Protection of Victims of Cybercrime in the Era of Industrial Technology 4.0

Submitted: 23 January 2025
Reviewed: 2 May 2025
Revised: 26 July 2025
Accepted: 27 July 2025

Article submitted to peer blind review

Gde Made Swardhana[*]
https://orcid.org/0009-0004-5969-3662
Sagung Putri M.E. Purwani[**]
https://orcid.org/0009-0009-0849-1506
Danial Kelly[***]
https://orcid.org/0000-0002-2895-6675

DOI: https://doi.org/10.26512/lstr.v17i2.56952

Abstract

[Purpose] To ascertain and examine the legal protection available to victims of cybercrime in the context of the advent of Industrial Technology 4.0.

[Methodology/approach/design] This paper employs a normative legal research method, utilising a literature study approach to examine the relevant laws, books and journals pertaining to this study. In Indonesia, positive law regulates all acts that are considered deviant and in need of legal regulation, including cybercrime. The prevalence and diversity of cybercrime are on the rise, with perpetrators targeting an increasing number of victims.

[Findings] Legal protection for victims of cybercrime in the context of industrial technology 4.0 is enshrined in various legislative instruments. Nevertheless, despite this legal framework, the evolving nature of cybercrime necessitates a more robust approach to ensure that victims are adequately safeguarded.

Keywords: Cybercrime. Legal Protection. Victims. Industrial Technology 4.0. Legal Arrangements.

[*]Professor of Criminal Law, with expertise in criminology, victimology, and cyber law. He is an active member of faculty at the University of Udayana, where he specialises in criminal law. E-mail: gdmade_swardhana@unud.ac.id.

[**]Associate Professor in the fields of Criminal Law, Health Law, Cyber Law, and Victimology. She occupies the position of Head of the Research and Community Service Unit at the Faculty of Law, Udayana University, and is also an active member of the teaching faculty at the same institution. E-mail: sagung_putri@unud.ac.id.

[***]Associate Professor in Indonesian Law at Charles Darwin University, Australia. He is an active lecturer at the same university and has provided research support at Udayana University and several institutions in Indonesia on numerous occasions. E-mail: danial_kelly@cdu.edu-au.

INTRODUCTION

The increasing sophistication of mobile phone technology is enabling the emergence of a range of innovative developments on an annual basis. Mobile phones serve a dual function: as a means of communication and as a conduit for the exchange of information, both in close proximity and at a distance. The advent of the internet has given rise to a new form of criminal activity, known as cybercrime, which has the potential to cause significant harm (Anggusti, 2022). The term "cybercrime," as defined by Barda Nawawi Arief, is synonymous with "mayantara crime." The term 'mayantara crime' as defined by Barda Nawawi Arief is intended to encompass criminal offences committed in the context of cyberspace, which are more commonly referred to as 'cybercrime' (Arief, 2003).

The use of technology, particularly information technology, including computers and the internet, has led to a significant increase in criminal activities, which are collectively known as cybercrime. The advancement of information technology has brought about a revolutionary change in the business world, which has become increasingly digitalised. However, this digital revolution has also given rise to a number of problematic issues, including the proliferation of pornography, computer crime, digital terrorism, information warfare and hacking (Siregar & Sinaga, 2021). The issue of lawlessness, or crime, is a responsibility shared by all members of society. It is not only a phenomenon that has existed throughout history; it is also a fundamental aspect of social development. The mere mention of crime is indicative of social insecurity and a potential threat to the social order (Gojali, 2023). It is therefore unsurprising that communities demonstrate a range of attitudes in response to this issue (Wahid & Labib, 2005).

The Internet and information technology represent a significant innovation in the last decade, exerting a profound influence on the lives of individuals across the globe (Hermanto, 2023). A number of human activities have undergone significant changes as a result of the increased efficiency, effectiveness and mobility afforded by these developments (Amin & Huda, 2021). It is, however, unfortunate that these technological advancements also give rise to new problems when they are used inappropriately or improperly (Sugama & Hariyanto, 2021). The phenomenon of cybercrime represents an unprecedented new form of threat to the global community. A series of internet crimes, including hacking, cracking, defacing, sniffing, carding, phishing, spamming, and scamming, have emerged as a significant threat to the global community, causing substantial losses to numerous individuals and entities.

