JSH
Supremasi Hukum: Jurnal Penelitian Hukum
P-ISSN: 1693-766X ; E-ISSN: 2579-4663, Vol. 33, No 2, Agustus 2024, 124-136
https://ejournal.unib.ac.id/supremasihukum/index
DOI: https://doi.org/10.33369/jsh.33.2.124-136

The Yogyakarta Police Overcoming Online Fraud Crimes Strategy At Society 5.0 Era

Lukman Khakim, Nabila Nur Fadlilah
Universitas Islam Negeri Sunan Kalijaga Yogyakarta
E-mail: lkmkhakim@gmail.com

Abstract

Online fraud is a crime in e-commerce using the internet. Online fraud crimes develop massively along with technological advances, giving rise to varied modus operandi. This study aims to analyze and explain the strategies applied by the Yogyakarta Special Region Police in overcoming online fraud crimes in the era of society 5.0. This study uses an empirical legal research method with a field research approach. This research presents primary and secondary data taken from various sources, such as interviews with police officials and data related to online fraud cases. The results show that the DIY Police in overcoming online fraud crimes in the era of society 5.0 has adopted various strategies, such as increasing public awareness, collaborating with digital platform providers, and improving digital investigation capabilities. Nonetheless, challenges in tackling online fraud remain, including legal constraints and technological lag. This research provides insights into how law enforcement is adapting to changes in the society 5.0 era and provides a basis for further improvements in efforts to tackle online fraud crimes.

Keywords: *Strategy; DIY Police; Online Fraud; Era Society 5.0.*

Introduction

Nowadays, the development of globalization is increasingly massive. This is one of the factors that triggered the rapid development of information technology throughout the world.[1] Information technology plays an important role in people's lives, because its development brings various kinds of benefits and great impacts to each country. The development of information technology will also always be closely

[1] Syalaisha Amani Puspitasari. "Tinjauan Yuridis Eksploitasi Manusia dalam Fenomena Mandi Lumpur." *JISIP (Jurnal Ilmu Sosial dan Pendidikan)* 7.3 (2023): 2840-2846. http://dx.doi.org/10.58258/jisip.v7i3.5349, p 2840.

related to improving the welfare of the people in a country.[2] Therefore, in a country, information technology acquires such an important position.

Technological developments will certainly have implications for social change.[3] Social change is not always positive, but also negative. This negative social change can be exemplified by the birth of new forms of crime with varied modus operandi. As a negative impact of technological advancement is crime in cyberspace or *cyber space*, hereinafter known as *cyber crime*.[4]

Intermediary *crime* or *cyber crime* is one of the crimes that currently requires serious attention from the Government of Indonesia.[5] This is because *cyber crime* is a type of crime that has a very broad scope and does not recognize legal boundaries.[6] One example of a case of mayantara crime or *cyber crime* is *online* fraud.

Along with the dynamics of digitalization, *online* fraud is one of the crimes that accounts for the most cases in *cybercrime*.[7] Various factors certainly influence this, both external factors and internal factors.[8] One of the external factors is the development of technology which has now transformed from the era of industrial revolution 4.0 to the era of *society* 5.0 which develops *artificial intelligence* systems. This transformation is certainly warmly welcomed by criminal elements because it is

[2] Ahmad M. Ramli, et al. "Pelindungan Kekayaan Intelektual dalam Pemanfaatan Teknologi Informasi di Saat Covid-19." *De Jure Journal of Legal Research* 21.1 (2021): 45-58. http://dx.doi.org/10.30641/dejure.2021.V21.045-058, p. 46.

[3] Wim Hapsoro, M. Aidjili, & Budijanto, H. A. "Yurisdiksi Hukum Pidana dalam Pembatasan Informasi Hoaks Terkait dengan Kejahatan *Cybercrime*". *Ristek: Journal of Research, Innovation and Technology of Batang Regency*, 7(1), (2022). 11-19. https://doi.org/10.55686/ristek.v7i1.124, p. 15.

