Pakistan Journal of Criminology
Vol. 16, No. 02, April—June 2024 (1061-1080)

Virtual Police: Guardians of Security and Consumer Protection in the Era of Electronic Information and Transactions

Yenny Aman Serah[1], Zico Junius Fernando[2] &
Temmy Hastian[3]

Abstract

In the digital era, cybersecurity is an important issue that requires a comprehensive and multi-dimensional approach. Virtual Police, as an initiative of POLRI, plays a vital role in combating cybercrime and maintaining digital security in Indonesia. However, challenges and obstacles related to human rights, privacy, and consumer protection must be considered. The results of this study relate to the implementation of Virtual Police must be carried out by considering the values of Pancasila and the 1945 Constitution of the Republic of Indonesia, as well as regulations such as the ITE Law and the Consumer Protection Law. In addition, increasing public awareness and education about cybersecurity is essential. Cooperation between the government, the private sector, and the community is vital in achieving a safe and inclusive digital environment. By doing so, we can ensure that everyone can enjoy the benefits of digital technology without fear of cybersecurity threats. Despite progress, Indonesia must continue strengthening cybersecurity by improving technology, public education, and cybersecurity. Despite this progress, Indonesia needs to continue to strengthen cybersecurity by updating technology and public education and always respecting and protecting the rights and privacy of internet users.

Keywords: Cybersecurity; Virtual Police; Human Rights; Consumer Protection; Indonesia.

Introduction

In the current era of information and electronic transactions, digital technology has changed various aspects of human life (Ngafifi, 2014). The way humans communicate, work, learn, and even shop has changed dramatically and has become more accessible thanks to the Internet (Allagui, 2017). Social interactions previously carried out face-to-face are now being replaced by digital communication. Working and studying remotely has become commonplace, with various supporting devices and applications (Hidayanto et al., 2015). Online shopping has become an alternative many people prefer because of its convenience (Putri et al., 2021). However, this

[1]Fakultas Hukum, Universitas Panca Bhakti Pontianak, Indonesia. yenny.upb@gmail.com
[2]Fakultas Hukum, Universitas Bengkulu, Indonesia. zjfernando@unib.ac.id
[3]Fakultas Hukum, Universitas Panca Bhakti Pontianak, Indonesia. temmy.hastian@upb.ac.id

progress has come with challenges. Cybercrime, which includes everything from credit card fraud to attacks on critical infrastructure, is a serious global threat (Gani, 2014). In this context, the role of the virtual police becomes essential. Virtual police are a particular division or unit in law enforcement that focuses on cybercrime. They deal with various types of crime, including, but not limited to, online fraud, malware attacks, identity theft, and attacks on critical infrastructure. Virtual policing requires specialized knowledge and skills, including a deep understanding of information and communications technology, digital forensics, and cyber law (Yuli Nurhanisah, 2023).

According to information released by the Patrolisiber.id site, there were 15,152 cybercrime complaints recorded from January to September 2021, with a total loss of 3.88 trillion. Online fraud is the type of crime most frequently reported by the public, with a total of 4,601 cases. Apart from fraud, other crimes that are often reported are threats and insults, with the number of complaints being 3,101 cases. Reports of cybercrime in the form of extortion were also relatively high, namely 1,606 cases. Meanwhile, cases of hoaxes and pornographic content reached 360 and 333 cases, respectively. The public also reports cybercrimes, such as document falsification, provocation or incitement, religious blasphemy, prostitution, etc. (Vika Azkiya Dihni, 2021). Cybercrime has a significant impact on society and the economy. Companies lose millions, even billions, of dollars every year to cybercrime (Oates, 2001). Besides that, consumers also feel unsafe when carrying out online transactions for fear of becoming fraud or data theft victims. This has created an urgent need for better protection against cybercrime, and this is where virtual police come in. Virtual police have a vital role in maintaining consumer security and protection. They do this in various ways, including law enforcement, cybercrime investigations, public education about cybercrime and how to prevent it, and collaboration with third parties, such as technology companies, to improve cybersecurity (Alifia Astika, 2021). Cyber security specialist Kaspersky has just released a report showing tens of millions of online crime threats targeting internet users in Indonesia. In more detail, Kaspersky recorded that around 11.8 million, or almost 12 million, online crime threats threatened website users in Indonesia during the first three months of 2022 (first quarter), which started from January to March. The number of threats increased by 22 percent compared to the same period in the previous year. At that time, online threats aimed at Indonesian users "only" reached around 9.6 million cases (Bill Clinten, 2022).

Virtual police face various, quite complex challenges. Along with technological developments, cybercrime is becoming more advanced and complicated (Arisandy, 2021). This requires the virtual police to continue to adapt and learn to keep up with this progress. Another obstacle is that rules and laws often have yet to adapt to

technological developments, which can complicate law enforcement. Apart from that, there are also problems related to resources, training, and availability of tools for the virtual police.

Despite facing various challenges, virtual police must continue adapting and developing to provide appropriate protection in today's digital era. This effort involves continuous and up-to-date training, additional resources and tools, and broader collaboration with related parties, such as technology companies and international organizations. The success of virtual police also relies heavily on cooperation from communities and businesses. The public needs to be educated about cybercrime and how to protect themselves. Businesses, especially those in the technology sector, are essential in maintaining data security and protecting their consumers. Apart from that, the role of the virtual police is broader than law enforcement and investigations. They also have an essential role in educating the public about cyber security. This can be through educational campaigns, workshops, or training for the general public or specific groups. By increasing public awareness and understanding of cybercrime and how to prevent it, we can all play a role in creating a safer digital environment. Furthermore, there needs to be more extraordinary efforts for international cooperation in fighting cybercrime.

