Semarang State University Undergraduate Law & Society Review
VOLUME 2 ISSUE 2, JULY 2022

ISSN (Print): 2807-8225 ISSN (Online): 2807-8683

History of Article
Submitted: December 2021
Revised: March 2022
Accepted: May 2022
Available Online: July 2022

How to cite:
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

Victims of Cyber Crimes in Indonesia: A Criminology and Victimology Perspective

Yudha Chandra ARWANA
Faculty of Law, Universitas Negeri Semarang
Jl. Kampus Timur, Sekaran, Gunungpati
Kota Semarang, 50229, INDONESIA
✉ yudhachandra@gmail.com

ABSTRACT. Crimes that occur in cyberspace are born as a result of the negative impact of technological developments, crimes that occur in various forms and types have consequences for the legal protection of users, this is important considering that every human being must be protected in accordance with his dignity as a human being. One form of state responsibility for the protection of its citizens is to provide legal

guarantees and concrete actions that protect the community from all forms of crime or other deviant acts that may be experienced by the community, both in the real world and in cyberspace. Crimes that occur in cyberspace or commonly referred to as cybercrime. This study is aims to analyze and examine the victims of cyber crime in the perspective of criminology and victimology. Criminology approach used to answer the motive, factors, and response of the crime, and victimology approach to understand more comprehensively concerning to the victim's protection and the role of the victims in the cybercrime.

KEYWORDS. *Victim Protection, Cybercrime, Victimology, Criminology*

I. INTRODUCTION

The development of globalization of information today has a very big influence on human life, this development has caused world relations to become limitless which also has an impact on significant social changes in society. The result of this technological development is a double-edged sword because in addition to providing benefits for the welfare and progress of society, it is also followed by the development of crime with various modes that use computers and computer networks as tools such as auction fraud, online gambling, identity fraud, child pornography, terrorists, theft of intellectual property rights and many other crimes that can harm both materially and non-materially for its users and can damage the life of the nation and state (Raodia, 2019; Antoni, 2017).

Crimes that occur in cyberspace are born as a result of the negative impact of technological developments, crimes that occur in various forms

and types have consequences for the legal protection of users, this is important considering that every human being must be protected in accordance with his dignity as a human being. One form of state responsibility for the protection of its citizens is to provide legal guarantees and concrete actions that protect the community from all forms of crime or other deviant acts that may be experienced by the community, both in the real world and in cyberspace. Crimes that occur in cyberspace or commonly referred to as cybercrime (Ramailis, 2020; Djanggih & Qamar, 2018; Wisnu A.S., Wiryawan, & Lanang PP, 2021).

Cybercrime in a narrow sense is a crime against a computer system, while cyber crime in a broad sense includes crimes against computer systems or networks and crimes using computer facilities. All crimes related to cyber crime have been regulated in Law No. 11 of 2008 concerning Information and Electronic Transactions (Fadhila, 2021; Napitupulu, 2017; Putra, 2015).

Cyber crime is a social phenomenon that opens scientific horizons in the legal world, cyber crime is a very powerful crime that is carried out only from in front of a computer without the need to go anywhere. Cyber crime is the dark side of advances in communication and information technology which has a very broad effect in all lines of life because it is closely related to economic crime and organized crime (Anugerah & Tantimin, 2022; Putra, 2015).

The problem of cyber crime is a big problem that has a negative impact as well as a positive effect, therefore laws / regulations are needed to be able to provide order, certainty and legal justice of different sizes and contents in dealing with crimes that arise due to the misuse of technology and information media.

Cybercrime is a crime that uses information technology and is a form of transnational crime that knows no boundaries (borderless), without violence (non violence), no physical contact (no physical contact) and without a name. Cybercrime perpetrators are very difficult to trace and the criminal elements are difficult to prove, especially with the limitations of regulation.

Protection of victims of cyber crime requires high seriousness and expertise from law enforcement officers, law enforcement officers are needed who master high technology in the field of information technology, both police, prosecutors and judiciaries due to the existence of cyberspace that is border state less. It requires a good and measurable cooperation between countries both regionally and globally in order to prevent and overcome the occurrence of transnational crimes such as cyber crime.

Due to the large number of crime cases in a borderless world, a rule of law is needed and its implementation in the field, cooperation between relevant agencies both on a national, regional and international scale in order to tackle, prevent and eradicate all perpetrators of crimes that occur in cyberspace. By conducting investigation efforts, proving and investigating all cyber criminals in order to protect cyberspace users (netizens) from black hackers (crackers).