[4] Fatma Yunita. "Aspek Hukum Penggunaan Media Sosial Berbasis Internet". *Journal of Notarius*, 2(1). (2023). https://jurnal.umsu.ac.id/index.php/notarius/article/view/15899, p 123.

[5] Miftakhur Rokhman Habibi and Isnatul Liviani. "Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia." *Al-Qanun: Journal of Islamic Legal Thought and Reform*, 23(2), (2020). https://www.academia.edu/download/95670346/480663504.pdf, p. 412.

[6] I Gusti Ayu Suanti Karnadi Singgi, I Gusti Bagus Suryawan, and I Nyoman Gede Sugiartha. "Penegakan Hukum terhadap Tindak Pidana Peretasan sebagai Bentuk Kejahatan Mayantara (*Cyber Crime*)". *Journal of Legal Construction*, 1(2), 334-339. https://doi.org/10.22225/jkh.1.2.2553.334-339, p. 336.

[7] Rian Dwi Hapsari and Kuncoro Galih Pambayun. "Ancaman cybercrime di indonesia: Sebuah tinjauan pustaka sistematis." *Constituent Journal* 5.1 (2023): 1-17. https://doi.org/10.33701/jk.v5i1.3208, p. 10.

[8] Priskila Askahlia Sanggo and Diana Lukitasari. "Pertanggungjawaban Pidana Pelaku Penipuan Arisan Online ditinjau dari Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik." *Journal of Criminal Law and Crime Prevention* 3.2 (2014): 221-230. https://doi.org/10.20961/recidive.v3i2.40524, p. 225.

considered to bring convenience and benefits to them in carrying out their actions with an increasingly systematized modus operandi.

On the other hand, this certainly provides homework as well as challenges for law enforcement officials in eradicating perpetrators of mayantara *crime* (*cyber crime*), especially *online* fraud. Because with mechanisms that evolve to become more systematic, it makes it easier for people to plan and strategize in order to launch their actions, making the identity of the person increasingly camouflaged. This will certainly make it more difficult for law enforcement officials to uncover cases of crime if it is not balanced with the existing x-factor.

There is previous research on law enforcement of *cyber crime* in the DIY Police jurisdiction conducted by Prasetiyo and Mukhtar Zuhdy. His research entitled "Law Enforcement by *Cyber Crime* Investigators in Cybercrime in the DIY Police Area" shows the obstacles of law enforcement of *cyber crime* at the level of investigation and investigation due to internal factors such as aspects of investigators and external factors such as evidence, supporting facilities, and jurisdiction.[9]

Meanwhile, Isnaeni Komalasari conducted research on the role of investigators in uncovering criminal acts of *online* fraud through e-commerce internet media. Her research entitled "The Role of Investigators in Uncovering the Crime of Fraud in *Online* Buying and Selling Transactions through *E-Commerce* Internet Media" shows that the role of an investigator in disclosing cases of *e-commerce* transaction fraud that occurred in Ternate City is to refer to the rules set out in the Criminal Procedure Code. The factors that hinder the disclosure of fraud cases that occur in Ternate City are internal factors and external factors.[10]

Therefore, this research seeks to explore and analyze the strategies carried out by the Yogyakarta Special Police in overcoming *online* fraud cases in line with the development of the *society* 5.0 era which develops artificial intelligence systems.

Based on the background description that has been stated above, the author in this case has formulated several problems as follows:

1. What are the obstacles that hinder the DIY Police in uncovering *online* fraud crimes in the era of *society* 5.0?

[9] Prasetiyo and Mukhtar Zuhdy. "Penegakan Hukum oleh Aparat Penyidik Cyber Crime dalam Kejahatan Dunia Maya (*Cyber Crime*) di Wilayah Hukum Polda DIY." *Indonesian Journal of Criminal Law and Criminology (IJCLC)* 1.2 (2020). 79-88, https://doi.org/10.18196/ijclc.v1i2.9611, p. 85.

[10] Isnaeni Komalasari. "Peran Penyidik dalam Mengungkap Tindak Pidana Penipuan Transaksi Jual Beli Online Melalui Media Internet E-Commerce." *Indonesian Journal of Criminal Law* 3.2 (2021). 201-210, https://journal.ilininstitute.com/index.php/IJoCL/article/view/1385, p. 208.

