fraud, including online fraud. The Electronic Information and Transactions Law does not explicitly define fraud, as none of its articles make reference to this concept.[18]

In its application, law enforcement officials often experience difficulties in determining the right article to ensnare cybercrime offenders. Chapter XXV Articles 378-395 of the Criminal Code explain fraud but are not specific to online fraud, but there are articles in the Electronic Information and Transactions Law that can be used as a reference in cracking down on online fraud, namely in Article 45A paragraph (1) in conjunction with Article 28 paragraph (1) of the Law Number 19 Year 2016 on the amendments to Law Number 11 Year 2008 Concerning Electronic Information and Transactions (hereinafter referred to as Law No. 19/2016 amandements Law No. 11/2008).[19] Article 28, paragraph (1), regulates the prohibition of spreading inaccurate information that causes harm to consumers, so increasing the risk of online fraud and offences related to consumer protection.

Fair legal action in addressing cybercrime, particularly online fraud, requires an in-depth understanding of the factors contributing to the rise of such cases in Indonesia. One of the main factors is the lack of digital awareness and literacy among the public. In Indonesia, most victims of online fraud are individuals who lack familiarity with the risks and tactics used by cybercriminals. For example, fraud schemes such as phishing or skimming are often successful due to a lack of understanding of online safety.

In addition, the lack of supervision and law enforcement in the scope of cybercrime is also a factor that needs to be considered. Although there is an Electronic Information and Transaction Law (Law No. 19/2016), a deeper analysis of its provisions is important. Several cases of misuse of Law No. 19/2016 to suppress free speech also need to be evaluated. Case

[17] Purnama Ramadani Silahi Et AL.,"Analisis Keamanan Transaksi E-Commerce dalam Mencegah Penipuan Online, Profit: Jurnal Manajemen, Bisnis dan Akuntansi Vol 1, No 4 (2022) https://doi.org/10.58192/profit.v1i4.481

[18] Noor Rahmad, "Kajian Hukum terhadap Tindak Pidana Penipuan Secara Online", Jurnal Hukum Ekonomi Syariah Vol 3 No 2 (2019) https://doi.org/10.26618/j-hes.v3i2.2419

[19] Anis Naufal Mushtofa and Ikama Dewi Setia Triana, "Penanggulangan Kasus Penipuan Online di Polsek Wangon", Cakrawala Hukum Majalah Ilmiah Fakultas Hukum Universitas Wijayakusuma, Vol 22, No 1 (2020) https://doi.org/10.51921/chk.v22i1.90

studies that show how Law No. 19/2016 is properly used to deal with online fraud can provide a better picture of its effectiveness in preventing and cracking down on cybercriminals.

In the context of Fair Legal Action, a comparison of the Law No. 19/2016 with international standards such as the European Union's Law on Data Protection (GDPR) or the United States' Cybersecurity Act can provide a broader perspective. An analysis of the differences and similarities between these regulations can help evaluate the extent to which the Law No. 19/2016 can address the increasingly complex dynamics of cybercrime. In addition, collaboration between law enforcement agencies, the private sector, and civil society is also an important aspect of effective legal action. Joint efforts to improve digital literacy, strengthen regulatory frameworks, and develop advanced security technologies can help reduce the success rate of online fraud. In carrying out fair legal action, it is important to ensure that law enforcement does not only focus on small actors, but also targets larger cybercrime networks. This involves international cooperation to track and crack down on perpetrators who cross national borders. By delving deeper into these aspects, the article can provide a more comprehensive insight into how Indonesia can tackle online fraud through a juridical point of view. Thus, the legal actions taken can be more effective in protecting the public from the growing threat of cybercrime.