Legal protection for those who use technology is of course very necessary, this is because when a criminal event occurs, the rule of law often focuses on punishing criminals so that victims of these crimes are often neglected. Even though the victim also deserves attention because basically the victim is the party who is quite disadvantaged in a criminal act. The impact of crime causes victims and losses. The resulting loss can be suffered by the victim himself, or indirectly by other parties (Sahetapy,

1987). The nature of the crime should be seen as something that is detrimental to the victim, therefore the punishment imposed on the violator must also pay attention to the interests of the victim in the form of recovering the losses he has suffered. The losses that must be recovered are not only physical losses but also non-physical losses.

Efforts to protect victims are actually very important. Because in addition to reducing the suffering of victims of the crime they experienced, it can also prevent the occurrence of ongoing victims, so that this can reduce the crime rate (Arief, 2000). For this reason, the author wants to see further how the legal protection for victims of cybercrime in Indonesia is.

II. LEGAL PROTECTION FOR CYBERCRIME VICTIMS IN INDONESIA

The law in principle is a regulation of the attitude (behavior) of a person and society for which the violators are sanctioned by the state. Even though the cyber world is a virtual world, the law is still needed to regulate people's actions, there are at least two things, namely: First, the people who exist in the virtual world are people who exist in the real world, people have values and interests both individually and together. must be protected. Second, even though they occur in cyberspace, transactions made by the public have an impact in the real world, both economically and non-economically (Sitompul, 2012; Afriansyah & Hermansyah, 2018).

Currently, the regulation used as the legal basis for cybercrime cases is Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE). With the existence of the ITE Law, it is hoped that it

can protect the information technology user community in Indonesia, this is important considering the number of internet technology users is increasing from year to year.

Specifically, in the sale and purchase agreement, what is meant by achievement is goods and prices. Meanwhile, in the regulations contained in Bukalapak in detail and in outline, what is meant by the object of the agreement is only the goods mentioned above.

The increasing use of the internet on the one hand provides a lot of convenience for humans in carrying out their activities, on the other hand it makes it easier for certain parties to commit a criminal act, this technological advance also affects the lifestyle and mindset of humans. information. The phenomenon of cybercrime, which is growing rapidly, which does not know any territorial boundaries, must indeed be watched out for because this crime is somewhat different from other crimes in general.

Utilization of Information Technology plays an important role in trade and national economic growth to realize people's welfare, that the government needs to support the development of Information Technology through legal infrastructure and regulations so that the use of Information Technology is carried out safely to prevent its misuse by taking into account the religious and socio-cultural values of the Indonesian people.

In Article 4 paragraph (2) of the ITE Law it is stated that the Government protects the public interest from all kinds of disturbances as a result of the misuse of Electronic Information and Electronic Transactions that disrupt public order, in accordance with the provisions of the Laws and Regulations.

Misuse of this information technology that can harm other people, nations and countries who use computer facilities that have internet facilities carried out by hackers or a group of crackers from a certain home or place without being noticed by the victim which can cause moral, material and time losses as a result of the destruction. data by hackers.

To overcome cybercrime crime, law enforcement officers are needed who understand and master technology, the obstacles faced by victims are due to ignorance, knowledge of computers and the internet so that if they are harmed, they cannot report all criminal events experienced, of course this is a problem for us together.

The principle and purpose of this law is that the use of Information Technology and Electronic Transactions is carried out based on the principles of legal certainty, benefit, prudence, good faith, and freedom to choose technology or be technology neutral. So, it can be interpreted that the use of information technology and electronic transactions is expected to be guaranteed with legal certainty, has benefits, is full of prudence, has good intentions, and has the freedom to choose technology and is neutral (Habibi & Liviani, 2020; Angkasa & Windiasih, 2022).