Cybercrime is a global threat, and a global approach is needed to combat it. This can be through cooperation between countries in law enforcement, sharing information and intelligence, and harmonizing cyber laws and regulations (Orlov, 2012). Overall, the information and electronic transactions era has opened up new opportunities and threats (Gulo et al., 2021). Virtual police, with their role in maintaining security and consumer protection, have an essential role in keeping this digital era safe and trustworthy. Despite the challenges, with the proper training, sufficient resources, and broad collaboration, virtual police can continue to protect the public in the digital world. Along with technological advances and increasingly rapid developments in the digital world, the existence and role of virtual police will continue to be relevant and even become increasingly important. Existing challenges should be considered as opportunities to continue learning, adapting, and developing better strategies to combat cybercrime. Virtual police are the front guard in our defense against cybercrime, and will always be the guardians of security and consumer protection in the era of information and electronic transactions.

Researchers use normative legal research methods to understand this research topic or research focusing on books and other data sources. It involves reading and analyzing legal texts and other documents to understand how the law works in rigorous situations. In this way, we can gather the information and insight we need to understand and provide advice on the legal issues we face (Soekanto & Mamudji, 2001). The research entitled "Virtual Police: Security Guard and Consumer

Protection in the Information and Electronic Transaction Era" collected various types of legal material. This material includes primary legal sources, such as laws and regulations; secondary legal sources, such as journals and books; and tertiary legal sources, such as legal dictionaries (Agusalim et al, 2022). To find solutions to the issues studied, this research uses various approaches. First is the statutory approach, which means examining and analyzing relevant laws. Second is a comparative approach, which compares how this issue is handled in various jurisdictions or situations. Third is the conceptual approach, which makes it possible to explore the theoretical or conceptual understanding of the problem the futuristic approach, which looks ahead to predict how this issue might develop (Peter Mahmud Marzuki, 2005). The type of research carried out in this study is descriptive-prescriptive. This means that this research explains or describes existing legal phenomena or issues (descriptive) and provides recommendations or suggestions about what should happen or how the issue should be handled (prescriptive) (Herlambang et al, 2022). In this research, a literature review was used as a method for collecting data. This involves searching for and reviewing relevant written sources such as legislation, books, official government documents, and academic publications. Furthermore, this research uses a content analysis method, namely a systematic approach to interpreting and understanding the information contained in these sources (Putra et al., 2023).

Analysis and Discussion

Getting to Know Virtual Police: Definition, Legal Basis, and Polemics

Cybercrime is increasingly becoming a very serious global issue in this digital era. This crime affects not only individuals or organizations but also countries (Clough, 2010). To fight cybercrime and maintain consumer security and protection in the era of information and electronic transactions, the Indonesian National Police (POLRI) launched a new unit called "Virtual Police" on February 23, 2021. Virtual Police, or Cyber World Police, is an initiative of National Police Chief General Listyo Sigit Prabowo in response to President Joko Widodo's direction for the police to be careful in implementing the articles in the Information and Electronic Transactions (ITE) La (Tsarina Maharani, 2021).

Implementing Virtual Police duties is referred to in the National Police Chief's Circular (SE) number SE/2/11/2021 concerning Ethical Cultural Awareness to Create a Clean, Healthy, and Productive Indonesian Digital Space. The Virtual Police aim to monitor, educate, provide warnings, and protect the public from potential cybercrimes. This Virtual Police activity monitors social media and will report to superiors if it finds content uploaded that has the potential to violate the ITE Law (Tsarina Maharani, 2021). Content reported by Virtual Police will be reviewed by criminal experts, language experts, and ITE experts to determine whether the content

has the potential to violate the law or not. The content will be handed over to the Director of Cyber Crime or an appointed official if a potential criminal act is found. Once approval is given, Virtual Police will alert the account owner. If the account owner does not respond to the warning and removes the problematic content, Virtual Police will send another notification. Suppose the second notification is also ignored, and a party feels aggrieved and makes a report. In that case, a legal process will begin, where the National Police will prioritize mediation between the reporter and the reported party (Tsarina Maharani, 2021).

In a broader context, the presence of the Virtual Police manifests the challenges law and law enforcement face in the digital era. Law must adapt to technological developments and the new challenges posed by this technology (Riswandi, 2016). Apart from that, the law must also provide adequate protection for the public in interacting and carrying out transactions in cyberspace (Ibrahim, 2003). In particular, law enforcement in cyberspace poses its challenges. On the one hand, law enforcement must be able to prevent and deal with cybercrime. On the other hand, law enforcement must also protect individual rights and freedoms in cyberspace (Cahyadi, 2016). In this case, Virtual Police tries to achieve this balance. However, this does not mean that these challenges can be overcome easily. As can be seen from the various responses to the presence of the Virtual Police, there are still different views and concerns about how law enforcement in cyberspace should be carried out. Therefore, there needs to be continuous dialogue and discussion between the parties involved, including the government, law enforcement, legal and technology experts, and the wider community.

The following is a description of the Virtual Police's work process in monitoring and enforcing the law on social media (Rifan Aditya, 2021).

1. The first stage is to monitor and provide warnings to social media accounts that are indicated to be sharing content that violates the law. Before issuing a warning, Virtual Police considers the opinions of experts;
2. If an account publishes posts or images that are suspected of violating criminal law, Virtual Police officers will store the content. The content will then be consulted with criminal, language, and ITE experts to get a more accurate assessment;
3. If the experts decide the content contains elements of a criminal offense, the next step is to submit the case to the cyber director;
4. After that, an official warning from the Virtual Police will be sent to the account owner. This warning is sent via direct message;
5. Direct messages are used to send this warning to maintain the confidentiality of communications between the Virtual Police and the

account owner. This is intended so that other parties do not know the warning.