2. How is the strategy applied by the DIY Police in handling cases of *online* fraud crimes in the era of *society* 5.0?

Research Methods

The method used by the author in this research is an empirical legal research method with a field research approach, which is a research method that uses facts that occur in the field. This research uses primary data and secondary data. Primary data collection techniques in the form of interviews with Unit 2 Sub-Directorate V *Cyber* Assistant Stakeholders of the Yogyakarta Special Region Police as sources, secondary legal sources in the form of data related to the research topic obtained from the Yogyakarta Special Region Police and laws and regulations.

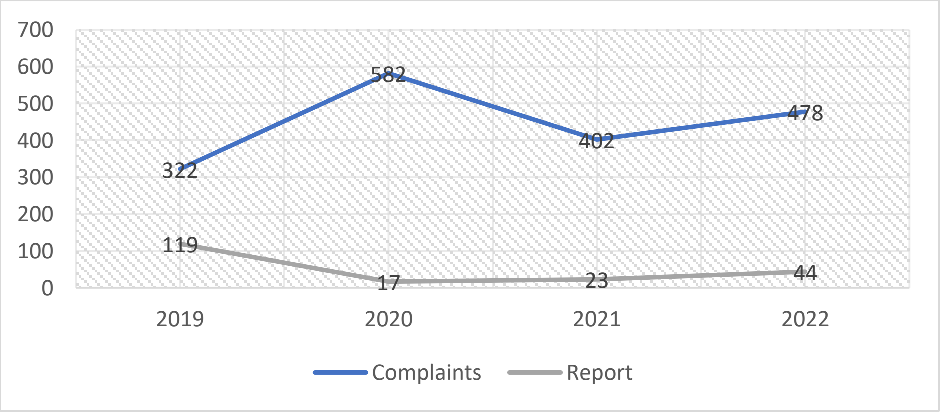
Results And Discussion

A. The Rise of *Online* Fraud in the Special Police Region of Yogyakarta

The Special Region of Yogyakarta is one of the most well-known provinces in Indonesia. This is partly because the region still maintains noble cultural values. In addition, there are many tourist destinations that also make the conversation by the general public. As a city dubbed the "City of Students", it is certain that every year there are many prospective students who flock to study in the area. This is slowly transforming the Special Region of Yogyakarta into a metropolitan city.

However, progress has its own implications. For example, the crime rate has increased compared to other regions. Not only in the form of conventional crimes, but also mayantara crimes or *cyber crimes.*

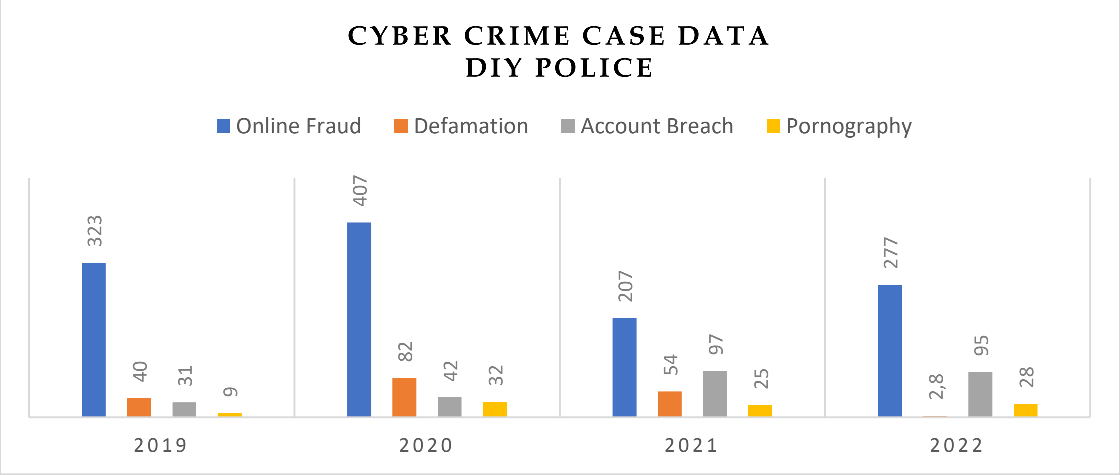
Table 1. *Data on Reports and Complaints of ITE Crimes from Yogyakarta Regional Police*