Responding to the demands and challenges of global communication via the Internet, the Act is expected to be able to answer all legal issues regarding the global development of technology and be anticipatory to all existing problems, including the negative impact of internet abuse which will ultimately cause harm to its users (Jaelani, 2020; Ismail, 2019). There are several other positive laws that are generally accepted and can be imposed on cybercrime perpetrators, especially for cases that use computers as a means as higlighted by Hasyim (2020) and Djanggih, et.al. (2018), including:

1. KUHP (Indonesian Criminal Code)

2. Law Number 11 of 2008 concerning ITE.
3. Law Number 44 of 2008 concerning Pornography.
4. Law Number 36 of 1999 concerning Telecommunications.
5. Law Number 19 of 2002 concerning Copyright.
6. Law Number 5 of 1999 concerning Prohibition of Monopolistic Practices and Unfair Business Competition.
7. Law Number 8 of 1999 concerning Consumer Protection.
8. Law Number 8 of 1997 concerning Company Documents
9. Law Number 25 of 2003 concerning Amendments to Law Number 15 of 2002 concerning the Crime of Money Laundering
10. Law Number 15 of 2003 concerning Combating Terrorism

In maintaining and protecting the community of technology users, cooperation and seriousness of all parties are needed, considering that information technology, especially the internet, has been used as a means to build an information culture society. The existence of laws that regulate cybercrime is expected to protect and provide a sense of security for those who use technology as a forum to conduct transactions and carry out economic activities.

In taking action against those who abuse technological developments, quality human resources are needed who have the ability and expertise in the field of technology. Law enforcement is at least influenced by several factors, namely the rule of law itself or the law, the implementing apparatus of the rule, namely law enforcement officials and the legal culture itself, namely the community itself who is the target of the law (Das & Nayak, 2013).

The electronic information and transaction law (ITE Law) or what is called cyberlaw, is used to regulate various legal protections for activities that use the internet as a medium, both transactions and the use

of information. The ITE Law also regulates various kinds of punishments for crimes via the internet. The ITE Law accommodates the needs of business actors on the internet and society in general to obtain legal certainty by recognizing electronic evidence and digital electronic signatures as legal evidence in court (Hong & Neilson, 2020; Gaoucher, 2010).

With the ITE law, it is hoped that it can provide a sense of security and can protect those who use technology. In addition, in certain circumstances and dangerous for those who are victims of technological crimes are also entitled to legal protection. 13 of 2006 concerning the Protection of Witnesses and Victims (hereinafter as UU PSK) (Widiasari & Thalib, 2022; Saputra, 2016; Arsawati, Darma & Antari, 2021). In the provisions of Article 5 of the UU PSK, it is stated that:

1. A witness and a victim have the right to:
    a. Obtain protection for the safety of his personal, family, and property, and be free from threats related to the testimony that he will, is currently, or has given;
    b. Participate in the process of selecting and determining the form of security protection and support;
    c. Provide information without pressure;
    d. Get a translator;
    e. Free from entangled questions;
    f. Get information about the progress of the case;
    g. Get information about court decisions;
    h. Knowing in the event that the convict is acquitted;
    i. Get a new identity;
    j. Get a new place of residence;
    k. Obtain reimbursement of transportation costs as needed;

l. Get legal advice and/or;
m. Obtain temporary living expenses assistance until the protection period ends.

2. The rights as referred to in paragraph (1) are granted to Witnesses and/or Victims of criminal acts in certain cases in accordance with LPSK decisions.

In the provisions of Article 1 paragraph (2) of the PSK Law states "*a victim is a person who experiences physical, mental and/or economic loss caused by a criminal act*". Victims in this case are those who have been harmed both materially and non-materially as a result of cybercrime. In legal protection for cybercrime victims, there are basically two models, namely the procedural rights model and the service model as higlighted by Muladi & Arief (1992), as follows:

1. The Procedural Rights Model
   In the procedural rights model, victims of cybercrime are given the right to carry out criminal charges or assist prosecutors, or the right to be presented at any level of justice where a statement is needed. In this procedural model, victims are also asked to be more active in assisting law enforcement officers in handling cases, especially those related to modern cybercrime. The existence of procedural rights can also re-establish the victim's confidence after being harmed by those who are not responsible (the defendant), besides that this can also be a consideration for the prosecutor in the event that the prosecutor makes a claim that is too light.
2. Service Model
   This service model focuses on the need to create standard standards for the development of cybercrime victims. This model sees the victim as a person who must be served by the police and other law

enforcement officers, services to victims of cybercrime by law enforcement officers if carried out properly will have a positive impact on law enforcement, especially cybercrime, thus victims of this technological development will have more confidence in institutions. law enforcers by providing services to victims, thus victims will feel that their rights are protected, and their interests are guaranteed. In the trial process, especially with regard to proving cyber crimes, many cases that occur due to the development of information technology, this requires law enforcement officers to prepare reliable human resources, understand, and understand technology, considering that cybercrime is a modern crime that must receive serious attention from the government, because crimes in cyberspace will impact on the real world. With the existence of Law No. 11 of 2008 is expected to assist law enforcement officers in protecting people who use technology.

