CHALLENGES OF CRIMINAL INVESTIGATION CYBER CRIME

Wandi Hartono[1], Dekky Muhardi[2], Ahmad Akhiruddin[3], Desi Valentianna Br Purba[4], Pandu Asa[5], HM Yusuf DM[6]
[1,2,3,4,5,6]Postgraduate Program in Master of Law, Lancang Kuning University, Pekanbaru, Indonesia

Received 2 Oct 2024 • Revised 1 Nov 2024 • Accepted 29 Nov 2024

Abstract

The investigation process still faces many cases of cybercrime that are stalled due to the limited equipment owned by the Police. For example, if there is a complaint or report from the public regarding cybercrime, the reporter submits the incident to the local Police, which usually does not have specialized equipment to examine the complaint or report. Therefore, the local Police must coordinate with the Resort Police, which, if its equipment is still inadequate, must transfer the complaint or report to the Regional Police level, which certainly has the necessary equipment to handle cybercrime cases. This becomes an obstacle in the investigation process within the internal sector. Meanwhile, for external factors, there are various obstacles faced by investigators. The problem formulation is how the challenges of cybercrime investigation are addressed. The research objective is to analyze the challenges in cybercrime investigations. The research method that will be conducted by the author is normative research, which is based on applicable legal principles. In conclusion, after understanding the regulations for investigating cybercrime cases as regulated in the Law on Information and Electronic Transactions, it can be concluded that the investigation process is carried out by a team of investigators from the Indonesian National Police who can be assisted by experts in specific fields related to the case being investigated, if needed, to resolve the case while maintaining privacy, data authenticity, and not disrupting public services or facilities. Searches and/or seizures of electronic systems related to suspected criminal acts must be carried out with permission from the local District Court.

Keywords: Investigation, Criminal Act, Cyber Crime

INTRODUCTION

In the rapidly developing digital era, cybercrime has become a serious threat to the security of individuals, organizations, and even countries. As society's dependence on information and communication technology increases, criminals are also increasingly adept at exploiting cybersecurity gaps to carry out their illegal actions. The challenges faced by law enforcement in handling cybercrime cases are not only limited to the technical complexity of the crime itself, but also to the evidentiary aspect which is often the main obstacle in the law enforcement process1 Cybercrime, or also known as cybercrime, includes various forms of illegal activities carried out through or using computer devices and internet networks. These forms of crime can include hacking, online fraud, data theft, malware distribution, and attacks on critical infrastructure. The unique characteristics of cybercrime, such as its cross-border nature, the anonymity of the perpetrators, and the rapid development of technology, make the process of proof much more complex compared to conventional crimes.

Currently, the world is in the information era which is a continuation of the prehistoric era, the agricultural era, and the industrial era. In the information era, the existence of information has a very important meaning and role for all aspects of life, and is one of the necessities of life for everyone, both individuals and organizations, so it can be said that in the information society, information has functioned like the blood flow of the source of life for the human body. The development of world politics that always changes from time to time so that it affects the entire order of world life. The dynamic world continues to experience changes that are sometimes colored by turbulence that affects relations between countries and the constellation of global issues so that it affects the joints of national and state life, not to mention the social life of society. Every global development in the world will always affect the entire national life in each country so that it forces each country to always observe and examine every development of the strategic environment both at the global, regional, national, and local levels.

The current globalization that is happening all over the world today has brought the world into an era of information and communication technology development, creating a digital world. In this case, the development of computer technology and the internet has become a new means for countries in the world to be used as a tool to carry out various penetrations, influences and infiltrations into various countries, thus greatly encouraging the world to develop in a complex, diverse and pluralistic way. One of the findings that has had the greatest influence on the information society is the discovery of the internet. The presence of the internet as a form of new technology has caused humans to be unable to be separated from the flow of communication and information. The internet has caused a major leap in life. As with other technologies, the internet is not value-free. Technology will be effective if we pay attention to the usefulness of technology that is adjusted to social and personal values and the existence of government regulations that protect society from the negative impacts it causes.