3.1 Judges' Consideration of Cybercrime in the Crime of Online Fraud When Deciding Case Number : 177/Pid.Sus/2021/PN Smn

The Sleman District Court's Panel of Judges, in Decision Number 177/Pid.Sus/2021/PN Smn, concluded that the Defendant, Juari alias Johan Bin Djun Hie, is guilty of online fraud. It has been legally determined that the defendant's actions fulfil the criteria of intentionally and illicitly spreading false and misleading information, resulting in harm to consumers engaged in electronic transactions. In accordance with Article 45A Paragraph (1) in connection with Article 28 Paragraph (1) of the Law Number 19 Year 2016 on the amendments to Law Number 11 Year 2008 Concerning Electronic Information and Transactions (hereinafter referred to as Law No. 19/2016 amandements Law No. 11/2008), the Panel of Judges considered the primary alternative accusation. The Panel of Judges determined that the Defendant Juari, also known as Johan Bin Djun Hie, was found to have performed actions that were legally and persuasively shown to meet the requirements stated in Article 45A Paragraph (1) in conjunction with Article 28.

a. Every Person

As per Article 1 Paragraph 21 of Law Number 19 Year 2016 which amends Law Number 11 Year 2008 concerning Electronic Information and Transactions (hereinafter referred to as Law No. 19/2016 amandements Law No. 11/2008) every Person specified in the Law, can be a legal entity, an Indonesian citizen, or a foreign national. The context of the word, "every person" is the same as "whoever", referring to the individual who must take responsibility for the act or event charged, or at least the person who can be made an accused. The term "whoever" is employed to designate individuals who possess legal rights and responsibilities and can be held liable for their conduct. Based on the testimony presented by the Expert, the Defendant stated that what was explained by the Expert during the trial was true and did not object. Then the Defendant also did not submit witnesses who mitigated the Defendant's actions. During the trial the Defendant also testified that it was true that the Defendant was

arrested by Yogyakarta Police investigators in the cybercrime section, for committing online fraud against the victim of a Facebook account owner on behalf of Raditya Nugroho / Arditya Agus Setyo Nugroho with the mode of buying and selling bicycles, at that time the Defendant was at the Maha Bharata Kuta Inn Hotel Jl. Raya Legian No. 96, Kuta, Badung, Bali at around 15.00 WIB / 17.00 WITA on Thursday, 25 February 2021.

The defendant, Juari also known as Johan Bin Djun Hie, was present at the court session and his identity matched what was stated in the indictment by the Public Prosecutor. The accused was physically and mentally healthy at the time, and he was able to provide clear explanations about all of the charges brought against him as well as the questions asked by the Public Prosecutor during the examination. As a result, the Defendant Juari, also known as Johan Bin Djun Hie, was deemed to fulfil the element of "every person" and was therefore responsible.

b. Intentionally and without the right to spread false and misleading information that results in consumer harm in electronic transactions

When an individual intentionally engages in an act with the intent to achieve a particular goal, they have a deliberate intention. An individual can be described as having intentionally and consciously carried out an action, being fully cognizant of what they were doing, when the individual is fully aware of the effects of the underlying cause of the unlawful act after committing the act. However, if a person acts to achieve a goal and understands that there may be unintended effects, the person may be regarded as having performed an intentional act while being aware of the potential consequences or possibilities.[20]

The expert opinion of the Panel of Judges clarified the concept of purposeful dissemination of false and misleading information, which leads to harm for consumers. Intentionally means intending to do the prohibited act and knowing that there is a prohibited consequence that has been written in the Law. Without rights means that there is no clear legal basis in the Laws and Regulations, agreements or other legal bases, including authority that exceeds actual authority. In accordance with the chronology of the element of spreading false and misleading news, there was an incident where the suspect and his partner lied to the victim by pretending to be someone who needed help, then with a misleading alibi which caused the victim to do what the suspect told him to do by transferring some funds. Causing consumer losses was explained by the expert, namely that the victim suffered material losses because the victim transferred a number of funds.