Through this mechanism, the Virtual Police seeks to monitor and prevent cybercrime effectively while maintaining the privacy and rights of social media users. In practice, the Virtual Police must comply with and comply with several important laws and regulations in Indonesia, including:

1. Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE) as amended by Law No. 19 of 2016
   The ITE Law is the primary law that regulates electronic information and transactions, including cybercrimes. Virtual Police must comply with this Law in their duties and functions. For example, they may not carry out actions that violate the provisions of this Law, such as violating the privacy of internet users.
2. Law Number 39 of 1999 concerning Human Rights
   This law regulates human rights in Indonesia and is a reference for all institutions in Indonesia, including the Virtual Police, in carrying out their duties and functions. Virtual Police must always respect and protect human rights in all their operations.
3. Law Number 8 of 1999 concerning Consumer Protection
   This law regulates consumer rights and service provider obligations. Virtual Police, as a cyber security service provider, must protect consumer rights, such as the right to comfort, security, and personal data protection.
4. Law of the Republic of Indonesia Number 2 of 2002 concerning the State Police of the Republic of Indonesia.
   It is the leading legal umbrella for all activities of the Republic of Indonesia Police, including the Virtual Police. Some critical articles in this law that are relevant to Virtual Police include:
   a. Article 4: This article defines the objectives of the Indonesian National Police, namely protecting, serving the community, and enforcing the law. This includes protection and service in cyberspace by the Virtual Police.
   b. Article 14: This article gives the National Police the authority to conduct inquiries and investigations into all criminal acts, including in cyberspace, which are the duties of the Virtual Police.
   c. Article 18: This article explains that in carrying out its duties, the National Police must respect human rights, including in Virtual Police activities.

   d. Articles 28 and 29: These articles emphasize that members of the National Police must uphold the police code of ethics and professionalism in carrying out their duties, including in carrying out their duties as Virtual Police.
5. National Police Chief Circular No. SE/2/II/2021 concerning Ethical Cultural Awareness to Create a Clean, Healthy, and Productive Indonesian Digital Space. It is a guideline for all members of the National Police, including the Virtual Police, to create a positive and safe digital environment for the entire community.

Readiness and Capability of Virtual Police in Facing Cyber Crime

Cybercrime has become an issue that has received serious attention in the last few decades, in line with the increasing use of the internet and digital technology (Wall, 2008). These crimes cover a wide range of illegal activities carried out through computer networks and systems, including fraud, identity theft, cyber-attacks on critical infrastructure, and various forms of personal information and data misuse (Arwana, 2022). In Indonesia, the Indonesian National Police (POLRI) has introduced a Virtual Police unit to respond to this challenge. However, an important question that arises is the extent of the Virtual Police's readiness and capability in dealing with this cybercrime.

First, regarding readiness, the Virtual Police has been equipped with various legal and regulatory tools to carry out its duties. Since its activation on February 23 2021, Virtual Police has operated based on the National Police Chief's Circular (SE) number SE/2/11/2021 concerning Ethical Cultural Awareness to Create a Clean, Healthy, and Productive Indonesian Digital Space (Maria Helen Oktavia, 2021). This SE functions as operational guidance for the Virtual Police in carrying out their preemptive and preventive duties, including monitoring, educating, providing warnings, and preventing the public from potential cybercrimes.

Second, regarding capabilities, the Virtual Police has the knowledge and technical skills to deal with cybercrime. This includes the ability to monitor activity on social media, analyze data, and identify content potentially violating the ITE Law. Suppose Virtual Police officers find content that can potentially violate the law. In that case, they will report it to superiors and ask for expert opinions, such as criminal, language, and ITE experts. The content will be submitted to the Director of Cyber Crime or an appointed official if there is a potential criminal act (Indonesian National Police, 2021). However, even though it is equipped with legal tools and technical capabilities, the readiness and capabilities of the Virtual Police still need to be improved. One of the main challenges is how to identify and deal with increasingly complex and sophisticated cybercrime. Cybercrimes often involve perpetrators and

victims in different locations and can even be in different countries. Cybercriminals often use sophisticated techniques to hide their identities and activities, making law enforcement increasingly difficult.

To overcome these challenges, Virtual Police need to strengthen their capabilities in various areas. First, they must increase their technical capacity in information technology and cybersecurity. This includes knowledge and skills in dealing with various cyber-attacks, identifying and tracking perpetrators, and analyzing obtained digital evidence. They must also understand the latest technological and cybercrime trends to adapt their methods and strategies according to these changes. Second, they must also increase cooperation with various parties at home and abroad. Cybercrime is a global problem that requires a global solution. Therefore, Virtual Police needs to collaborate with law enforcement from other countries, as well as international organizations involved in the field of cyber security. In addition, cooperation with the private sector, such as internet service providers and technology companies, is also essential, considering that they have access to data and information that can assist in cybercrime investigations. Third, the Virtual Police also needs to strengthen laws and regulations related to cybercrime. Even though Indonesia already has an ITE Law, many aspects of cybercrime still need to be regulated in law. For example, the law needs to be more apparent in defining what is considered a cybercrime, determining appropriate penalties for different types of cybercrime, and establishing procedures to be followed when collecting and using digital evidence in legal proceedings. Fourth, educating the public is also very important. Many cybercrimes occur due to a lack of public knowledge and awareness about the risks and how to protect themselves from cyber-attacks. Therefore, Virtual Police needs to increase public awareness about cyber security, for example, through educational campaigns or collaboration with educational institutions.

Overall, while Virtual Police has made significant strides in confronting cybercrime, a lot of work still needs to be done. With increased readiness and capability and strong collaboration with various parties, Virtual Police can become effective security guards and consumer protection in the information and electronic transactions era. Even though the challenges faced are significant, with strong commitment and strategic steps, the Virtual Police has the potential to become an essential force in fighting cybercrime and protecting Indonesian society in cyberspace.