Based on the results of the data above, *cybercrime* in the jurisdiction of the Yogyakarta Special Region Police in the period 2019 to 2022 has relatively increased. This can be seen from the number of complaints in 2019 totaling 322 complaints, increasing in 2020 to 582 complaints. Then it dropped to 402 complaints in 2021, but increased again in 2022 to 478 complaints. The data that has been presented indicates that cases of mayantara *crime* (*cyber crime*) in the jurisdiction of the DIY Police are still relatively high.

Cybercrime cases that occur in the jurisdiction of the Yogyakarta Regional Police are certainly not only filled by one type of crime, but many crimes that contribute to the number of complaints reported to the Yogyakarta Special Police as shown in the following diagram.

Table 2. *Cyber Crime Case Data of Yogyakarta Police*



Source: Ditreskrimsus Polda DIY

According to the data observed above, *online* fraud cases are the highest-ranking cases in the reports received by the Yogyakarta Police. *Online* fraud is an act of fraud or fraud committed through the internet or *online platforms*. *Online* fraud itself in reality has no significant difference when compared to conventional fraud or fraud in general. The point of difference is only seen in the means of action.[11]

[11] Yusri Ardiyah Pramesti and Emy Rosnawati. "Tindak Pidana Penipuan dalam Media Jual Beli Online." *Web of Scientist International Scientific Research Journal* 2. 4. (2023). 1-15 https://doi.org/10.47134/webofscientist.v2i4.8, p. 6.

Online fraud in Indonesian positive law is regulated in Article 28 paragraph (1) of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, which states that:

> *"Every person intentionally and without the right to spread false and misleading news that results in consumer harm in Electronic Transactions."*

Then regarding the explanation of the implementation of Article 28 paragraph (1) is regulated in the Joint Decree of the Minister of Communication and Information of the Republic of Indonesia (Number 229 of 2021) and the Attorney General of the Republic of Indonesia (Number 154 of 2021), and the Chief of the Indonesian National Police (Number KB/2/VI/2021) concerning Guidelines for the Implementation of Certain Articles in Law Number 11 of 2008 concerning Electronic Information and Transactions as amended by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions which states:

> *"a) The criminal offense in Article 28 paragraph (1) of the ITE Law is not a criminal offense against the act of spreading false news (hoaxes) in general, but rather the act of spreading false news in the context of electronic transactions, such as online trading......."*

Then when viewed from the community's point of view regarding the causes of *online* fraud, of course this cannot be separated from the awareness of each individual community. But on the other hand, there are factors that cause an individual to commit a criminal act of fraud according to the results of an interview with Iptu Robertus Wuriyan Kristama, S.H. as the Acting Assistant Unit 2 Subdit V Cyber of the DIY Regional Police, including:

1. Economic Factors

Based on the data in Table 2, *online* fraud cases in 2020 experienced the highest percentage compared to the years before and after. This is due to the *Covid-19* pandemic which at that time made the transition in people's lives change and had implications for the weakening economy.

One of the impacts of the transition period is that many people have become unemployed due to the number of companies that have gone out of business. So that in urgent conditions, many people commit acts that are prohibited by applicable norms and laws, one of which is committing fraud.

2. Environmental Factors

Environmental factors are the next factor that causes someone to commit *online* fraud. As a continuation of the first factor, Indonesia only released the emergency status of the *Covid-19* pandemic at the end of 2022, which means that in the previous year there was still a ban on leaving the house. At that time, many activities must be carried out online, including buying and selling transactions.

From this, *e-commerce* is experiencing a tsunami of consumers. Moreover, the consumptive lifestyle of Indonesians, of course, the criminals do not want to waste this golden opportunity to launch their actions. Thus, it is proven that during this period of time, *online* fraud cases were able to rank first in cases of mayantara crime or *cyber crime* in the jurisdiction of the Yogyakarta Special Police.