These crimes are facilitated by computer networks or devices and have as their main target independent computer networks or devices (Sumarwani,

2014). The various types of cybercrime that occur in Indonesia in the 4.0 era have a significant impact on both the victims and the global community. This is because these crimes utilise digital communication tools, which are currently a primary necessity for all Indonesian people, and can be used to commit a range of real crimes as outlined in the preceding paragraph. Consequently, despite the virtual nature of cyber activities, they can be classified as tangible legal actions and deeds. From a legal standpoint, it is no longer feasible to categorise cyber activities and objects using the same legal qualifications as those employed for conventional activities and objects. This is because doing so would result in an unmanageable number of legal issues and instances of lawlessness going unaddressed. Cyber activities are virtual activities with a tangible impact, despite the electronic nature of the evidence (Yusa, et.al., 2021). Consequently, the perpetrator must also be regarded as a person who has committed a genuine legal act.

The article's research is distinctive in comparison to previous studies on this topic, including the work of Manthovani (2023). Unlike this earlier study, the article's research addresses the ongoing challenges in law enforcement related to cybercrime in Indonesia. The formulation of criminal policies. However, when compared to the article written at this time, this research also focuses on encouraging aspects of access to justice and the realisation of substantive justice for witnesses and victims in relation to the dynamics of the development of cybercrime regulations in Indonesia. Furthermore, when compared to the work of Azmi (2020), which asserts that the formulation of cyber law in Indonesia is lagging behind the dynamics of the Industrial Revolution 4.0, the research of the article written at this time is particularly noteworthy for its emphasis on encouraging aspects of regulations that reflect substantive justice in addressing the negative potential of the Industrial Revolution 4.0 against various areas of life that require the role of cyber. Ultimately, Imran (2023) posited that cybercrime must be addressed through a system-based and context-specific approach. However, this is deemed inadequate in the current research article due to the necessity for aspects of substantive justice and the implementation of criminal law policies in cybercrime that foster certainty, justice, and benefits for victims and witnesses.

In light of the shortcomings identified in the preceding studies, this article is specifically designed to examine the advent of new technologies has given rise to a new phenomenon: crimes committed in cyberspace. These crimes, which manifest in various forms and types, have significant implications for the legal protection of users. It is imperative that every individual is safeguarded in accordance with their inherent 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.

In light of the aforementioned conditions, it is imperative to establish a set of regulations that specifically address computer crime and legal protection against the use of information technology, media, and communication. This is crucial for the optimal development of these fields. In order to address the aforementioned issues, the government enacted Law No. 11/2008 on Electronic Information and Transactions (ITE Law) on 21 April 2008.

In light of this, the following questions will be examined:

1. How is the positive legal regulation of cybercrime in Indonesia?
2. How is the protection of victims of cybercrime in the era of industrial technology 4.0?

RESEARCH METHODOLOGY

This study employs a normative juridical research method, as outlined by Hutchinson and Duncan (2012), which focuses on examining legal norms through the analysis of statutes, legal concepts, and factual contexts (Sudiarawan et al., 2020). The methodology integrates a statutory approach, legal conceptual approach, and legal fact approach to provide a structured framework for analysing the protection of victims of cybercrime in Indonesia. Legal materials used in this research comprise primary sources (such as legislation and court decisions), secondary sources (such as academic journals and legal commentaries), and tertiary sources (such as encyclopaedias and legal dictionaries). These sources were collected through a comprehensive literature review and analysed using interpretation and legal systematisation techniques (Hutchinson, 2015).

Importantly, the research does not merely describe the legal texts, but it also seeks to examine the underlying normative values, particularly those embedded in victimology theories. Victimology, as a theoretical foundation, explores the position, treatment, and rights of victims within the criminal justice system. This research uses these theoretical perspectives—such as the concept of secondary victimization, victim precipitation theory, and general victim rights theory—as lenses through which to analyse the Indonesian legal framework. These theories help identify the extent to which Indonesian legislation accommodates the psychological, social, and legal needs of cybercrime victims.

In line with Suartha et al. (2022), the methodology juxtaposes the normative ideals found in legislation with the practical realities experienced by victims. It explores whether current laws adequately reflect the insights from

victimology and whether victims are meaningfully protected or, conversely, further harmed by the legal process. The analysis aims to reveal potential dissonances between legal ideals and implementation practices, and to highlight gaps where victimological concerns are underrepresented.

Given its nature, this study is descriptive-analytical. It does not only map out existing laws and regulations but critically examines them through the prism of victimology, with a specific focus on how Indonesian law responds to the distinct and evolving challenges of cybercrime victimisation. In doing so, it seeks to contribute a prescriptive insight into how laws might be refined to better serve and protect victims in the digital era.