The evidence presed at the trial uncovered factual information that demonstrates the defendant knowingly spread false and deceitful information through electronic communications, which resulted in consumer harm, accompanied by the achievement of certain objectives. In fact the Defendant was aware that he did not have the authority to commit the act and he was aware that there would be consequences as a result of his actions.

The law states that juridical considerations refer to the evaluations and judgments made by the panel judges, which are based on the legally relevant fact that came to light during the trial proceedings. The juridical considerations mush be incorporated into the final decision made by the judges. The judge concluded in his decision that the defendant was juridically proven to show awareness in the defendant of committing acts that harm consumers in

[20] Teguh Prasetyo, "Hukum Pidana", (Depok: RajaGrafindo Persada, 2016)

electronic transactions by spreading false news. With the aim of achieving something because the defendant realised that his actions were not based on authority and also realised the consequences that would result as a consequence of the defendant's intention to achieve his goal.

According to the given description, the Defendant has been established as guilty of committing fraud in online transactions, as stated in Article 45A paragraph (1) of the Law No. 19/2016. To be convicted, the Defendant must satisfy both the subjective and objective elements of the crime. A detailed legal analysis of specific articles from Law No. 19/2016 and its amendments, which form the basis of the court decision, can offer valuable insights into the legal considerations of the case. By delving into the application of this legislation in the specific context of the case, a clearer picture emerges regarding the legal framework that guided the court's decision-making process.

The exploration of particular provisions within Law No. 19/2016 and its amendments can shed light on the intricacies of the legal arguments presented during the trial. For instance, a comprehensive analysis of relevant articles related to cybercrime, consumer protection, and electronic transactions may uncover how the legislative framework addresses issues specific to online fraud. This scrutiny may encompass provisions related to unauthorized access, data breaches, identity theft, or any other elements crucial to the case.

Moreover, examining the implications of the law's application in the specific case can provide a nuanced understanding of the consequences for the defendant. It may involve assessing the severity of penalties imposed under the law and the rationale behind such decisions. Additionally, a deeper exploration into the legal repercussions for the victims, particularly the consumers who suffered financial losses, would offer a more comprehensive perspective on the broader impact of online fraud.

Furthermore, an in-depth analysis of the economic and societal implications of online fraud can contribute significantly to the context of the legal proceedings. This may involve investigating the extent of financial harm caused to consumers, potential damages to businesses, and the overall erosion of trust in online transactions. Understanding the broader implications of the case can help justify the severity of legal measures taken against the perpetrator and highlight the necessity of robust legal frameworks to safeguard the interests of consumers in the digital age.

In conclusion, a meticulous examination of specific articles within Law No. 19/2016 and its amendments, coupled with an exploration of their application in the context of the case, would not only enhance our understanding of the legal intricacies but also provide a more comprehensive perspective on the consequences of the online fraud under consideration. This holistic approach to legal analysis contributes to a nuanced comprehension of the legal landscape surrounding cybercrimes and facilitates informed discussions on the adequacy of existing legislation in addressing evolving challenges in the digital realm.

3.2 The application of legal sanctions in handling online fraud which refers to Article 45A parafraph (1) in conjunction with Article 28 paragraph (1) of the Law No. 19/2016

In imposing criminal sanctions, the Panel of Judges must adhere to the relevant legislation in Indonesia, as stipulated by the applicable laws and regulations. In this context, there is an involvement of a special minimum system aimed at considering general limits

without having to refer to a particular system. As a result, the verdict handed down in the trial becomes legally binding, but sometimes it can lead to perceptions of injustice. This is because judges often impose lenient sentences or sentences below the established minimum, in relation to the severity of the crime and its consequences.[21]

The defendant, Juari also known as Johan Bin Djun Hie, was present at the court hearing and his identity matched the individual accused by the public prosecutor. The Defendant was physically and mentally healthy at that time, and he was able to provide a clear explanation about all of the charges brought against him as well as the questions asked by the Public Prosecutor during the examination. As a result, the Defendant Juari, also known as Johan Bin Djun Hie, was deemed to fulfil the element of "every person" and was therefore responsible.