One case that serves as the background for the title "CHALLENGES OF CYBERCRIME INVESTIGATION" is the massive data breach that occurred in Indonesia in 2020, where personal data of over 279 million Indonesians was leaked and sold on the dark web. This case highlighted the significant challenges in cybercrime investigation, particularly regarding the limited tools and expertise possessed by the police in handling cases involving technology and electronic data. Additionally, issues of coordination between local and regional police agencies also became obstacles to effective investigation.

Related to the internet there are a number of related concepts namely telematics, multimedia and cyber space. The term telematics is known as the new hybrid of technology which emerged due to the development of digital technology which made the development of telecommunications and informatics technology increasingly integrated or commonly called convergence. The convergence between telecommunications, media and informatics technology finally encouraged the implementation of electronic systems based on digital technology which was later known as the net. Convergence itself is a symptom that emerged in the Information and Communication Technology (ICT) service industry which emerged in line with the rapid progress of electronic technology in the late 20th century. The social impact of convergence has been felt by society both positively and negatively. One of the negative impacts that emerged in cyber-space is the occurrence of cyber crime. The rise of cyber crime requires attention and seriousness in developing cyber security for a country including Indonesia.

In the context of Indonesian law, the proof of cybercrime cases is regulated in Law Number 11 of 2008 concerning Information and Electronic Transactions which has been updated by Law Number 19 of 2016. Although this legal framework has provided a foundation for handling cybercrime cases, its implementation in the field still faces various challenges. One of the main challenges is how to

collect, analyze, and present digital evidence that is admissible in court. Digital evidence has different characteristics from conventional physical evidence. Its volatile, easily erased, and often scattered nature across multiple locations and jurisdictions makes the process of collecting and storing it very critical. In addition, the ability of criminals to hide their digital footprints, using encryption techniques, or utilizing anonymous services such as VPNs and the dark web, further complicates the investigation and evidence process.

Another challenge faced is the limited resources and expertise among law enforcement. Cybercrime investigations require in-depth technical knowledge of computer systems, networks, and digital forensics techniques. However, not all law enforcement agencies have personnel with adequate expertise in these areas. This can lead to errors in handling digital evidence or an inability to analyze evidence effectively.

The jurisdictional aspect is also a significant issue in handling cybercrime cases. The transnational nature of the internet allows criminals to operate from locations far from where the impact of the crime occurs. This raises questions about legal jurisdiction and requires effective international cooperation in the investigation and prosecution process. However, differences in legal systems and procedures between countries often become obstacles in this process. In addition, the rapid development of technology is also a challenge in itself. The methods and tools used by criminals continue to develop, while the process of updating regulations and increasing the capacity of law enforcement often lags behind. This creates gaps that can be exploited by cybercriminals. In the context of court evidence, another challenge that arises is how to explain technical concepts and evidence to judges and juries who may not have a strong technical background. The presentation of complex digital evidence must be done in a way that the court can understand without reducing its probative value.

Viewed from the perspective of criminal law, efforts to combat cyber crime can be seen from various aspects, namely from the aspect of criminalization policy (formulation of criminal acts), the aspect of criminal liability or punishment (including the aspect of evidence/proof), and the aspect of jurisdiction which can help in combating cyber crime. Cyber activities are no longer simple, because these activities are no longer limited by the territory of a country, which is easily accessible anytime, anywhere. Losses can occur, both to the perpetrators of the transaction, and to other people who do not make transactions on the internet. Proof is very important, considering that electronic information has not been accommodated in the legal procedure system in Indonesia comprehensively, and it turns out that it is also very vulnerable to being changed, tapped, falsified, and sent to various corners of the world in a very short time, thus the impacts it causes can be very complex and complicated.

To date, the police are still facing obstacles in handling cybercrime in carrying out their duties, especially in implementing the role of the Indonesian National Police forensic laboratory as a scientific supporter of investigators in the criminal justice system in Indonesia. The obstacles faced are regarding limited personnel, limited investigators in terms of information technology, inadequate and not up-to-date facilities which also affect the results of work and examinations such as digital forensic laboratories which are still very limited in the Regional Police in Indonesia, limited budgets and so on which this needs to be considered by the Government for the sake of improving the performance of the Republic of Indonesia Police, therefore the author is very interested in conducting research on the real reality in the field faced by the police in dealing with cyber crime.