RESULTS AND DISCUSSION

The legal framework for cybercrime in Indonesia

The term "cybercrime" encompasses a range of activities that involve the misuse of the internet, which may extend beyond the boundaries of conventional criminality (Swardhana, Anggarita, & Kurniawan, 2022). The term "computer crime" is generally understood to refer to criminal activities that require a specific level of expertise in computer technology. The legislation is insufficiently agile to accommodate the evolving landscape of computer technology, which is characterised by rapid advancements and transformations. The Internet, as a consequence of technological engineering, utilises both sophisticated computer technology and telecommunications technology in its operation.

Cybercrime exhibits distinctive characteristics compared to conventional crime. These include (Setiawan, 2005):

a. The perpetrators engage in illegal, unethical, or unscrupulous acts in cyberspace, making it challenging to ascertain which country's legal jurisdiction applies to the crime.

b. The perpetrators utilise any equipment that can connect to the internet to commit the act.

c. The act results in material and immaterial losses, including time, value, services, money, goods, self-esteem, dignity, and the confidentiality of information. These losses are often greater than those associated with conventional crimes.

d. The perpetrators are individuals who possess expertise in the use of the internet and its applications. Such acts are frequently perpetrated on a transnational scale, traversing national borders.

The function of legal instruments is to provide a foundation or guideline for law enforcement agencies in the application of legislation to cybercrime

offenders (Nadriana & Sukmana, 2022). As a positive law, its formation is undoubtedly achieved through the legislative process, while simultaneously aligning with the characteristics of *ius constitutum*, a positive law that imposes penalties for criminal activities involving computers. The establishment of laws and regulations in the cyber realm is predicated on the community's aspiration to attain security, justice, and legal certainty. As a norm of cyber law, it is binding for each individual to submit to and comply with all the rules set forth therein. The criminal justice system comprises four principal components: the police, prosecutors, courts and correctional institutions.

Regulation represents a means of controlling information technology crime (Purwani & Dewi, 2022). Information technology crime, otherwise known as cybercrime, may take the form of rules that are currently in force (ius constitutum) or rules that will be enacted in the future (ius constituendum) (Hermanto & Aryani, 2021). The term "cybercrime" is used to describe criminal activities that are conducted in cyberspace using information technology, particularly the internet. In this context, Indonesian Criminal Law represents the material criminal law. It constitutes part of the overall legislation applicable in Indonesia, providing the basis and rules for determining three key issues:

a) The problem of criminal acts,

b) The problem of criminal liability, and

c) Criminal sanctions (Lamintang, 1997).

Cybercrime is a broad category that includes illegal activities conducted over the internet, often exploiting technological advancements to commit crimes such as fraud, identity theft, and hacking. These activities pose unique challenges for law enforcement, as cybercriminals can operate across national borders, using digital platforms to perpetrate crimes that are difficult to trace and prosecute.

With regard to the regulation of cybercrime penalties in Indonesia, it can be observed that the majority of cybercrime offences in Indonesia have not been clearly defined in legal norms within the country's legislation. Consequently, in cases of cybercrime, the provisions of the Criminal Code and those set out in laws outside the Criminal Code are applied (Hermanto, 2021). Cybercrime often involves activities such as hacking, phishing, and the unauthorized access to private data. Under the current legal framework, crimes like these can be prosecuted under provisions in the Criminal Code (KUHP), including those related to criminal offences of forgery (as delineated in Articles 263 to 276), criminal offences of theft (as outlined in Articles 362 to These include criminal offences of forgery (as regulated in Articles 263 to 276), criminal offences of theft (as regulated in Articles 362 to 377), and criminal offences of damage to property (as regulated in Articles 407 to 412) (Laksana, 2019).

The application of articles of the Criminal Code in cases where the computer is the target of the crime and cases where the computer is used as a means of crime can be categorised as follows:

1) The destruction of goods used for evidence before the authorities
2) Theft
3) Fraudulent competition

Those who perpetrate cybercrime do not possess any distinctive characteristics, except in relation to their proficiency in the use of computers and information technology. Criminals employ information technology media to identify and exploit their victims (Pane & Situmeang, 2011). Similarly, victims of cybercrime are individuals and institutions (business and state) that utilise information technology. The forms of crime categorised as cybercrime include carding, which is the misuse of other people's credit card numbers to purchase goods through online services.