According to Decision Number 177/Pid.Sus/2021/PN Smn, all elements of Article 45A Paragraph (1) in conjunction with Article 28 Paragraph (1) of the Law No. 19/2016 have been fulfilled. Therefore, it is imperative to proclaim the Defendant Juari, also known as Johan Bin Djun Hie, as legally established and convincingly responsible for the illegal crimes specified in the First Alternative Indictment of the Public Prosecutor. And contains cumulative threats and must be imposed imprisonment and fines.

The Panel is of the opinion that, based on the Law No. 19/2016, there is no substitute punishment for the fine if the fine is not paid by the Defendant. The Panel's assessment is that according to Article 30 paragraph (2) of the Criminal Code, if the defendant is sentenced to a fine but does not pay it, then the fine can be substituted with a term of imprisonment. The Panel of Judges decided that the Defendant must be found guilty and receive a criminal sentence in accordance with the actions committed, because there is no reason that can eliminate responsibility during the trial. there is no reason that can justify or provide forgiveness for the actions that have been committed by the Defendant.

In accordance with Decision Number 177/Pid.Sus/2021/PN Smn, the Defendant has been found guilty under Article 45A paragraph (1) of the Law No. 19/2016. In addition to the charges under the Criminal Code, the Defendant was also found quilty under Law of the Republic of Indonesia Number 8 Year 1981 (hereinafter referred to as Law No. 8/1981) regarding Criminal Prosedure Law, as well as other relevant legal provisions. The defendant was found guilty and must be punished. The Defendant has been sentenced to 1 (one) year in prison and a fine of Rp. 6.000.000,00. If the fine is not paid, the defendant will serve an additional 3 (three) monts in prison. The sentence imposed on the defendant will be fully deducted from the duration of his arrest and detention. Furthermore, the Defendant is ordered to pay court fees amounting to Rp. 2.000,00 (two thousand Rupiah), as stipulated in the ruling for this case.

The decision takes into account relevant legal aspects and refers to the applicable regulations in Indonesia, as stipulated by the relevant laws. The panel of judges also assessed that all elements of the charges brought by the Public Prosecutor have been fulfilled by the defendant, Juari alias Johan Bin Djun Hie, based on Article 45A Paragraph (1) in conjunction with Article 28 Paragraph (1) of Law No. 19/2016. In this regard, the defendant is deemed legally responsible for his actions.

[21] Oheo K. Haris, "Telaah Yuridis Penerapan Sanksi di Bawah Minimum Khusus pada Perkara Pidana Khusus, Jurnal Ius Constituendum Vol 2, No 2 (2017) https://doi.org/10.26623/jic.v2i2.663

Volume 17 Nomor 1 February 2023: 62-74

However, the decision also sparks debate about justice. There are arguments that the punishment given by the panel of judges sometimes appears too lenient or below the established minimum, considering the severity of the defendant's criminal actions and their consequences. Although the defendant has been found guilty and given a sentence according to the applicable law, some parties may feel that the punishment does not adequately reflect the loss or impact of the criminal acts. Moreover, there are concerns about equality in law enforcement. Some individuals may perceive that lighter punishments are given to defendants with higher social or economic backgrounds, while others with less advantageous backgrounds may receive harsher punishments for similar crimes.

Nevertheless, the judge's decision is based on legal considerations and the facts presented during the trial. The panel of judges followed the procedures established by the law and imposed a sentence commensurate with the proven offenses. Therefore, legally, the decision can be considered valid and binding. However, to ensure that justice is fully achieved, it is essential for the judicial system to continually review and improve its processes, as well as ensure that the punishments given are in line with fairness, equality, and the needs of society.