Investigations based on Law Number 11 of 2008 concerning Information and Electronic Transactions are carried out by paying attention to the protection of privacy, confidentiality, smoothness of public services, data integrity, or data integrity in accordance with the provisions of the Laws and Regulations. Searches and/or seizures of electronic systems related to alleged criminal acts must be carried out with the permission of the head of the local district court. In the case of making arrests and detentions, investigators through the public prosecutor are required to request a determination from the head of the local district court within one time of twenty-four hours. In order to uncover criminal acts of Information and Electronic Transactions, investigators can cooperate with investigators from other countries to share information and evidence.

Investigation based on the Criminal Procedure Code is a series of steps taken by investigators against the meaning of the method whose regulations are stated in this Law to search for, find and collect evidence which with evidence can make it clear for a criminal act and in order to find the perpetrator in a criminal act committed by an Officer of the Republic of Indonesia National Police or a certain Civil Servant Officer who is given special authority by law, because of his obligations, investigators have the authority including receiving reports or complaints from someone about a criminal act, taking the first action at the scene of the incident, ordering a suspect to stop and checking the suspect's identification. Therefore, in practice, investigations must have the aim of

clarifying a criminal case and finding the suspect and so that the criminal case can be resolved quickly.

However, in reality, in the investigation process, there are still many cases of cybercrime that are left unsolved due to the limited equipment owned by the Police, for example, if there is a complaint or report from the public regarding the occurrence of cybercrime, the reporter reports the incident to the local Police, which usually does not have special equipment to examine complaints or reports from the public, so the Police must coordinate with the Resort Police, which if its equipment is still inadequate, must forward the complaint or report to the Regional Police level which certainly has adequate equipment to handle cybercrime cases, this is an obstacle in the investigation in the internal sector. While for external factors themselves, there are various obstacles faced by investigators.

RESEARCH METHOD

The research that the author will conduct is normative, namely research that is based on applicable legal principles, in this case the research is conducted onChallenges of Cyber Crime Investigation.This type of normative research is a process of finding legal rules, legal principles, or legal doctrines, to answer the legal issues faced. This is in accordance with the prescriptive character of legal science. This normative legal research is carried out to produce new arguments, theories or concepts as prescriptions for solving the problems faced. Furthermore, the research approach used to answer the research problem is also explained: Statute Approach is an approach used to examine all laws and regulations related to the legal problems or issues faced. The approach used to examine and analyze laws/regulations related to research problems, namely:

1) Civil Code
2) Law Number 11 of 2008 concerning Electronic Information and Transactions

The Conceptual Approach is an approach used which is based on the views and doctrines that have developed in legal science.

RESULTS AND DISCUSSION

Challenges of Cyber Crime Investigation

Cybercrimehas become a serious challenge for law enforcement in this digital era. Its unique characteristics, such as transnationality, anonymity of perpetrators, and volatility of digital evidence, create significant complexity in the evidentiary process. This study reveals that the main challenges in proving cybercrime cases in Indonesia include the complexity of ever-evolving technology, limited resources and expertise among law enforcement, jurisdictional issues in handling cross-border cases, the need for legal framework updates, and difficulties in collecting, analyzing, and presenting digital evidence in court. These findings emphasize the need for a multidimensional approach to address these challenges.

The complexity of technology is one of the main factors that complicates the process of proof. Rapid developments in information and communication technology have created new loopholes that can be exploited by cybercriminals. The use of increasingly sophisticated encryption techniques, the use of anonymous networks such as Tor, and the proliferation of cryptocurrency as a means of illegal transactions have increased the level of difficulty in tracking and identifying perpetrators. In addition, the variety of devices and platforms used in cybercrime requires investigators to have extensive and continuously updated knowledge of various systems and applications.

Limited resources and expertise among law enforcement are significant obstacles in handling cyber crime cases. The results of the study show that there is still a large gap between the complexity of cyber crime and the capacity of law enforcement in Indonesia. The lack of trained digital forensic experts, limited up-to-date forensic equipment and software, and limited budget for investigations are the main obstacles. This results in the process of collecting and analyzing digital evidence being less than optimal, which in turn can affect the quality of evidence in court.