Carding can be defined as a form of forgery or fraud under the criminal law of a given jurisdiction, representing an offence that has been committed in the past (den Bergh & Junger, 2018). The act of illegally gaining access to another individual's website via the Internet with the intention of demonstrating that the security techniques employed by the website owner can be circumvented (Swardhana, 2021). Hacking may be considered a form of intrusion into an individual's private domain without their consent. Cracking is similar to hacking, but involves gaining access to a computer program and potentially causing damage to it (Robalo & Razwana, 2023). Cracking can be classified as criminal damage, which is also referred to as vandalism in the field of criminology. Spamming can be defined as the sending of unsolicited electronic mail (e-mail) to addresses that do not require such communication from the recipient. The recipient is unaware of, and has no prior relationship with, the sender (Yusa, 2017). The emails in question are typically advertisements offering a variety of goods and services, including pornography. In the context of criminal law, spamming can be considered an unpleasant act. If the email is sent to a specific recipient and the content of the letter contains words that defame or threaten the recipient, then the act is referred to as cyber stalking. The criminal act of e-commerce-based fraud is, in essence, analogous to conventional fraud (Rahmanto, 2019).

In addition to the aforementioned forms of criminal activity, information technology can be exploited for the distribution of pornographic material, copyright infringement, and other illicit purposes. Furthermore, information technology-based accounting can also be misused, which is essentially the same as manual accounting or bookkeeping fraud. Given the ongoing advancement of information technology and the emergence of new technologies that may not be

fully regulated, it is imperative for the government to anticipate and address potential legal issues promptly (Djanggih & Qamar, 2018).

In Indonesia, the legislative framework pertaining to cybercrime is currently anchored in the Information and Transactions (ITE) Law. However, it is regrettable that the current enforcement pattern is still not optimal and often appears to be a mere formality. The use of electronic documents as evidence in criminal cases is still a relatively new phenomenon in the context of cyber space, as the relevant legislation does not currently permit this (Subawa & Hermanto, 2023). The number of cybercrime activities is currently increasing at a rapid rate, due to the high number of internet and social media users (Hong & Neilson, 2020). It is evident that the majority of individuals possess sophisticated mobile devices, namely personal mobile phones and Android devices, which are utilised on a daily basis for communication and financial transactions, including business-related activities. (Yudha, et.al. 2023)

This should prompt greater vigilance to prevent the occurrence of crimes in the digital domain, whether against ourselves, our immediate family and friends, or our business colleagues.

The current legal basis for cybercrime cases is Law Number 11/2008 on Electronic Information and Transactions (ITE) (Bunga, 2019). The enactment of the ITE Law is intended to safeguard the users of information technology in Indonesia, a goal that is particularly crucial in light of the exponential growth in the number of internet technology users on an annual basis. The increasing use of the internet provides convenience for humans in carrying out their activities. However, it also facilitates criminal acts by certain parties. Technological advancement affects human lifestyle and mindset (Astariyani, et.al. 2023). Currently, there are numerous crimes using information technology. The rapidly growing phenomenon of cybercrime, which has no territorial boundaries, must be monitored because this crime is somewhat different from other crimes in general.

The Electronic Information and Transaction Law (ITE Law), also referred to as cyberlaw, is employed to oversee the implementation of legal safeguards pertaining to activities conducted via the Internet, encompassing both transactions and the utilisation of information (Jhon, 2018). Furthermore, the ITE Law prescribes a range of penalties for offences committed online. The ITE Law is designed to accommodate the needs of business actors on the internet and the public in general with regard to the recognition of electronic evidence and digital electronic signatures as valid evidence in court (Wijaya & Arifin, 2020). The ITE Law itself is a relatively recent phenomenon in Indonesia, having been passed by the DPR on 25 March 2008. The ITE Law is comprised of 13 chapters and 54 articles, which provide a comprehensive examination of

the rules governing activities in cyberspace and the transactions conducted therein.

Indonesia's legal response to cybercrime is primarily anchored in a combination of general criminal law provisions and specific regulations addressing digital crimes. As cybercrime evolves, so too does the need for robust legal frameworks to address these new and increasingly sophisticated criminal activities. The ITE Law (Electronic Information and Transactions Law) plays a pivotal role in this regard, alongside provisions in the Criminal Code (KUHP), Telecommunications Law, and various other laws that apply to specific forms of cybercrime.

The ITE Law was enacted in 2008 to regulate activities related to electronic transactions, cybercrimes, and the use of the internet. It offers legal protections for individuals and businesses against cybercrimes such as hacking, cyber fraud, and defamation through digital means. However, there are significant challenges associated with this law, particularly in its ability to address the rapid development of digital technologies and the increasing complexity of cybercrime. The law has been criticized for being overly broad and, in some cases, vague, especially when it comes to defining certain digital crimes.