The importance of legal protection for victims of cyber crime, in addition to realizing the rule of law, this is important to do as a preventive action taken by law enforcement officials in reducing or preventing the occurrence of victims of cyber crime and of course not only as a container for reports but what is expected is there is real action from law enforcement officers so that technology users really feel safe in carrying out their activities in cyberspace.

III. REGULATION OF CYBER CRIME IN THE INDONESIAN CRIMINAL LAW SYSTEM

As a state of law, it is an obligation of the state to protect every citizen from any actions that can damage or harm society, one of which is the

legal protection provided by the state to people who use technology, law and technology are two different words but affect each other and it can also affect people's lives.

The Indonesian legal system has not specifically regulated cyber law (cyber crime) but several laws have regulated the prevention of cyber crime, such as Law Number 36 of 1999 concerning Telecommunications, Law Number 19 of 2002 concerning Copyright, Law No. -Law Number 15 of 2003 concerning Countering Terrorism, Law Number 11 of 2008 concerning Information and Electronic Transactions. These laws and regulations have criminalized the types of cyber crimes and the threat of punishment for each violator (Raharjo & Sudrajat, 2018; Siregar & Sinaga, 2021; Amin & Huda, 2021)

Broadly speaking, cyber crimes are all criminal acts using facilities or with the help of an electronic system, this means that all conventional criminal acts in the Criminal Code (KUHP) as long as using assistance or means such as terrorism, trafficking in persons, can include in the category of cyber crime in a broad sense as well as banking crimes and money laundering. However, in a narrow sense, the regulation of cyber crimes is regulated in Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE). In this ITE Law, several criminal acts that fall into the cybercrime category are grouped, namely:

1. Criminal acts related to illegal activities, namely:
    a. Distribution or dissemination, transmission, accessibility of illegal content consisting of:
        1) Morals (Article 27 paragraph (1) UU ITE)
        2) Gambling (Article 27 paragraph (2) of the ITE Law)
        3) Insults and defamation (Article 27 paragraph (3) of the ITE Law)

4) Extortion or threats (Article 27 paragraph (4) UU ITE)
5) Fake news that misleads and harms consumers (Article 28 paragraph (1) of the ITE Law)
6) Generating hatred based on SARA (Article 28 paragraph (2) of the ITE Law)
7) Sending information that contains threats of violence or intimidation aimed at personally (Article 29 of the ITE Law)

b. In any way by conducting illegal access (Article 30 of the ITE Law):
1) Every person intentionally and without rights and against the law accesses Computers and/or Electronic Systems belonging to other people in any way.
2) Everyone intentionally and without rights or against the law accesses a computer and/or Electronic System in any way with the aim of obtaining Electronic Information and/or Electronic Documents.
3) Any person intentionally and without or against the law accessing a computer and/or Electronic System in any way by violating, breaking through, exceeding, or breaking into the security system.

c. Illegal interception of information or electronic documents and electronic systems (Article 31 UU ITE)
Everyone intentionally and without rights or against the law intercepts or intercepts Electronic Information and/or Electronic Documents in a certain Computer and/or Electronic System belonging to another person.

2. Crime related to interference

a. Interference with Information or Electronic Documents (data interference Article 32 of the ITE Law)
b. Interference with Electronic Systems (system interference Article 33 of the ITE Law)

3. The crime of facilitating prohibited acts (Article 34 of the ITE Law)
   1) Any person who knowingly and without rights or unlawfully produces, sells, reproduces for use, imports, distributes, makes available, or owns:
   2) Computer hardware or software designed or specifically developed to facilitate the actions as referred to in Article 27 to Article 33
   3) Password via Computer, Access Code or something similar which is intended to make the Electronic System accessible with the aim of facilitating the actions as referred to in Article 27 to Article 33.
4. The crime of falsifying information or electronic documents (Article 35 of the ITE Law)
5. Additional crime (accessoir Article 36 UU ITE)

The ITE Law also regulates formal criminal acts, particularly in the field of investigation. Article 42 of the ITE Law stipulates that the investigation of criminal acts in the ITE Law is carried out based on the provisions in Law No. 8/1981 on the Criminal Procedure Code (KUHAP) and the provisions in the ITE Law. This means that the investigation provisions in the Criminal Procedure Code remain valid as long as it is not regulated otherwise in the ITE Law. With the existence of material and formal rules that regulate crime in cyberspace, at least it can help law enforcement officers in dealing with crimes that occur in cyberspace, both conventional crimes and modern crimes. With the hope of providing a

sense of security for the information technology user community, considering that this technology crime does not know space and time and can happen to anyone and at any time.