The era of globalization is marked by the rapid development of science and technology, especially in the fields of information, communication and transportation, as if making the world transparent without recognizing national borders. This condition creates a new structure, namely the global structure. Cybercrime is one of the new forms of crime in modern times that has received special attention in the international world because it is considered very dangerous. Cybercrime is a crime committed in groups or individuals using computer devices or any telecommunications devices connected to the internet, usually carried out by people who are experts in using computers who can commit the crime.

Technically, cybercrime can be divided into cybercrime, semi-online crime, and off-linecrime, each has different characteristics but the most distinguishing is its relationship with internet

information. Cybercrime in Indonesia has been increasingly rampant lately, here are some cases of cybercrime that often occur in Indonesia, including:

1. Internet User Account Theft is one of the categories of fraud and identity theft of a particular person.
2. Hacking a website is a crime that involves changing the appearance of a website or web according to the perpetrator's wishes.
3. Probing and Port ScanningOne of the steps taken by the perpetrator before entering the targeted server is by spying.
4. Denial of Service attack,This is a type of attack on a computer or server on an internet network by using up resources on the computer until the computer cannot function properly, thus indirectly preventing other users from gaining access to services from the computer.
5. Cardingis the activity of purchasing goods on the internet using a pirated credit card. The credit card is obtained by requesting from another carder or by joining a carder community on a particular IRC server, or by using the carder's social engineering skills. Carding crimes are also often carried out with a Phishing system, namely by tapping through a fake website so that customer personal data can be stolen.

Often law enforcement in Indonesia experiences difficulties when conducting investigations that attempt to ensnare perpetrators due to evidentiary issues that do not meet the provisions of the Indonesian criminal law system, however, efforts to arrest perpetrators of cybercrime must still be carried out, efforts to expand evidence are a solution for law enforcement.

Therefore Opsporing in Dutch has the same meaning as investigation. Investigating means an initial examination by an official who has been determined based on the law immediately after they in any way know news that is simply reasonable, that a crime has occurred according to De Pinto.

Investigations based on Law Number 11 of 2008 concerning Information and Electronic Transactions are carried out by paying attention to the protection of privacy, confidentiality, smoothness of public services, data integrity, or data integrity in accordance with the provisions of the Laws and Regulations. Searches and/or seizures of electronic systems related to alleged criminal acts must be carried out with the permission of the head of the local district court. In the case of making arrests and detentions, investigators through the public prosecutor are required to request a determination from the head of the local district court within one time of twenty-four hours. In order to uncover criminal acts of Information and Electronic Transactions, investigators can cooperate with investigators from other countries to share information and evidence.

Investigation based on the Criminal Procedure Code is a series of steps taken by investigators against the meaning of the method whose regulations are stated in this Law to search for, find and collect evidence which with evidence can make it clear for a criminal act and in order to find the perpetrator in a criminal act committed by an Officer of the Republic of Indonesia National Police or a certain Civil Servant Officer who is given special authority by law, because of his obligations, investigators have the authority including receiving reports or complaints from someone about a criminal act, taking the first action at the scene of the incident, ordering a suspect to stop and checking the suspect's identification. Therefore, in practice, investigations must have the aim of clarifying a criminal case and finding the suspect and so that the criminal case can be resolved quickly.

Investigation is a term that has the same meaning or understanding as the Dutch definition, namely opsporing and in English investigation and in Malaysian Penyiasatan. Investigations are regulated in Article 1 paragraph (2) of the Criminal Procedure Code, which is formulated as a series of steps carried out by investigators in accordance with the meaning of the method, the provisions of which are stated in the Criminal Procedure Code, to search for, find and collect evidence which can make it clear that a crime has been committed and to find the perpetrator of the crime.