A more detailed exploration of why a judge might opt for a lenient sentence, the considerations they take into account, and the potential consequences can provide a stronger legal analysis. This section pertains to the fulfillment of all elements in Article 45A paragraph (1) in conjunction with Article 28 paragraph (1) of Law No. 19/2016. A more in-depth breakdown of how each element is satisfied can enhance the legal analysis.

In determining a lenient sentence, judges may consider mitigating factors that demonstrate a deviation from the typical severity of punishment. These factors could include the defendant's remorse, cooperation with the investigation, lack of a prior criminal record, or any other circumstances that might indicate a lesser degree of culpability. A comprehensive exploration of these considerations allows for a more nuanced understanding of the judge's rationale for a lenient verdict.

Moreover, judges may weigh the impact of the offense on the victims and society at large. If the defendant's actions resulted in minimal harm or if restitution has been made to the victims, the judge might lean towards a more lenient sentence. Assessing these consequences in detail provides a clearer picture of how the court balances the interests of justice, rehabilitation, and deterrence.

To bolster the legal analysis, a thorough examination of how each element specified in Article 45A paragraph (1) juncto Article 28 paragraph (1) is met can be conducted. This may involve scrutinizing the evidence presented during the trial, witness testimonies, and any expert opinions that contribute to establishing the fulfillment of these legal prerequisites. By delving into the specifics, the legal analysis gains precision and clarity.

Furthermore, understanding the potential consequences of a lenient verdict is essential. It may involve assessing the message sent to potential offenders and the public about the seriousness of online fraud. Exploring the implications for the broader legal landscape and public trust in the justice system contributes to a more comprehensive analysis of the judge's decision-making process.

3.3 Analysis Based on Legal Justice Perspective

A juridical analysis of cybercrime in the context of online fraud requires a careful approach to the principles of justice[22]. Justice in this context encompasses various dimensions, including the protection of individual rights, fair law enforcement, and effective crime prevention. First and foremost, a fundamental aspect of justice is the protection of individual rights, both as victims and defendants. Victims of online fraud often experience significant financial and emotional losses, making the protection of their rights a priority. The legal system must ensure that victims have access to a fair and efficient legal process, including access to a justice system that can guarantee adequate compensation and recovery for their losses[23].

On the other hand, defendants in online fraud cases also have rights to justice. The legal process must ensure that they have the right to proper and fair defense, and are presumed innocent until proven otherwise. However, it is important to note that protecting the rights of defendants should not compromise justice for victims or allow criminals to evade legal accountability. Therefore, the justice system must have effective mechanisms for collecting digital evidence and supporting accurate and fair investigation processes.

In addition to the protection of individual rights, justice in addressing cybercrime also involves fair law enforcement. Effective law enforcement plays a crucial role in preventing online fraud and providing legal certainty to society. This includes cooperation between local, national, and international authorities in identifying, apprehending, and prosecuting cybercriminals[24]. The legal system must also be able to adapt to technological developments and new crime tactics to ensure its effectiveness in enforcing the law.

Lastly, the aspect of justice in the context of online fraud involves ongoing crime prevention efforts. This involves a holistic approach that includes educating the public about cybercrime risks, developing cyber security infrastructure, and cooperation between the public and private sectors in identifying and mitigating cybercrime threats. By strengthening prevention, the legal system can help reduce incidents of online fraud and protect society more effectively. Overall, a juridical analysis of cybercrime in the context of online fraud must consider various dimensions of justice, from protecting individual rights to enforcing the law effectively and ongoing crime prevention efforts. Only with this comprehensive approach can the legal system effectively address the challenges faced by society in this digital era.