Finally, improving the quality of infrastructure and technological equipment is also very important in increasing the capabilities of the Virtual Police. To deal with various types of increasingly sophisticated cyber-attacks, Virtual Police must have adequate technological infrastructure, such as secure data centers, the latest cyber

security software and hardware, and tools for capturing and analyzing digital evidence. This infrastructure also needs to be maintained and updated regularly to keep up with the latest technological developments. Improving the quality of human resources is also an essential part of preparing and improving Virtual Police capabilities. This includes improving the quality of education and training for Virtual Police members at home and abroad. For example, they can take training or specialization courses on cybersecurity, digital forensics, or data analysis. In addition, the recruitment system also needs to be improved to attract individuals with skills and knowledge relevant to cyber security. As part of efforts to improve their capabilities, Virtual Police also need to implement a proactive approach in dealing with cybercrime. In addition to responding to and dealing with cybercrime after it occurs, they also need to prevent cybercrime by monitoring suspicious activity in cyberspace, identifying and tracking potential perpetrators, and carrying out early intervention to prevent attacks. Apart from that, a community-oriented approach also needs to be implemented by the Virtual Police. This means that they not only focus on law enforcement but also on efforts to protect and support society, including victims of cybercrime. For example, they can provide support and assistance to victims of cybercrime, such as technical, psychological, and legal assistance. They can also work with communities and civil society organizations to increase public awareness and knowledge about cyber security. With these efforts, the Virtual Police can increase its readiness and capabilities in dealing with cybercrime, thereby protecting the Indonesian people from the threats and risks posed by cybercrime. Even though the challenges faced are significant, with solid efforts and commitment, the Virtual Police can become an essential force in fighting cybercrime and protecting Indonesian society in cyberspace.

Virtual Police, or cyber police, is not a phenomenon unique to Indonesia. Several other countries have also implemented this concept in some form or capacity, including the United Kingdom, the United States, and Singapore.

1. English
   The UK has a unit known as the National Crime Agency's National Cyber Crime Unit (NCCU).(Saunders, 2017) NCCU is responsible for combating the threat of cybercrime at national and international levels. They work closely with several other organizations at home and abroad, including local police, MI5, GCHQ, and international organizations such as Europol. The advantage of NCCU is its ability to operate nationally and internationally and close collaboration with other institutions in preventing and dealing with cybercrime.
2. United States of America

The FBI in the United States has a particular unit known as the Cyber Division.(Fox, 2015) The Cyber Division is responsible for confronting cybercrime threats and coordinating cybercrime investigations nationwide. They have a Cyber Action Team (CAT), a rapid response unit that can be deployed anytime and anywhere worldwide to respond to significant cybercrime incidents.(Federal Bureau of Investigation, 2023) The advantages of the FBI's Cyber Division are their speed of response and broad operational capabilities.

3. Singapore
   Singapore has a Technology Crime Forensic Branch under the Criminal Investigation Department (Criminal Investigation Department).(Singapore Police Force, 2023) Singapore has a strong focus on digital forensics and cybercrime. Their strengths are a strong focus on law enforcement and advanced forensic capabilities.

Although each of these models differs in structure and focus, they all have the same goal of protecting society and the country's infrastructure from the threat of cybercrime. The Virtual Police concept in Indonesia can learn from these models regarding organizational structure, inter-agency partnerships, and law enforcement to increase its effectiveness in preventing and dealing with cybercrime. Based on the experience and practice of countries that have implemented virtual police or cyber police models, Indonesia can learn the following essential things:

1. Collaboration between Institutions
   As seen from the examples of the United Kingdom and the United States, cooperation between agencies is essential in preventing and responding to cybercrime. Indonesia can learn to strengthen cooperation between the Virtual Police and other institutions, be they government institutions, the private sector, or international organizations working in cyber security.
2. Specialization and Education
   Singapore shows how important it is to specialize in dealing with cybercrime, especially in digital forensics. Indonesia can strengthen its capabilities in this field by increasing education and training for Virtual Police members.
3. Quick response
   The example of the United States shows how important it is to have a fast response in dealing with cybercrime. Indonesia could consider establishing a unit similar to the Cyber Action Team (CAT) at the FBI to handle major cybercrime incidents quickly and effectively.
4. Society and Education

Apart from that, it is also essential to involve the public and provide education about cyber security. An educated public will be more aware of potential threats, which can be essential to preventing cybercrime.

5. Compliance with human rights
   In its implementation, Virtual Police must also pay attention to Human Rights (HAM) aspects, ensuring that law enforcement efforts do not violate citizens' privacy and digital rights.

Applying and learning from the experiences of other countries will undoubtedly help Virtual Police Indonesia improve its capabilities and quality of work. However, it is essential to remember that each country has its unique context and challenges, so the solutions implemented must be adapted to the needs and conditions in Indonesia.

Public Awareness and Education About Cyber Security

Increasing public awareness and education about cyber security is a challenge and an urgent need in this digital era (Angkasa & Windiasih, 2022). Cybercrime, ranging from online fraud identity hijacking to attacks on critical infrastructure, poses a real threat to individuals and society (Supanto, 2016). Therefore, the role of society in maintaining cyber security must be addressed, and increasing awareness and education are essential in mitigating these risks and threats. First, society must understand that cyber security is not the sole responsibility of the government or the private sector but is a shared responsibility (Azra Heriana et al., 2022). Cybersecurity involves everyone connected to the internet, from individual users to corporations to government institutions. Why is that? This is because inappropriate or unsafe access and use of technology and information by individual users can become an entry point for cybercriminals. In other words, users' ignorance or negligence in keeping their information secure can harm themselves and others. So, all parties need to correctly understand how to safeguard and protect personal data and information, as well as the systems and networks they use. To achieve this, cybersecurity education and training is critical. This education must start early and become part of the primary and secondary education curriculum. Students should be taught the basics of cybersecurity, such as the importance of using strong and unique passwords, identifying and avoiding phishing and other scams, updating software and operating systems, and more. Cybersecurity training and workshops should also be carried out for adult and corporate users to ensure they are constantly updated with the latest threats and security solutions. Apart from formal education, the government and related organizations must also carry out cyber security campaigns and outreach widely and regularly. The public must understand that cyber security is not optional but must. This campaign can be carried out through various media, both offline and

online, and must be able to reach all levels of society. Of course, increasing awareness and education must be supported by adequate policies and regulations from the government. Regulations must provide adequate protection for the public from potential cybercrime. Still, they must also be balanced and not limit the rights and freedoms of the public in using and accessing technology and information.