However, in reality, in the investigation process, there are still many cases of cybercrime that are left unsolved due to the limited equipment owned by the Police, for example, if there is a complaint or report from the public regarding the occurrence of cybercrime, the reporter reports the incident to the local Police, which usually does not have special equipment to examine complaints or reports from the public, so the Police must coordinate with the Resort Police, which if its equipment is still inadequate, must forward the complaint or report to the Regional Police level which certainly has adequate equipment to handle cybercrime cases, this is an obstacle in the investigation in the internal sector. While for external factors themselves, there are various obstacles faced by investigators.

The elements contained in the formulation of the Investigation of Article 1 paragraph (2) of the Criminal Procedure Code are as follows:

1. Investigation is a literature in an action carried out by investigators which are interconnected with each other in these actions;

2. Public officials are investigators who carry out investigative actions;
3. Implemented based on statutory regulations;
4. The purpose of an investigation is to search for, collect and obtain evidence to clarify a crime and find the perpetrator of the crime.

Based on the elements above, it is necessary to know that before the investigation and inquiry is carried out, it is known that a criminal act has occurred, but it is not yet known and not yet clear who the perpetrator is, and therefore to make it clear in a criminal act and who the perpetrator is through a series of investigative actions (Chazawi, 2005).

Investigations based on Law Number 11 of 2008 concerning Information and Electronic Transactions are carried out by paying attention to the protection of privacy, confidentiality, smoothness of public services, data integrity, or data integrity in accordance with the provisions of the Laws and Regulations. Searches and/or seizures of electronic systems related to alleged criminal acts must be carried out with the permission of the head of the local district court. In the case of making arrests and detentions, investigators through the public prosecutor are required to request a determination from the head of the local district court within one time of twenty-four hours. In order to uncover criminal acts of Information and Electronic Transactions, investigators can cooperate with investigators from other countries to share information and evidence. Law Number 11 of 2008 concerning Electronic Information and Transactions regulates investigations which are carried out in the following manner:

1. Civil Servant Officials within the Government who have special expertise in the field of Information Technology and Electronic Transactions may be given special authority as investigators in accordance with the Law on Criminal Procedure to conduct investigations into criminal acts in the field of Information Technology and Electronic Transactions.
2. Maintaining privacy, confidentiality, not disrupting public services, data integrity, or not damaging original data.
3. The local District Court has full authority to search and confiscate electronic systems that are strongly suspected of having a role in the occurrence of a crime.
4. The authority of investigators is regulated in the laws which form the legal basis for each and are under the supervision of investigators in carrying out their respective duties.
5. Investigators are required to uphold applicable laws during the investigation process.
6. Does not hinder the smooth running of public interests during the investigation process.

The evidence for investigation based on Law Number 11 of 2008 concerning Electronic Information and Transactions is as follows:

1. Electronic Information
   Electronic data including writing, images, sound, photo designs, maps, electronic mail, electronic data interchange (EDI), telegrams, letters, signs, numbers, access codes, symbols, which contain signals or codes that can only be understood by certain people.
2. Electronic Documents
   All electronic information created, sent, received, forwarded or stored in any form that can be seen, displayed or heard via electronic devices, including writing, images, sounds, designs, photos, maps, letters, signs, numbers, access codes, symbols containing signals or codes that can only be understood by certain people.
3. Electronic devices connected to the internet
   Every electronic device, whether in the form of software or hardware owned by a particular individual or is a public facility connected to the internet network that has very broad benefits or uses can almost facilitate all human activities or needs.

Acts prohibited under Law Number 11 of 2008 concerning Electronic Information and Transactions:

1) Every person intentionally and without right creates, distributes and trades a file or document in audio, visual and written form which is contrary to morality;
2) Every person intentionally and without authorization creates or creates, disseminates and trades files or documents that can be easily accessed relating to gambling activities;
3) Any person who intentionally and without right creates or creates, distributes, and sells documents or files of a personal nature that contain insults or defamation which may result in certain losses;