The criminalization policy which is included in the category of cybercrime has been formulated in the Draft Criminal Code (RKUHP) as formulated in the second book: Criminal Acts, Chapter VIII: Crimes that endanger public safety for people, goods, the environment, Part Five: Crimes against Informatics and Telematics Article 373-Article 379, which regulates criminal acts of illegal access, illegal interception, data interference and system interference, abuse of domain names, and child pornography.

With the existence of material and formal rules that regulate crime in cyberspace, at least it can help law enforcement officers in dealing with crimes that occur in cyberspace, both conventional crimes and modern crimes. With the hope of providing a sense of security for the information technology user community, considering that this technology crime does not know space and time and can happen to anyone and at any time.

In the discourse of the development of criminal law in the future, the countermeasures against cyber crime need to be balanced with the improvement and development of the criminal law system as a whole, which includes the development of the structure, culture, and substance of criminal law.

IV. CONCLUSION

This study come into conclusion that in providing legal protection for victims of cybercrime, the government has issued Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE). The ITE Law

also regulates various kinds of punishments for crimes via the internet. The ITE Law accommodates the 112 needs of business actors on the internet and society in general to obtain legal certainty with the recognition of electronic evidence and digital electronic signatures as legal evidence in court. live in cyberspace and the transactions that occur in it. Prohibited acts (cybercrime) are described in Chapter VII (articles 27-37). Furthermore, if necessary for certain cases, victims of cybercrime can request assistance from the LPSK and furthermore regarding legal protection for witnesses and victims of crime is regulated in Law Number 13 of 2006 concerning Protection of Witnesses and Victims (UU PSK). In legal protection of victims of cybercrime, there are basically two models of approaches that can be used, namely: 1) the model of procedural rights in this case the victim plays a more active role and can assist prosecutors in carrying out prosecutions and the right to be present at every level of the judicial process and 2) model Services in this case see the victim as a person who must be served by the police and other law enforcement officers, thus the victim will feel that his interests are guaranteed in a fair atmosphere.

V. REFERENCES

Afriansyah, R., & Hermansyah, A. (2018). Tinjauan Kriminologis Terhadap Penipuan Lowongan Kerja Melalui Facebook. *Jurnal Ilmiah Mahasiswa Bidang Hukum Pidana*, *2*(2), 297-308.

Amin, M. E., & Huda, M. K. (2021). Harmonization of Cyber Crime laws with the Constitutional Law in Indonesia. *International Journal of Cyber Criminology*, *15*(1), 79-94.

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.

Antoni, A. (2017). Kejahatan Dunia Maya (Cyber Crime) Dalam Simak Online. *Nurani: Jurnal Kajian Syari'ah dan Masyarakat*, *17*(2), 261-274.

Anugerah, F., & Tantimin, T. (2022). Pencurian Data Pribadi di Internet dalam Perspektif Kriminologi. *Jurnal Komunikasi Hukum (JKH)*, *8*(1), 419-435.

Arsawati, I. N. J., Darma, I. M. W., & Antari, P. E. D. (2021). A Criminological Outlook of Cyber Crimes in Sexual Violence Against Children in Indonesian Laws. *International Journal of Criminology and Sociology*, *10*, 219-223.

Das, S., & Nayak, T. (2013). Impact of cybercrime: Issues and challenges. *International Journal of Engineering Sciences & Emerging Technologies*, *6*(2), 142-153.

Djanggih, H., & Qamar, N. (2018). Penerapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime). *Pandecta Research Law Journal*, *13*(1), 10-23.

Djanggih, H., Thalib, H., Baharuddin, H., Qamar, N., & Ahmar, A. S. (2018, June). The effectiveness of law enforcement on child protection for cybercrime victims in Indonesia. In *Journal of Physics: Conference Series* (Vol. 1028, No. 1, p. 012192). IOP Publishing.