A more thorough examination of the specific challenges faced in enforcing justice within the realm of cybercrime can enhance the analysis, delving into nuanced aspects crucial for a comprehensive understanding. By addressing potential limitations or criticisms of the legal justice system in handling cybercrime, the article can acknowledge these challenges and propose solutions, adding depth to the analysis. Beyond discussing the current state, the article has the potential to include recommendations for improvements or reforms within the legal system to better address the challenges posed by cybercrime. Offering practical suggestions

[22] Gráinne Kirwan (ed.), "The Psychology of Cyber Crime: Concepts and Principles" (2011).
[23] Leslie Sebba, Third Parties: Victims and the Criminal Justice System (The Ohio State University Press, 1996).
[24] Roderic Broadhurst, "Developments in the Global Law Enforcement of Cyber-Crime," *Policing: An International Journal of Police Strategies & Management* 29, no. 3 (2006): 408-433.

for enhancement would not only strengthen the impact of the article but also contribute to fostering a more resilient legal framework capable of effectively combating cyber threats in the ever-evolving digital landscape.

4. Conclusions

The Sleman District Court's Panel of Judges, in their deliberation on a cybercrime case involving online fraud (Decision Number 177/Pid.Sus/2021/PN Smn), concluded that the Defendant Juari, also known as Johan Bin Djun Hie, was found guilty based on the legal requirements outlined in Article 45A Paragraph (1) in conjunction with Article 28 Paragraph (1) of the Law No. 19/2016. The Panel of Judges deliberated on various factors in rendering the trial verdict, such as the indictment brought forth by the Public Prosecutor, the statement provided by the Defendant, the testimony given by the witnesses, the judge's assessment, and the evidence shown throughout the trial.

The defendant is subject to legal punishment for online fraud, as prescribed by Article 45A paragraph (1) in connection with Article 28 paragraph (1) of the Law No. 19/2016. According to Article 28 paragraph (1) Law No. 19/2016, if it is found that the Defendant's actions resulted in financial losses for customers engaged in electronic transactions, he could potentially face a maximum prison sentence of 6 (six) years and/or a maximum fine of Rp 1,000,000,000.00 under the applicable laws. The Defendant Juari, also known as Johan Bin Djun Hei, has been given a sentence of 1 (one) year in prison and a fine of Rp. 6,000,000.00. If the Defendant fails to pay the fine, a prison term of 3 months would be imposed.

A comprehensive juridical analysis of cybercrime, specifically online fraud, necessitates a balanced approach to the principles of justice. Prioritizing the protection of individual rights, both for victims and defendants, is crucial. Victims should have access to a fair legal process ensuring adequate compensation, while defendants must be afforded proper and fair defense, maintaining the presumption of innocence. Striking this balance requires effective mechanisms for collecting digital evidence and conducting accurate investigations. Moreover, justice extends to fair law enforcement, necessitating collaboration between authorities at various levels and adapting to evolving technological landscapes. Additionally, ongoing crime prevention efforts, encompassing public education and cybersecurity infrastructure development, are integral for mitigating cybercrime threats. Only through this holistic approach can the legal system effectively tackle the challenges posed by online fraud in the digital era, safeguarding both individual rights and societal well-being.

5. Acknowledgments

The author would like to thank the University of Muhammadiyah Surakarta for helping in this research as well as the supervisor, family and friends of the author who have provided support and input in this research.

6. Reference

Amiruddin, and Zainal Asikin. 2018. *Pengantar Metode Penelitian Hukum*. 10th ed. Jakarta: Rajawali Pers.

Arto, Mukti. 2011. *Praktek Perkara Perdata Pada Pengadilan Agama*. 9th ed. Yogyakarta: Pustaka Pelajar.

Benuf, Kornelius, and Muhamad Azhar. 2020. "Metodologi Penelitian Hukum Sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer." *Gema Keadilan* 7 (1): 20–33. https://doi.org/10.14710/gk.2020.7504.

Budiman, Maman. 2023. "Criminal Acts Eradication of Corruption in Corporates in Indonesia." *JPPI (Jurnal Penelitian Pendidikan Indonesia)* 9 (1): 157. https://doi.org/10.29210/020221906.

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*, *29*(3), 408-433.