3. Factors making it easy to commit *online* fraud crimes

Online fraud in the era of sophisticated technology is increasingly easy to commit. For example, by creating *fake* accounts and taking other people's content for promotion. Another convenience is that there are many *online shops* that have developed, thus opening a gap for people to trick the public because of their negligence.

4. Minimal risk of being caught by law enforcement officials

The rapid development of technology in addition to providing benefits to society, also provides a gap of opportunity for criminals to develop their modus operandi so that it is more systematic and secret. This certainly makes it difficult for law enforcement officials or requires more time to track the digital traces of individuals amid the rise of *online* fraud cases due to technological limitations and so on.

B. Factors Hindering the Yogyakarta Special Police Force in Solving *Online* Fraud Crimes

The Yogyakarta Special Police's efforts in uncovering *online* fraud crimes do not always run smoothly. Of course, in every action there will be pebbles that become factors that hinder the procession of disclosing *online* fraud cases by the Yogyakarta Special Police. These factors are not only internal to the Yogyakarta Police, but also many external factors which are beyond the control of the Yogyakarta Police investigators.

This is in line with the results of an interview with Iptu Robertus Wuriyan Kristama, S.H. as Acting Assistant Unit 2 Subdit V Cyber Polda DIY, he said:

> *"There are many factors that cause an investigation and investigation activity in uncovering online fraud crime cases to be hampered and not run as planned. These factors are not only internal but also external factors."*

The following are the factors that hinder the investigation and investigation process by the Yogyakarta Special Region Police in uncovering *online* fraud crimes:

1. Internal Factors

a) Human Resources (HR) of DIY Police Investigators

One of the internal factors that become obstacles in uncovering *online* fraud cases in the jurisdiction of the Yogyakarta Special Region Police is the limited number of human resources. With the number of cases that are relatively large and increasing every year, if compared with the number of human resources (HR) of the Yogyakarta Special Region Police, in this case, the investigators of the Special Criminal Investigation Unit of Subdit V Siber Polda DIY, of course, will not find a balance point.

In addition, the lack of investigators who can be said to be proficient or have abilities in the field of ITE and mayantara *crime (cyber crime*). This will certainly be an obstacle in disclosing the rise of *online* fraud crime cases. In fact, in the author's opinion, this can be a threat in the future because of technological advances which have implications for the increase in *crime* cases, especially cybercrime, which has not yet had a meeting point of balance with the quantity and quality of the human resources of the investigators of the Special Criminal Investigation Unit of Subdit V Siber Polda DIY itself.

b) Limited Facilities and Infrastructure

The next obstacle is due to the limited technological facilities owned by the Yogyakarta Special Region Police. This can certainly hinder the investigators of the Special Criminal Investigation Unit (Ditreskrimsus) Subdit V Cyber of the Yogyakarta Special Region Police in uncovering cases of *online* fraud crimes. As we already know, the times are getting more modern and technological developments are becoming very fast and rapid. This means that the modus operandi used by *online* fraud criminals is certainly very varied with a systematic plan. Therefore, with limited technological means, it will certainly be very difficult to uncover *online* fraud crimes with an increasingly sophisticated system.

2. External Factors

a) Account Forgery

Tracking the perpetrators of fraud in *online* buying and selling transactions is difficult because often the perpetrators tend to use fake identities or even take other people's identities. Starting from falsified phone numbers for registration purposes, to the use of account numbers that actually belong to other people, as well as various other facilities used by the perpetrators to facilitate their crimes. What is crucial in this *online* buying and selling fraud crime is that the perpetrator and victim do not have a direct meeting, making the investigation more complicated.

b) Misaligned Laws and Regulations

Legal regulations that are not in line with technological developments and *online* fraud methods can hinder the investigation process. The non-fulfillment of the elements of an article causes the escape of *online* fraud criminals from the snares of law enforcement officials.

c) Lack of Public Awareness

A significant external factor in hampering the criminal investigation process is the lack of public awareness. Public awareness refers to the level of public understanding and knowledge about legal issues, crime, and the importance of cooperation with law enforcement. When people lack legal awareness, the investigation process is hampered. This can be caused by a variety of factors, including low or poor quality education, which makes people less familiar with the law.