In parallel with the ITE Law, other provisions in the Criminal Code serve to address various forms of cybercrime. For example, crimes such as fraud and identity theft can be prosecuted under the sections related to theft (Articles 362 to 377) and forgery (Articles 263 to 276). In these cases, the internet serves as a tool for committing traditional crimes, such as stealing money or falsifying documents, but with the added complexity of digital means.

In addition, Law No. 36 of 1999 on Telecommunications plays a critical role in addressing crimes such as illegal interception of communications and hacking. As technology advances, however, some argue that these legal frameworks need to be updated to provide more comprehensive coverage and to keep pace with emerging forms of cybercrime, such as cyberbullying, phishing, and ransomware attacks.

Furthermore, Indonesia's legal system has been slow to incorporate international treaties and agreements on cross-border cybercrime. Given that cybercrime often occurs transnationally, Indonesia's failure to fully engage with international conventions like the Budapest Convention on Cybercrime is seen as a significant gap in the legal framework. The lack of international cooperation complicates the investigation and prosecution of cybercriminals who operate across borders.

In conclusion, while Indonesia has made significant strides in addressing cybercrime through the ITE Law and Law No. 27 of 2022 concerning Data

Protection, there remains a need for ongoing legal reform. Moving forward, it is crucial that the Indonesian government continues to refine and expand these legal frameworks to better protect citizens and businesses from the risks of cybercrime. Efforts should focus on both on clarifying existing laws, closing gaps in regulation, improving the enforcement capabilities of law enforcement agencies, especially in handling digital evidence, prosecuting cybercriminals who often operate anonymously across borders, and increasing international cooperation to effectively combat the growing threat of cybercrime.

Protection for victims of cybercrime in the context of industrial technology 4.0

The accelerated evolution of computer and information technology has led to the emergence of new forms of criminal activity that exploit these technologies. This phenomenon is commonly referred to as cybercrime (Drew & Farrell, 2018). The advent of communication technology has had a profound impact on human communication behaviour, facilitating ease of communication and conferring numerous benefits. However, this technological advancement also presents a number of challenges and potential risks (Fuady, 2015).

As cybercrime continues to evolve, the protection of victims has become an increasingly important aspect of the legal and law enforcement response. Cybercrimes, such as identity theft, fraud, and cyberbullying, can have devastating impacts on individuals and businesses, both financially and emotionally. Thus, ensuring that victims are provided with adequate legal protections and support services is crucial in mitigating the harm caused by these crimes.

In Indonesia, the legal framework provides several avenues for the protection of victims of cybercrime. The ITE Law includes provisions for victims to seek legal redress, and the Criminal Code allows for the prosecution of cybercriminals who cause harm to others. However, victims often face significant barriers in accessing justice, including a lack of awareness about their rights and difficulties in proving the existence of digital crimes.

One of the most important aspects of victim protection is the provision of legal remedies. Under Indonesian law, victims of cybercrime have the right to report crimes to the police and seek restitution for damages caused by the crime. This can include financial compensation for losses resulting from fraud or identity theft, as well as protection from further harm, such as in the case of online harassment or cyberbullying.

In addition to legal remedies, victims of cybercrime often require psychological and emotional support, especially in cases involving

cyberbullying or online defamation. Victims of these crimes may experience significant mental distress, and law enforcement agencies, along with NGOs, must provide resources for counseling and support. Furthermore, Indonesia has enacted victim protection laws, such as Law No. 13 of 2006 concerning Witness and Victim Protection, which ensures that victims of serious crimes, including cybercrimes, receive necessary protection and assistance.

In certain circumstances and in the event of victimisation at the hands of those perpetrating technological crimes, legal protection is also afforded to such individuals, as set forth in Law Number 13 of 2006 concerning Witness and Victim Protection (UU PSK). In the provisions of Article 5 of the aforementioned Law on Witness and Victim Protection, it is stated that:

1) A witness and victim are entitled to:

a. Obtain protection for their personal safety, family, and property, and to be free from threats related to the testimony they will, are, or have given;

b. Participate in the process of selecting and determining the form of protection and security support;

c. Provide testimony without pressure;

d. Receive an interpreter;

e. Be free from incriminating questions Furthermore, the following rights are to be afforded to witnesses and victims:

f. Receive information on the progress of the case;

g. Receive information about court decisions;

h. Be informed in the event that the convicted person is released;

i. Obtain a new identity;

j. Get a new place of residence;

k. Obtain reimbursement of transport costs in accordance with the needs;

l. Receive legal advice and/or;

m. Obtain temporary living expenses until the protection time limit expires.