Finally, it is essential to remember that cybercrime is a global threat that requires cooperation and coordination between countries around the world. Indonesia, for example, must actively participate and collaborate in international forums and initiatives related to cyber security. In this way, Indonesia can learn and adopt best practices from other countries and share its own experiences and insights. The active role of society in maintaining cyber security cannot be ignored. There are several practical steps that individuals can take to protect themselves and their data from cyber threats. Among other things, always be alert to suspicious emails or messages, never click on links or download files from unknown or untrusted sources, and constantly update software and applications to the latest versions. It is also essential to maintain hardware security. Protect devices such as computers, laptops, or smartphones from unauthorized physical access. Use strong, unique passwords for every account and online service you use. And use two-factor authentication services whenever available. However, it is essential to remember that public education and awareness about cyber security is not the sole solution to the problem of cybercrime. This must be accompanied by increased cybersecurity capabilities and resources at the national level and strong cooperation between the government, the private sector, and civil society. More than that, there is also a need for clear and firm laws and regulations to take action against cybercriminals. Public awareness and education about cyber security is an integral part of a broader solution in facing the challenge of cybercrime. Through education and awareness, communities can actively protect themselves and their communities from cyber threats. Meanwhile, we can create a safer and more secure digital environment through good cooperation between all parties involved.

In looking at the implementation of Virtual Police in Indonesia, we can refer to the country's two main constitutional foundations, namely the 1945 Constitution of the Republic of Indonesia and Pancasila. According to the 1945 Constitution, Article 28F, everyone has the right to communicate and obtain information to develop their personality and social environment and has the right to search for, obtain, own, store, process, and convey information using all types of available channels. However, this right must be balanced with the responsibility not to misuse it to commit criminal acts, such as spreading hate speech or false information. From a Pancasila perspective, the implementation of Virtual Police also needs to consider the noble values contained in the 2nd principle, Just and Civilized Humanity, and the 5th

principle, Social Justice for all Indonesian People. The 2nd principle, Just and Civilized Humanity, emphasizes respecting human rights and dignity. In this context, the Virtual Police must operate in a manner that respects individual rights and privacy and does not discriminate in performing its duties. The 5th principle, Social Justice for all Indonesian People, means that justice must be the main principle in applying this technology. Virtual Police must be used to ensure justice for everyone, not just as a surveillance tool that creates feelings of fear or insecurity (Asmah et al, 2023). Overall, in the context of the 1945 Constitution of the Republic of Indonesia and Pancasila, Virtual Police must be used as a tool that supports the principles of justice, humanity, and democracy, not as a tool to curb freedom of speech or violate human rights. It is essential to balance the need for law enforcement and protecting individual rights and freedoms. This requires strong cooperation between governments, communities, and the private sector, a people-centered approach, and respect for democratic values and social justice. In line with the values of Pancasila and the 1945 Constitution of the Republic of Indonesia, the implementation of Virtual Police must always be oriented towards improving the community's quality of life and protecting human rights.

Viewing Virtual Police implementation from a consumer protection perspective is also essential. According to Law No. 8 of 1999 concerning Consumer Protection, consumers have the right to comfort, security, and safety when using a product or service. In this context, as consumers of digital services, internet users have the right to a safe and comfortable virtual environment. The Virtual Police, in its functions and duties, should aim to protect these consumers. For example, monitoring and dealing with hate speech, spreading false information, online fraud, and other cybercrimes could harm consumers. However, consumer protection also means that consumers' privacy and personal data must be protected. According to Law No. 11 of 2008 concerning Information and Electronic Transactions (ITE), everyone has the right to protect their data (Setyaningrum et al., 2022). Virtual Police must ensure that in carrying out their duties, there is no violation of the right to privacy and protection of personal data. In addition, it is also essential to ensure that consumers receive clear and transparent information about how Virtual Police works and how their data is used. This transparency is integral to consumer protection and is essential for building public trust in the Virtual Police. So, from a consumer protection perspective, the implementation of Virtual Police must consider the protection and convenience of internet users while ensuring their privacy and personal data remain safe. This will require cooperation and coordination between various parties, including governments, internet service providers, and human rights organizations.

Information and Electronic Transactions Law (UU ITE) no. 11 of 2008 and its revision, Law no. 19 of 2016, is a necessary regulation for implementing Virtual

Police in Indonesia. One of the main objectives of the ITE Law is to create a safe and responsible digital environment (Pan Dhadha et al., 2021). In this case, Virtual Police can be seen as a tool that helps realize this goal by carrying out supervision and law enforcement in cyberspace. The ITE Law regulates various violations in cyberspace, such as the spread of false and misleading information, insults and slander, and misuse of personal data (Safitri, 2018). In carrying out its duties, the Virtual Police must refer to this regulation to take action against violations. However, the implementation of Virtual Police must also pay attention to aspects of human rights protection regulated in the ITE Law. Article 26 of the ITE Law confirms that everyone has the right to security and protection of personal privacy, family, respect, good name, and other personal rights when carrying out electronic transactions and gaining access to legal mechanisms if these rights are violated (Rumlus & Hartadi, 2020). This means that in carrying out its duties, the Virtual Police must not carry out actions that violate internet users' privacy and personal rights. Therefore, the government and related parties need to ensure that Virtual Police operations are carried out in a manner that aligns with the ITE Law, especially in protecting human rights. It is important to note that although the ITE Law provides a legal framework for law enforcement in cyberspace, there is still criticism and controversy regarding its implementation, particularly regarding freedom of expression and human rights. Therefore, the implementation of the ITE Law and the implementation of Virtual Police must constantly be reviewed and adjusted to ensure a balance between the needs of law enforcement and the protection of human rights.