In addition, distrust of law enforcement, which may arise due to scandals or unethical behavior, can discourage people from participating in investigations. Cultural factors and traditions can also play an important role in determining people's attitude towards the law. The result of this lack of public awareness is underreporting of crimes, difficulty in obtaining testimonies, disruption in the judicial process, and a decreased sense of justice in society.

d) Difficulty in Collecting Enough Evidence

Online fraud investigations are often faced with external factors that hinder the collection of sufficient evidence. *Online* fraud involves clever perpetrators who often use sophisticated technology to hide their tracks. Evidence in *online* fraud cases, such as transaction records or electronic communications, can be easily altered or deleted by perpetrators, making them difficult to locate and preserve as solid evidence. In addition, cross-jurisdictional cooperation can be difficult in *online* fraud cases, as perpetrators often operate in different countries or regions. This can make it difficult for investigators to gather evidence from scattered sources. Therefore, *online* fraud investigations require extra effort in digital forensic techniques.

C. The Yogyakarta Special Police's Strategy in Overcoming *Online* Fraud Crimes in the Era of *Society* 5.0

The era of *society* 5.0 projects a substantial transformation in the way people live and interact. In this period, advances in the development of information and communication technology have brought together physical reality and the virtual world, creating a strong global network.[12] The era of *society* 5.0 opens a new chapter in the development of information technology, which enables the utilization of IoT-based science (*Internet of Things*) and artificial intelligence (*Artificial Intelligence*) in people's daily lives with the aim of improving the convenience of human life. [13]

The development of the *society* 5.0 era raises a number of challenges that need to be faced. One of them is skills in the use of technology, where every individual and organization must have the ability in this regard. In addition, cybercrime has grown rapidly and not only attacks individuals, but can also threaten the integrity and credibility of organizations or even countries. Today, almost every job, be it an individual or an organization, involves the use of technology connected to cyberspace. Public and private data can be accessed by anyone, anytime, and anywhere. All of this really depends on how each individual is able to manage and protect the privacy of their personal data.

The term *society* 5.0 era was first introduced by Japan. This era is aimed at creating a super-smart society, where information technology becomes a very important necessity for all elements of society.[14] The era of *society* 5.0 is faced with various challenges, such as cyber attacks or threats in the digital world that can jeopardize security aspects in various forms.[15] One example of technological threats includes various actions such as *phishing* or fraud attempts, attempts to trick or deceive system users, DDoS (*Distributed Denial of Service*) attacks in the cyber world, attempts to access illegal sites, and utilization of the *dark web* for illegal activities that can harm certain individuals or groups.

This of course requires serious handling. Because with the massive development of technology, it is certainly a challenge as well as a threat to all elements, both from the elements of society and government.[16] Therefore, the

[12] Decky Hendarsyah. "E-commerce di Era Industri 4.0 dan *Society* 5.0." *Iqtishaduna: Scientific Journal of Our Economy* 8.2 (2019): 171-184. https://doi.org/10.46367/iqtishaduna.v8i2.170, p. 176.

[13] Dita Septasari. "*Cyber Security and The Challenge of Society* 5.0 *Era in* Indonesia". *Aisyah Journal of Informatics and Electrical Engineering* 5 No. 2 (2023): 227-233. https://doi.org/10.30604/jti.v5i2.231, pp 229-230.

[14] Afiffudin Al Hadiq. "Epistimologi Pendidikan Karakter Islami di Era Society 5.0." *Social Science Academic* 1.1 (2023): 185-192. https://doi.org/10.37680/ssa.v1i1.3357 , p. 178.

[15] Hildawati, et al. *Literasi Digital: Membangun Wawasan Cerdas dalam Era Digital terkini,* (Yogyakarta: PT. Green Pustaka Indonesia, 2024), p 182.