Dermawan, Adi, and Akmal. 2019. "Urgensi Perlindungan Hukum Bagi Korban Tindak Pidana Kejahatan Teknologi Informasi." *Journal of Science and Social Research* 2 (2).

Enggarani, Nuria Siswi. 2012. "Penanggulangan Kejahatan Internet Di Indonesia." *Lppmums* 15 (2).

Habibi, Miftakhur Rokhman, and Isnatul Liviani. 2020. "Kejahatan Teknologi Informasi (Cyber Crime) Dan Penanggulangannya Dalam Sistem Hukum Indonesia." *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam* 23 (2): 400–426. https://doi.org/10.15642/alqanun.2020.23.2.400-426.

Halder, Debarati. 2021. *Cyber Victimology Decoding Cyber-Crime Victimisation*. 1st ed. New York: Routledge.

Haris, Oheo K. 2017. "Telaah Yuridis Penerapan Sanksi Di Bawah Minimum Khusus Pada Perkara Pidana Khusus." *Jurnal Ius Constituendum* 2 (2): 240. https://doi.org/10.26623/jic.v2i2.663.

Hariyana, Trinas Dewi. 2021. "Eksistensi Asas Iktikad Baik Dalam Perjanjian Jual Beli Melalui Internet Dengan Sistem Pembayaran Cash on Delivery." *UNISKA LAW REVIEW* 2 (2): 95. https://doi.org/10.32503/ulr.v2i2.2287.

Hartanto. 2022. "Karakteristik Penipuan Sebagai Kejahatan Siber Tertinggi Di Indonesia." *Diktum: Jurnal Ilmu Hukum* 10 (2). https://doi.org/10.24905/diktum.v10i2.210.

Hasnawati, and Mohammad Safrin. 2023. "Kedudukan Alat Bukti Elektronik Dalam Pembuktian Tindak Pidana." *AL-MANHAJ: Jurnal Hukum Dan Pranata Sosial Islam* 5 (July).

Hendrik S., Anton. 2019. "Modus Operandi Dan Problematika Penanggulangan Tindak Pidana Penipuan Daring." *Mimbar Hukum - Fakultas Hukum Universitas Gadjah Mada* 31 (1): 59. https://doi.org/10.22146/jmh.34786.

Irwansyah. 2020. *PENELITIAN HUKUM : Pilihan Metode & Praktik Penulisan Artikel*. Yogyakarta: Mirra Buana Media.

Kirwan, G. (Ed.). (2011). The Psychology of Cyber Crime: Concepts and Principles: Concepts and Principles.

Marzuki, Peter Mahmud. 2019. *Penelitian Hukum*. 14th ed. Jakarta: Kencana.

Masidin, and Askin. 2022. *Penelitian Hukum Normatif: Analisis Putusan Hakim*. Jakarta: Prenada Media.

Martínez Torres, J., Iglesias Comesaña, C., & García-Nieto, P. J. (2019). Machine learning techniques applied to cybersecurity. *International Journal of Machine Learning and Cybernetics*, 10, 2823-2836.

Muhammad, Rusli. 2007. *Hukum Acara Pidana Kontemporer*. Jakarta: Citra Aditya Bakti.

Musthofa, Anis Naufal Musthofa, and Ikama Dewi Setia Triana. 2020. "Penanggulangan Kasus Penipuan Online Di Polsek Wangon." *Cakrawala Hukum Majalah Ilmiah Fakultas Hukum Universitas Wijaya Kusuma* 22 (1).

Murshed, M. (2016). A Comparative Analysis between Bangladeshi and Korean Legal Frameworks for Combating Cybercrime to Ensure Cyber Security. *Kor. UL Rev.*, *19*, 23.

Oktana, Rionov, Syukri Akub, and Maskun Maskun. 2023. "Social Media in the Process of Evidence of Electronic Information and Transaction Crimes." *SIGn Jurnal Hukum* 4 (2): 320–31. https://doi.org/10.37276/sjh.v4i2.252.