Challenges, Obstacles, and Human Rights Issues Related to Virtual Police in Indonesia

Virtual Police, an initiative by the Indonesian government to monitor and regulate behavior in cyberspace, raises various challenges, obstacles, and human rights issues. Even though it aims to combat criminal acts, hate speech, and the spread of false information, implementing this technology requires special attention regarding freedom of speech, privacy, and personal data protection. First, the public must see the main challenges in implementing Virtual Police. On the one hand, this challenge is related to the need for more digital literacy among Indonesian citizens. Even though internet penetration in Indonesia is increasing rapidly, understanding and knowledge about digital ethics, online privacy, and awareness of the potential misuse of personal data is still lacking. This leaves many users vulnerable to various security risks and abuse in cyberspace (Budi et al., 2021). Apart from that, the "digital divide" or digital gap between people is also a challenge that must be faced, especially between urban communities with easy access to digital technology and rural communities with limited access. Another obstacle is the technical aspect of

implementing Virtual Police. A robust infrastructure and sufficient technical expertise are needed to carry out effective surveillance in cyberspace. However, this is a challenge in itself because there is still a lack of human resources who are experts in the fields of information and communication technology (ICT) and cybersecurity in Indonesia. Adapting to the dynamics of speedy technological developments is also an obstacle to implementation.

Next is the issue of human rights. Please remember that every individual has the right to privacy, including digital privacy (Revilia & Irwansyah, 2020). Keeping this in mind, the Virtual Police must ensure no privacy and human rights violations. Even though it has noble aims, there is potential for misuse of Virtual Police, which can violate privacy and damage freedom of expression. This problem requires a balance between law enforcement and human rights protection. From an Indonesian perspective, it is essential to understand that social and cultural values also influence the implementation of Virtual Police. Indonesian people are known to have high values of cooperation and togetherness. Therefore, the implementation approach must consider community participation and education about the importance of ethics and responsibility on the Internet. Overall, implementing Virtual Police in Indonesia raises various challenges and obstacles. However, if done correctly and accompanied by increased digital literacy and severe attention to human rights, this can be an essential step in fighting crime in cyberspace.

Cooperation between government, society, and the private sector is needed to increase awareness and knowledge about cyber security and digital ethics. In particular, the government needs to take the lead in developing and implementing Virtual Police with high levels of transparency and accountability. Independent monitoring and review mechanisms must also be implemented to ensure no human rights violations in its operations. In line with Indonesian values, involving the community in this process is essential. Education and digital literacy must be an integral part of this strategy so that people not only understand how the Virtual Police works and the objectives, but also their rights and obligations as internet users. The private sector, especially technology and telecommunications companies, is vital in this process. They can contribute to improving the necessary infrastructure and technology and training and developing competent human resources in cyber security. Challenges, obstacles, and human rights issues in implementing Virtual Police are complex problems and require a holistic approach. Indonesia, with its spirit of cooperation and togetherness, has the potential to address these challenges and take maximum advantage of this technology for the good of society. Safety and security in cyberspace are truly our shared responsibility. We can create a safe and inclusive digital environment for all Indonesian citizens with good understanding and intense cooperation.

Concretely, here are several steps that can be taken to address challenges, obstacles, and human rights issues related to the implementation of Virtual Police in Indonesia:

1. Increasing Digital Literacy
   The government can collaborate with educational institutions and non-government organizations to organize training and workshops on digital literacy. The main focus is understanding digital ethics, online privacy, and misuse of personal data. This is important to help people understand their rights and obligations in cyberspace.
2. Strengthening Infrastructure and Technical Expertise
   The government must invest in developing digital infrastructure and developing competent human resources in information and communications technology (ICT) and cybersecurity. Collaboration with the private sector, especially technology companies, can help.
3. Protection of Human Rights
   In implementing Virtual Police, there must be a precise mechanism to ensure that there are no violations of human rights, especially the right to privacy. This could involve establishing independent oversight bodies and implementing transparent and accountable review mechanisms.
4. Collaboration and Mutual Cooperation
   Adopting Indonesian values such as cooperation in implementing Virtual Police is very important. This can mean involving the public in decision-making processes and strategy development and promoting active participation in maintaining digital security and ethics.
5. Openness and Transparency
   The implementation and operational process of Virtual Police must be carried out with openness and transparency. This is important to build public trust and ensure that this technology is used for the good of society, not the other way around.

With this approach, it is hoped that challenges and obstacles in implementing Virtual Police can be overcome while ensuring that human rights are protected. If done correctly, Virtual Police can effectively combat cybercrime and create a safe and inclusive digital environment for all Indonesian citizens.

Conclusion

In this digital era, cyber security challenges are increasingly complex and dynamic. Cybercrime not only causes material losses but can also threaten national security and social stability. Countering this threat requires a comprehensive and multi-dimensional approach. Virtual Police, as the National Police's effort to monitor

and handle cyber crime cases, has demonstrated its essential role in maintaining security and order in Indonesia's digital space. However, there is still room for improvement in readiness, capability, operational transparency, and accountability. Comparisons with other countries, such as the United States and Singapore, show that international cooperation, increased capabilities, transparent policies, and public education and awareness can strengthen the role of the Virtual Police. The experiences of these countries can be a valuable lesson for Indonesia in dealing with cybercrime issues. Furthermore, increasing public awareness and education about cyber security is essential. An aware and educated public will be the first layer of defense in preventing cybercrime. However, there are many solutions. Cooperation between government, the private sector, and civil society is needed, as well as strict laws and regulations to deal with cybercrime. Ultimately, facing cybersecurity challenges is a shared responsibility. Governments, the private sector, and society must work together to create a safe and inclusive digital environment where everyone can enjoy the benefits of information and communications technology without worrying about cybersecurity threats.