4) Any person who intentionally and without authority creates or creates, distributes, and sells certain documents or files that contain blackmail or threats that can cause certain losses;
5) Any person who intentionally and without authority creates or creates, distributes, or otherwise causes harm to users, buyers or individuals in Electronic Transactions;
6) Any person who intentionally and without right creates or distributes information in the form of news, reports or facts that can give rise to feelings of displeasure or hatred or hostility towards people or individuals or groups of people or certain groups based on race, ethnicity and religion;
7) Any person who intentionally and without right creates or distributes information that may be in the form of news, reports or facts in the form of electronic files or documents that contain elements of threats of violence or intimidation or are of a blackmailing nature that attacks certain people or individuals;
8) Any person who intentionally and without right creates or creates, distributes, and trades illegally using or exploiting an electronic system or computer device that does not belong to that person or belongs to another person by any method;
9) Any person who intentionally and without the right creates or creates, distributes, and trades illegally using or utilizing electronic systems or computer devices by any method with the intention of obtaining electronic documents or electronic information and/or certain files;
10) Any person who intentionally and without the right creates or creates, distributes, and trades illegally, runs or utilizes an electronic system or computer device in a way that deviates from, forces, exceeds, or damages a security system or safety system;
11) Any person who intentionally and without permission creates or creates, distributes, and trades illegally, taps or intercepts an electronic document or electronic information or certain files in an electronic system or computer device belonging to another person;
12) Any person who intentionally and without right creates or creates, distributes, and trades illegally, intercepts or intercepts an electronic document or electronic information or a certain file that is confidential (not intended for the public) in an electronic system or computer device belonging to another person, even though there is no change, destruction or removal whatsoever or that causes any change, destruction or removal, or forcibly stops an electronic document or electronic information or a certain file that is being run;
13) Any person who intentionally and without right creates or creates, distributes, and trades illegally by any method, changes, adds, deletes or reduces, damages, eliminates, moves, hides an electronic document or electronic information or certain files belonging to the public or individuals;
14) Any person who intentionally and without right creates or creates, distributes, and trades illegally by any method, transfers or carries out the transfer of an electronic document or electronic information or certain files to the Electronic System belonging to another person or certain individual;
15) Any person who intentionally and without the right creates or creates, distributes, and trades illegally carries out activities in any form that can disrupt the working method or hinder the working method of an electronic system as it should;
16) Any person who intentionally and without rights creates or creates, provides, imports, distributes, and sells illegally for use or possession of certain software or passwords;
17) Any person who intentionally and without right creates or creates, distributes, and trades illegally, falsifies, changes, removes, reduces, damages or creates an electronic document or electronic information with the intention that an electronic document or electronic system or certain file is considered to be original or authentic data;
18) Any person who intentionally and without the right creates or creates, distributes, and trades in an unlawful manner acts as referred to in Articles 27 to 34 which results in losses for certain people or individuals;
19) Any person who intentionally creates or creates, distributes, and trades in an unlawful manner that is prohibited as referred to in Articles 27 to 36 outside the scope of Indonesian territory against computer devices or electronic systems that are within the scope of Indonesian legal

territory.

The issue of jurisdiction in handling cross-border cybercrime cases is a challenge in itself. The transnational nature of the internet allows criminals to operate from locations far from where the crime occurred. Differences in legal systems and procedures between countries often become obstacles in the investigation and prosecution process. Effective international cooperation in the exchange of information and mutual legal assistance is crucial, but its implementation still faces various obstacles, including differences in cybersecurity priorities between countries and limitations in existing cooperation mechanisms.

The current legal framework, although it has provided a foundation for handling cybercrime cases, still needs to be updated to accommodate the latest technological developments. The ITE Law and its amendments have not been able to fully anticipate the complexity of contemporary cybercrime. Legal interpretation of digital evidence also remains a challenge, especially in determining its admissibility and evidentiary weight in court. The high standard of proof in the Indonesian criminal justice system is sometimes difficult to meet in cybercrime cases, given the easily manipulated nature of digital evidence.

Challenges in collecting and analyzing digital evidence are critical aspects of the evidence process. The volatility of digital evidence requires investigators to act quickly and accurately in securing evidence, but this is often hampered by legal procedures that take time, such as the process of obtaining a search warrant. Maintaining the integrity of digital evidence through a strict chain of custody is also a challenge, given the ease of manipulating digital data. Complex evidence analysis, especially in cases involving large volumes of data, requires sophisticated forensic tools and specialized expertise that are not always available.