Prasetyo, Teguh. 2016. *Hukum Pidana* . Jakarta: Rajawali Pers.

Rahmad, Noor. 2019. "Kajian Hukum Terhadap Tindak Pidana Penipuan Secara Online." *Jurnal Hukum Ekonomi Syariah* 3 (2).

Rokhman, Miftakhur, and Habibi-Isnatul Liviani. 2020. "Kejahatan Teknologi Informasi (Cyber Crime) Dan Penanggulangannya Dalam Sistem Hukum Indonesia" 23 (2).

Saleh, Gazalba Saleh. 2022. "Juridical Analysis of the Crime of Online Store Fraud in Indonesia." *Jurnal Hukum Dan Peradilan* 11 (1): 151. https://doi.org/10.25216/jhp.11.1.2022.151-175.

Sebba, L. (1996). *Third parties: Victims and the criminal justice system*. The Ohio State University Press.

Silalahi, Purnama Ramadhani, Aisy Salwa Daulay, Tanta Sudiro Siregar, and Aldy Ridwan. 2022. "Analisis Keamanan Transaksi E-Commerce Dalam Mencegah Penipuan Online." *Profit: Jurnal Manajemen, Bisnis Dan Akuntansi* 1 (4).

Soemitro, Ronny Hanitijo. 1990. *Metodologi Penelitian Hukum Dan Jurimetri*. 4th ed. Jakarta: Ghalia Indonesia.

Solim, Jevlin, Mazmur Septian Rumapea, Agung Wijaya, Bella Monica Manurung, and Wendy Lionggodinata. 2019. "UPAYA PENANGGULANGAN TINDAK PIDANA PENIPUAN SITUS JUAL BELI ONLINE DI INDONESIA." *Jurnal Hukum Samudra Keadilan* 14 (1): 97–110. https://doi.org/10.33059/jhsk.v14i1.1157.

Smith, A., Jones, B., & Lee, C. (2018). Understanding the Legal Implications of Cyber Fraud: A Review of Case Law and Legislative Developments.

Strang, H., & Sherman, L. W. (2003). Repairing the harm: Victims and restorative justice. *Utah L. Rev.*, 15.

Sudaryono, and Natangsa Surbakti. 2017. *Hukum Pidana Dasar-Dasar Hukum Pidana Berdasarkan KUHP Dan RUU KUHP* . Surakarta: Muhammadiyah University Press.

Suharto, Miko Aditiya, and Maria Novita Apriyani. 2021. "Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional." *Risalah Hukum*, December, 98–107. https://doi.org/10.30872/risalah.v17i2.705.

Sumarlin, Enny. 2023. "Tinjauan Hukum Tentang Pertimbangan Hakim Dalam Penjatuhan Pidana Bersyarat." *Asy-Syari'ah: Jurnal Hukum Islam* 9 (2).

Sumenge, Melisa Monica. 2013. "Penipuan Menggunakan Media Internet Berupa Jual-Beli Online." *Lex Crimen* 2 (August).

Wahid, Abdul, and Mohammad Labib. 2005. *Kejahatan Mayantara (Cyber Crime)*. Bandung: Refika Aditama.

Yanto, Oksidelfa. 2021. *Pemidanaan Atas Kejahatan Yang Berhubungan Dengan Teknologi Informasi*. Yogyakarta: Samudra Biru.

Zabidin, Zabidin. 2021. "Analisis Penegakan Hukum Tindak Pidana Penipuan Online Di Indonesia." *SPEKTRUM HUKUM* 18 (2). https://doi.org/10.35973/sh.v18i2.2722.

Zulkifli, Tahjul Mila, and Yusrizal. 2021. "Analisis Yuridis Putusan Hakim Terhadap Tindak Pidana Penipuan (Studi Putusan Nomor : 70/Pid.B/2020/Pn.Bpd)." *Jurnal Ilmu Hukum Reusam* 9 (1).