The implementation of Virtual Police in Indonesia raises challenges and obstacles related to issues of human rights, privacy, and consumer protection. While Virtual Police can be an essential tool in fighting cybercrime and creating a safe digital environment, ensuring its implementation is carried out with respect for individual rights and freedoms is vital. This requires a holistic approach involving all stakeholders, including government, the private sector, and society. In addition, there must be transparency and accountability in Virtual Police operations, as well as effective monitoring and review mechanisms. The values of Pancasila and the 1945 Constitution of the Republic of Indonesia, as well as regulations such as the ITE Law and the Consumer Protection Law, must be a guide in implementing Virtual Police. In line with these values, Virtual Police must be directed at improving the community's quality of life and protecting human rights. In this way, Virtual Police can be an effective and responsible tool for creating a safe and inclusive digital environment for all Indonesian citizens, as long as it is done in a way that respects and protects individual rights and freedoms. Despite significant efforts, it remains essential for Indonesia to continue strengthening its cyber security infrastructure, creating an adequate legal framework, and keeping up-to-date with technological developments and cybercrime trends. In this regard, investment in research and development, professional training, and public education is essential. Initiatives such as Virtual Police must be continually evaluated and updated to ensure effectiveness and relevance in a changing environment. Moreover, such initiatives must always respect and protect the rights and privacy of internet users. Ultimately, the main goal of cybersecurity is to create a safe and trusted digital environment where everyone

feels safe and free to access, use, and share information. Building a society aware and educated about cyber security is not easy, but it is essential. It requires a holistic approach that includes formal education in schools and universities, public awareness campaigns, and specialized training for parents, educators, and professionals. Individuals must also take personal responsibility to protect themselves and others from cyber threats. Cybersecurity challenges in this digital era require combined efforts and shared commitment from the government, the private sector, and society. With this cooperation and commitment, we can create a safe and inclusive digital environment and ensure that everyone can enjoy the benefits of digital technology without fearing cyber security threats.

References

Agusalim et al. (2022). Green Victimology: Sebuah Konsep Perlindungan Korban dan Penegakan Hukum Lingkungan di Indonesia. *Bina Hukum Lingkungan*, *7*(1), 60–79. https://doi.org/10.24970/BHL.V7I1.302

Alifia Astika. (2021). *Apa Itu Polisi Virtual? 3 Hal yang Harus Kamu Ketahui Soal Virtual Police*. Https://Www.Sonora.Id.

Allagui, I. (2017). Internet in the Middle East: an asymmetrical model of development. *Internet Histories*, *1*(1–2), 97–105. https://doi.org/10.1080/24701475.2017.1305715

Angkasa, A., & Windiasih, R. (2022). Cybercrime Di Era Industri 4.0 Dan Masyarakat 5.0 Dalam Perspektif Viktimologi. *Journal Justiciabelen (Jj)*, *2*(2), 104–119. https://doi.org/10.35194/jj.v2i2.2113

Arisandy, Y. O. (2021). Penegakan Hukum terhadap Cyber Crime Hacker. *Indonesian Journal of Criminal Law and Criminology (IJCLC)*, *1*(3), 162–169. https://doi.org/10.18196/ijclc.v1i3.11264

Arwana, Y. C. (2022). Victims of Cyber Crimes in Indonesia: A Criminology and Victimology Perspective. *Semarang State University Undergraduate Law and Society Review*, *2*(2), 181–200. https://doi.org/10.15294/lsr.v2i2.53754

Asmah et al. (2023). Pancasila's Economic Existence In Business Development: The Efforts To Realize Justice In Business Law. *Jurnal IUS Kajian Hukum Dan Keadilan*, *11*(2), 266–280. https://doi.org/https://doi.org/10.29303/ius.v11i2.1224

Azra Heriana, K. M., Prawita, A., Cakra Dewa, M. M., Satino, S., & Navael, L. D. (2022). Peran Bela Negara Sebagai Upaya Menanggulangi Cybercrime Dalam Era Digital. *Kertha Semaya : Journal Ilmu Hukum*, *10*(5), 1134–1147. https://doi.org/10.24843/ks.2022.v10.i05.p13

Bill Clinten. (2022). *Awal 2022, Indonesia Hadapi 11 Juta Ancaman di Dunia Maya*. Https://Tekno.Kompas.Com.

Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO)*, *3*(November), 223–234. https://doi.org/10.54706/senastindo.v3.2021.141

Cahyadi, I. (2016). Tata Kelola Dunia Maya Dan Ancaman Kedaulatan Nasional. *Politica*, *7*(2), 210–232. https://doi.org/10.22212/jp.v7i2.1134

Clough, J. (2010). Principles of Cybercrime. In *Principles of Cybercrime*. Cambridge University Press. https://doi.org/10.1017/CBO9780511845123

Federal Bureau of Investigation. (2023). *The Cyber Action Team*. Https://Www.Fbi.Gov/.

https://www.fbi.gov/news/stories/the-cyber-action-team

Fox, B. H. (2015). Federal Bureau of Investigation (FBI). *The Encyclopedia of Crime and Punishment*, 1–6. https://doi.org/10.1002/9781118519639.WBECPX128

Gani, A. G. (2014). Cybercrime (Kejahatan Berbasis Komputer). *Jurnal Sistem Informasi Universitas Suryadarma*, *5*(1), 16–29. https://doi.org/10.35968/jsi.v5i1.18

Gulo, A. S., Lasmadi, S., & Nawawi, K. (2021). Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *PAMPAS: Journal of Criminal Law*, *1*(2), 68–81. https://doi.org/10.22437/pampas.v1i2.9574

Herlambang et al. (2022). Kejahatan Memperkaya Diri Sendiri Secara Melawan Hukum (Illicit Enrichment) Dan Aparatur Sipil Negara: Sebuah Kajian Kritis. *RechtsVinding*, *11*(2), 247–264. https://doi.org/http://dx.doi.org/10.33331/rechtsvinding.v11i2

Hidayanto, F., Mohammad, D., & Ilmi, Z. (2015). Memanfaatkan Perkembangan Teknologi Internet Dan Situs Web Untuk Kepentingan Warga Sekaligus Sebagai Sarana Promosi Potensi Desa Gerbosari. *Inovasi Dan Kewirausahaan*, *4*(1), 13–20.