[16] Henike Primawanti and Sidik Pangestu. "Diplomasi Siber Indonesia Dalam Meningkatkan Keamanan Siber Melalui Association of South East Asian Nation (Asean) Regional Forum." *Global Mind* 2.2 (2020): 1-15. https://doi.org/10.53675/jgm.v2i2.89, p. 3.

strategy of law enforcers in responding to *cyber crime* along with the sophistication of technology is needed. The following are some of the strategies carried out by the Special Criminal Investigation Unit of the Yogyakarta Special Region Police as an effort to respond to the transformation of the era of *society* 5.0 summarized from an interview with Iptu Robertus Wuriyan Kristama, S.H. as the Temporary Assistant Unit 2 Subdit V Siber Polda DIY:

a) Technical Capability Enhancement: Police departments recognize the importance of having personnel skilled in information technology. They provide continuous training to their officers, including investigators and cyber analysts, to understand technological developments and tactics used by cyber criminals. This helps them in identifying and tracking down increasingly proficient *online* fraudsters.
b) Cooperation with External Entities: The police work with internet service providers (ISPs), financial institutions, and other authorities. This collaboration allows them to access data and information relevant to the investigation. With this cross-sector cooperation, they can be more effective in collecting digital evidence and tracking down perpetrators.
c) Community Education: The police are active in educating the public about *online* fraud risks and preventive measures. They conduct awareness campaigns and provide information to the public so that they can recognize the signs of *online* fraud and report suspicious activity.
d) Utilization of Technology: The police use technology to support their efforts in uncovering *online* fraud cases. They can utilize sophisticated software and equipment for data analysis and investigation.
e) Digital Investigation: Investigators are equipped with powerful digital investigation capabilities. They can track IP addresses, digital footprints, and collect electronic evidence that can be used in court.
f) Strong Laws and Regulations: The police ensure that they operate in accordance with applicable laws and regulations in uncovering *online* fraud cases. They collaborate with legal authorities to ensure due process.

By implementing this strategy, the Yogyakarta Police are committed to tackling *online* fraud more effectively in the era of *society* 5.0, which is characterized by rapid technological change. This effort aims to maintain public safety in the ever-evolving digital world.

JSH
Supremasi Hukum: Jurnal Penelitian Hukum
P-ISSN: 1693-766X ; E-ISSN: 2579-4663, Vol. 33, No 2, Agustus 2024, 124-136
https://ejournal.unib.ac.id/supremasihukum/index
DOI: https://doi.org/10.33369/jsh.33.2.124-136

Conclusion

The Special Region of Yogyakarta is one of the provinces that is vulnerable to crime, including *cyber crime*. This can be seen based on the diagram of mayantara (*cyber crime*) cases by the Yogyakarta Special Police from 2019 to 2022. *Online* fraud is the most prevalent type of *cybercrime* reported to the Yogyakarta Police. There are factors that cause individuals to commit *online* fraud crimes, such as economic factors, the environment, the ease of committing *online* crimes, and the minimal risk of being caught by law enforcement officials. The obstacles in uncovering *online* fraud crime cases include internal factors, such as limited human resources and technological facilities, as well as external factors, such as falsification of perpetrator accounts and data privacy issues. To overcome *online* fraud crimes in the era of *society* 5.0, the Yogyakarta Special Police has several strategies such as improving the technical capabilities of officers and collaborating with various parties, including *providers* and financial institutions. Increasing awareness and digital literacy in the community is also key in reducing *online* fraud cases.

References

Al Hadiq, Afiffudin. "Epistimologi Pendidikan Karakter Islami di Era *Society* 5.0." Social Science Academic 1.1 (2023): 185-192. https://doi.org/10.37680/ssa.v1i1.3357

Habibi, M. R., & Liviani, I. (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://www.academia.edu/download/95670346/480663504.pdf.

Hapsari, Rian Dwi dan Kuncoro Galih Pambayun. "Ancaman *cybercrime* di indonesia: Sebuah tinjauan pustaka sistematis." *Jurnal Konstituen* 5.1 (2023): 1-17. https://doi.org/10.33701/jk.v5i1.3208.