Presenting digital evidence in court is a crucial stage in the evidentiary process. The gap in technical understanding between investigators, prosecutors, judges, and juries often hinders the effective communication of digital forensic findings. The ability to explain complex technical concepts in a way that is understandable to those without an IT background is required. The use of digital forensic experts in court has helped bridge this gap, but there is still a need to improve digital literacy among law enforcement officers and judges.

To address these challenges, a comprehensive strategy involving various stakeholders is needed. Increasing the capacity of law enforcement through ongoing training programs and investment in digital forensics technology is a top priority. Strengthening international cooperation, including harmonization of cyber law and improving information exchange mechanisms, is needed to handle cross-border cases more effectively. Technological innovation in the development of more sophisticated forensic tools, including the use of artificial intelligence and machine learning in evidence analysis, is also an area that needs to be developed.

The ethical and legal aspects of proving cybercrime cases are also important concerns. The balance between the needs of investigation and the protection of individual privacy is becoming an increasingly relevant issue, especially with the increasing use of surveillance technology. The protection of suspects' digital rights, including the right not to self-incriminate in the digital context, requires careful legal consideration. Strict supervision of the use of investigative technology is needed to ensure that the principles of due process are maintained in the digital environment.

The challenges of proof in cybercrime cases in Indonesia require a holistic approach that combines legal, technological, and ethical aspects. Close collaboration between law enforcement, technologists, academics, and policymakers is key to developing effective and sustainable solutions. As technology continues to play an increasing role in everyday life, the importance of addressing these challenges is increasingly crucial to ensure cybersecurity and the integrity of the justice system in the digital age. Further research and ongoing evaluation of the strategies implemented will be essential to address the future evolution of cybercrime.

CONCLUSION

After understanding the regulation of investigation of cybercrime cases regulated in the Law on Information and Electronic Transactions, it can be concluded that the investigation process is carried out by a team of investigators from the Republic of Indonesia National Police who can be assisted by people who are experts in certain fields related to the case that is under investigation if needed in solving a case by maintaining privacy, data authenticity, and not disrupting public services or public facilities. Searches and/or seizures of electronic systems related to suspected criminal acts must be carried out with the permission of the local District Court.

REFERENCES

Adami, C. (2019). Material and formal criminal law of corruption in Indonesia. Malang: Bayumedia Publishing.

Agus, R. (2018). Legal aspects of handling cybercrime in Indonesia. Jurnal Yuridika, 33(1), 1-15.

Andi, H. (2016). Indonesian criminal procedure law. Jakarta: Sinar Grafika.

Arief, B. N. (2020). Criminal law policy in combating cyber crime. IUS Law Journal Quia Iustum, 27(1), 45-60.

Eddy, O. (2019). Principles of criminal law. Yogyakarta: Cahaya Atma Pustaka.

GreatNugroho. (2021). Technological developments and their implications for cybercrime in Indonesia. Journal of Law & Development, 51(1), 123-138.

H. Sutanto. (2019). Cyber security: Hacking, ethics & network security. Yogyakarta: Andi Offset.

Joshua, S. (2020). Cyberlaw: Legal aspects of information technology. Jakarta: Tatanusa.

Law Number 11 of 2008 concerning Electronic Information and Transactions. (2008). State Gazette of the Republic of Indonesia, No. 58, 2008.

M. Arief, M., & Elistris, G. (2020). Cyber law - Legal aspects of information technology. Jakarta: Refika Aditama.

Oktaplandi, S. (2017). Police obstacles in efforts to combat cyber crime in Indonesia. E-Journal Gloria Yuris, 5(4), 42-57.

Prakoso, A. (2022). Digital forensic challenges in cybercrime law enforcement. Journal of Law and Justice, 11(1), 22-34.

Raharjo, A. (2018). Legal aspects of handling cybercrime in Indonesia. Jurnal Yuridika, 33(1), 15-28.

Sutarman. (2007). Cyber crime modus operandi and its prevention. Yogyakarta: LaksBang PRESSindo.

Widodo. (2009). Criminal system in cyber crime. Yogyakarta: Laksbang Meditama.