Ibrahim. (2003). Jurisdiksi Dunia Maya (Cyberspace) Dalam Sistem Hukum Nasional Abad XXI. *Jurnal Hukum IUS QUIA IUSTUM*, *10*(24), 119–127. https://doi.org/10.20885/iustum.vol10.iss24.art10

Indonesian National Police. (2021). *INP Explains How Virtual Police Work - INP | Indonesian Natinonal Police*. Https://Inp.Polri.Go.Id/. https://inp.polri.go.id/2021/02/25/explains-how-virtual-police-work/

Maria Helen Oktavia. (2021). *Indonesia to Activate "Virtual Police" Unit To Educate Public on Cybercrime*. Https://Go.Kompas.Com/. https://go.kompas.com/read/2021/02/18/153132374/indonesia-to-activate-virtual-police-unit-to-educate-public-on-cybercrime

Ngafifi, M. (2014). Kemajuan Teknologi Dan Pola Hidup Manusia Dalam Perspektif Sosial Budaya. *Jurnal Pembangunan Pendidikan: Fondasi Dan Aplikasi*, *2*(1), 41. https://doi.org/10.21831/jppfa.v2i1.2616

Oates, B. (2001). Cyber Crime: How Technology Makes it Easy and What to do About it. *Information Systems Management*, *18*(3), 92–96. https://doi.org/10.1201/1078/43196.18.3.20010601/31295.12

Orlov, V. (2012). Cyber Crime: A Threat to Information Security. *Security Index: A Russian Journal on International Security*, *18*(1), 1–4. https://doi.org/10.1080/19934270.2011.644444

Pan Dhadha, T., Rahayu, L. A., Resmi, D. S., & Kusumastuti, D. (2021). Efektivitas Peran Uu Ite Dalam Rangka Melindungi Serta Menjaga Seluruh Aktivitas Siber Yang Ada Di Indonesia. *Legal Standing : Jurnal Ilmu Hukum*, *6*(1), 40–48. https://doi.org/10.24269/ls.v6i1.3541

Peter Mahmud Marzuki. (2005). *Penelitian Hukum*. Kencana Prenada Media.

Putra, P. S., Fernando, Z. J., Nunna, B. P., & Anggriawan, R. (2023). Judicial Transformation: Integration of AI Judges in Innovating Indonesia's Criminal Justice System. *Kosmik Hukum*, *23*(3), 233–247. https://doi.org/10.30595/kosmikhukum.v23i3.18711

Putri, A., Pebriani, A., Rumi, M. J., & Siregar, J. H. (2021). Pemanfaatan Aplikasi Toko Online Terhadap Kebutuhan Konsumen Selama Pandemi Covid-19. *Prosiding Seminar Nasional Pengabdian Masyarakat LPPM UMJ*, *3*(3), 1–8.

Revilia, D., & Irwansyah, N. (2020). Social Media Literacy: Millenial's Perspective of Security and Privacy Awareness. *Jurnal Penelitian Komunikasi Dan Opini Publik*, *24*(1), 1–15. https://doi.org/10.33299/jpkop.24.1.2375

Rifan Aditya. (2021). *Cara Kerja Polisi Virtual atau Virtual Police, Polri Patroli Siber*. Https://Www.Suara.Com. https://www.suara.com/news/2021/02/27/095639/cara-

kerja-polisi-virtual-atau-virtual-police-polri-patroli-siber

Riswandi, B. A. (2016). Hukum dan Teknologi: Model Kolaborasi Hukum dan Teknologi dalam Kerangka Perlindungan Hak Cipta di Internet. *Jurnal Hukum IUS QUIA IUSTUM*, *23*(3), 345–367. https://doi.org/10.20885/iustum.vol23.iss3.art1

Rumlus, M. H., & Hartadi, H. (2020). Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik. *Jurnal HAM*, *11*(2), 285–299. https://doi.org/10.30641/ham.2020.11.285-299

Safitri, R. (2018). Undang-Undang Informasi dan Transaksi Elektronik Bagi Perguruan Tinggi. *SALAM: Jurnal Sosial Dan Budaya Syar-I*, *5*(3), 197–218. https://doi.org/10.15408/sjsbs.v5i3.10279

Saunders, J. (2017). Tackling Cybercrime – The UK Response. *Journal of Cyber Policy*, *2*(1), 4–15. https://doi.org/10.1080/23738871.2017.1293117

Setyaningrum, W., Morana, A. C., Vaizi, K. N., Damarina, R., Akbar, S. A., & Oktasari, S. (2022). Anticipation of the ITE Law and Reconciliation of Its Forms Freedom of Expression through the E-Hights Website. *Jurnal Hukum Novelty*, *13*(2), 266. https://doi.org/10.26555/novelty.v13i2.a23799

Singapore Police Force. (2023). *SPF | Criminal Investigation Department*. Https://Www.Police.Gov.Sg/. https://www.police.gov.sg/Who-We-Are/Organisation-Structure/Specialist-Staff-Departments/Criminal-Investigation-Department

Soekanto, S., & Mamudji, S. (2001). *Penelitian Hukum Normatif Suatu Tinjauan Singkat*. Raja Grafindo Persada.

Supanto. (2016). Perkembangan Kejahatan Teknologi Informasi (Cyber Crime) dan Antisipasinya Dengan Penal Policy. *Yustisia Jurnal Hukum*, *5*(1), 52–70. https://doi.org/https://doi.org/10.20961/yustisia.v5i1.8718

Tsarina Maharani. (2021). *Mengenal Virtual Police: Definisi, Dasar Hukum, Hingga Polemiknya*. Https://Nasional.Kompas.Com. https://nasional.kompas.com/read/2021/03/17/14414171/mengenal-virtual-police-definisi-dasar-hukum-hingga-polemiknya

Vika Azkiya Dihni. (2021). *Kerugian Akibat Kejahatan Siber Capai Rp 3,88 Triliun, Apa Saja Bentuknya?* Https://Databoks.Katadata.Co.Id.

Wall, D. S. (2008). Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime. *International Review of Law, Computers & Technology*, *22*(1–2), 45–63. https://doi.org/10.1080/13600860801924907

Yuli Nurhanisah. (2023). *Virtual Police, Edukasi Masyarakat di Dunia Maya*. Https://Indonesiabaik.Id.