Hapsoro, W., Aidjili, M., & Budijanto, H. A. (2022). “Yurisdiksi Hukum Pidana dalam Pembatasan Informasi Hoaks Terkait dengan Kejahatan *Cybercrime*”. *Ristek: Jurnal Riset, Inovasi dan Teknologi Kabupaten Batang, 7(1)*, 11-19. https://doi.org/10.55686/ristek.v7i1.124

Hendarsyah, D. (2019). “E-commerce di Era Industri 4.0 dan *Society* 5.0”. *Iqtishaduna: Jurnal Ilmiah Ekonomi Kita*, 8 (2), 171-184. https://doi.org/10.46367/iqtishaduna.v8i2.170

Hildawati, et al. *Literasi Digital: Membangun Wawasan Cerdas dalam Era Digital terkini*. (Yogyakarta: PT. Green Pustaka Indonesia, 2024).

Komalasari, I. (2021). "Peran Penyidik dalam Mengungkap Tindak Pidana Penipuan Transaksi Jual Beli *Online* melalui Media Internet *E-Commerce*". *Jurnal Hukum Pidana Indonesia,* 3 (2), 201-210. https://journal.ilininstitute.com/index.php/IJoCL/article/view/1385

Pramesti, Y. A., & Rosnawati, E. (2023). "Tindak Pidana Penipuan dalam Media Jual Beli *Online*". *Web of Scientist: International Scientific Research Journal (WoS)*, 2(4). https://doi.org/10.47134/webofscientist.v2i4.8

Prasetiyo dan Mukhtar Zuhdy. "Penegakan Hukum oleh Aparat Penyidik *Cyber Crime* dalam Kejahatan Dunia Maya (*Cyber Crime*) di Wilayah Hukum Polda DIY." *Indonesian Journal of Criminal Law and Criminology (IJCLC)* 1.2 (2020): 79-88. 10.18196/ijclc.v1i2.9611.

Primawanti, H., & Pangestu, S. (2020). "Diplomasi Siber Indonesia dalam Meningkatkan Keamanan Siber Melalui Association of South East Asian Nation (Asean) Regional Forum". *Global Mind*, 2(2), 1-15. https://doi.org/10.53675/jgm.v2i2.89

Puspitasari, Syalaisha Amani. "Tinjauan Yuridis Eksploitasi Manusia dalam Fenomena Mandi Lumpur." *JISIP* (*Jurnal Ilmu Sosial dan Pendidikan*) 7.3 (2023): 2840-2846. http://dx.doi.org/10.58258/jisip.v7i3.5349.

Ramli, Ahmad M., et al. "Pelindungan Kekayaan Intelektual dalam Pemanfaatan Teknologi Informasi di Saat Covid-19." *Jurnal Penelitian Hukum De Jure* 21.1 (2021): 45-58. http://dx.doi.org/10.30641/dejure.2021.V21.045-058.

Sanggo, P. A., & Lukitasari, D. (2014). "Pertanggungjawaban Pidana Pelaku Penipuan Arisan *Online* Ditinjau Dari Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik". *Recidive: Jurnal Hukum Pidana dan Penanggulangan Kejahatan,* *3*(2), 221-230. https://doi.org/10.20961/recidive.v3i2.40524

Septasari, D. (2023). "Keamanan Siber dan Tantangan Era Masyarakat 5.0 di Indonesia". *Aisyah Journal of Informatics and Electrical Engineering (AJIEE), 5* (2), 227-233. https://doi.org/10.30604/jti.v5i2.231

Singgi, I. G. A. S. K., Suryawan, I. G. B., & Sugiartha, I. N. G. (2020). "Penegakan Hukum terhadap Tindak Pidana Peretasan sebagai Bentuk Kejahatan Mayantara (*Cyber Crime*)". *Jurnal Konstruksi Hukum, 1*(2), 334-339. https://doi.org/10.22225/jkh.1.2.2553.334-339

Yunita, F. (2023). "Aspek Hukum Penggunaan Media Sosial Berbasis Internet". *Jurnal Notarius, 2*(1), https://jurnal.umsu.ac.id/index.php/notarius/article/view/15899.