Fadhila, A. P. (2021). Tinjauan Kriminologi Dalam Tindakan Penipuan Ecommerce Berdasar Peraturan perundang-undangan Pada Masa Pandemi Covid19 di Indonesia. *Jurnal Suara Hukum*, *3*(2), 274-299.

Goucher, W. (2010). Being a cybercrime victim. *Computer Fraud & Security*, *2010*(10), 16-18.

Habibi, M. R., & Liviani, I. (2020). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. *Al-Qanun: Jurnal Pemikiran dan Pembaharuan Hukum Islam*, *23*(2), 400-426.

Hasyim, A. F. (2020). Implementasi Perlindungan Korban Cyber Crime dalam Bidang Perbankan dalam Peraturan Hukum Pidana Indonesia. *Jurnal Pro Justice: Kajian Hukum dan Sosial*, *1*(2), 1-12.

Hong, Y., & Neilson, W. (2020). Cybercrime and punishment. *The Journal of Legal Studies*, *49*(2), 431-466.

Ismail, M. (2019). Kebijakan Hukum Pidana Cyberpornography Terhadap Perlindungan Korban. *Jurnal Hukum Ekonomi Syariah*, *1*(2), 117-134.

Jaelani, N. H. (2020). Tinjauan Viktimologis Terhadap Korban Tindak Pidana Cybercrime Illegal Content di Wilayah Hukum Polrestabes Bandung Dihubungkan dengan Undangundang No 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. *Varia Hukum*, *2*(1), 65-87.

Napitupulu, D. (2017). Kajian Peran Cyber Law dalam Memperkuat Keamanan Sistem Informasi Nasional. *Deviance Jurnal Kriminologi*, *1*(1), 100-113.

Oktaviana, E. P., & Priambada, B. S. (2022). Tinjauan Viktimologi Terhadap Korban Tindak Pidana Cybercrime Illegal Content. *Rechtstaat Nieuw: Jurnal Ilmu Hukum*, *6*(2), 74-87.

Putra, E. N. (2015). Kejahatan Tanpa Korban Dalam Kejahatan Cyberporn. *Jurnal Cakrawala Hukum*, *6*(1), 1-12.

Rafi, M., & Amri, P. (2022). The Importance of Strengthening Legal Concepts in Overcoming Cybercrime During the Covid-19 Pandemic in Indonesia. In *International Conference on Human-Computer Interaction* (pp. 469-479). Springer, Cham.

Raharjo, A., & Sudrajat, T. (Eds.). (2018, November). Legal protection for cyber crime victims on victimological perspective. In *SHS Web of Conferences* (Vol. 54, p. 08004). EDP Sciences.

Ramailis, N. W. (2020). Cyber Crime dan Potensi munculnya Viktimisasi Perempuan di Era Teknologi Industri 4.0. *Sisi Lain Realita*, *5*(01), 1-20.

Raodia, R. (2019). Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (Cybercrime). *Jurisprudentie: Jurusan Ilmu Hukum Fakultas Syariah dan Hukum*, *6*(2), 230-239.

Saputra, R. W. (2016, July). A survey of cyber crime in Indonesia. In *2016 International Conference on ICT For Smart Society (ICISS)* (pp. 1-5). IEEE.

Siregar, G., & Sinaga, S. (2021). The Law Globalization in Cybercrime Prevention. *International Journal of Law Reconstruction*, *5*(2), 211-227.

Widiasari, N. K. N., & Thalib, E. F. (2022). The Impact of Information Technology Development on Cybercrime Rate in Indonesia. *Journal of Digital Law and Policy*, *1*(2), 29-42.

Wisnu A. S., M., Wiryawan, I. W. G., & Lanang PP, K.S. (2021). Faktor Penyebab Terjadinya Kejahatan Cyber Crime yang Dilakukan oleh Orang Asing di Bali Ditinjau dari Perspektif Kriminologi. *Jurnal Yusthima*, *1*(01), 58-70.

Conflicting Interest Statement

All authors declared that there is no potential conflict of interest on publishing this article.

Funding

None

Publishing Ethical and Originality Statement

All authors declared that this work is original and has never been published in any form and in any media, nor is it under consideration for publication in any journal, and all sources cited in this work refer to the basic standards of scientific citation.