2) The rights set forth in paragraph (1) shall be granted to witnesses and/or victims of criminal offenses in certain cases, in accordance with the decision of the LPSK.

Moreover, Article 1, paragraph (2) of the SFM Law defines a victim as "a person who has suffered physical, mental and/or economic loss as a result of a criminal offence." In this context, victims are defined as individuals who have suffered material and non-material harm as a result of cybercrime (Anwary, 2022).

For example, Article 5 of the Witness and Victim Protection Law grants victims the right to be shielded from threats, harassment, or intimidation by the perpetrator, and provides avenues for receiving new identities, relocation, and

financial assistance. This is particularly relevant in cases of cyberstalking or revenge pornography, where the perpetrator may continue to harass or harm the victim even after the crime has occurred.

In the context of legal protection for victims of cybercrime, two principal models have emerged: the procedural rights model and the service model.

1.The procedural rights model is one such approach. In the procedural rights model, victims of cybercrime are afforded the opportunity to file criminal charges or provide assistance to the prosecutor, or to be present at any level of court where their testimony is required. This model implicitly allows the victim to "retaliate" against the perpetrator of the crime that has harmed them. In this procedural model, victims are also required to play a more active role in assisting law enforcement officials in the handling of their cases, particularly in the context of modern cybercrime. The existence of procedural rights can also serve to restore the trust of victims after they have been harmed by those who are not responsible (defendants). Furthermore, this can also be a consideration for the prosecutor in the event that the prosecutor makes charges that are too light.

2. The Service Model (henceforth referred to as "the Model") is concerned with the necessity of establishing uniform standards for the assistance of individuals who have fallen victim to cybercrime. This model regards victims as individuals who must be assisted by the police and other law enforcement agencies. If carried out effectively, the provision of services to cybercrime victims by law enforcement officers will have a positive impact on law enforcement, particularly in the context of cybercrime. Consequently, victims of this technological development will have greater trust in law enforcement institutions and the services they provide. This will lead to a perception that their rights are protected and their interests are safeguarded. In the context of the trial process, particularly in cases pertaining to the prosecution of cybercrime, the advent of information technology has given rise to a number of challenges. This underscores the need for law enforcement agencies to cultivate a cadre of reliable personnel who possess a deep understanding of and familiarity with the intricacies of technology (Djanggih, 2018). The prevalence of cybercrime as a contemporary phenomenon necessitates the allocation of significant attention from the government, as the crimes committed in the digital domain can have tangible consequences in the tangible world. It is anticipated that Law Number 11 of 2008 and Law Number 19 of 2016 courted and assist law enforcement officers in the protection of the community utilising technology.

The protection of victims of cybercrime is a priority for law enforcement agencies, particularly the police. In order to combat the prevalence of criminal activity in cyberspace (Halder & Jaishankar, 2015), law enforcement has

implemented various measures, including the dissemination of information to the technology-using community. It has correlations with Law Enforcement and Cybercrime Investigations matters.

Law enforcement plays a crucial role in the detection, investigation, and prosecution of cybercrime in Indonesia. However, the nature of cybercrime presents unique challenges for traditional law enforcement agencies, as cybercriminals often operate anonymously and across international borders. Effective cybercrime investigations require specialized training, advanced technology, and a comprehensive understanding of digital platforms.

The Cybercrime Unit within the Indonesian National Police (Polri) is tasked with investigating cybercrimes, including hacking, identity theft, and online fraud. This unit works closely with other branches of law enforcement, such as the Directorate of Criminal Investigation and the Anti-Cybercrime Task Force, to gather evidence and build cases against cybercriminals.

For those who have fallen victim to cybercrime, the option of reporting the incident is made available by sending an email to cybercrime@polri.go.id. In order to facilitate the prompt tracing of the perpetrator, it is recommended that the account number and telephone number be included in the report. This approach can be effectively employed in the context of fraud and online sales, which have become increasingly prevalent. The National Police provides a dedicated email address for the submission of reports pertaining to cybercrime. The importance of legal protection for victims of cybercrime extends beyond the realisation of a state of law. It is also a crucial preventive measure for law enforcement officers, enabling them to reduce or prevent the occurrence of victims of cybercrime. Furthermore, it is not merely a repository for reports; rather, it is expected that there will be tangible action from law enforcement officers, ensuring that the community of technology users feels secure in carrying out their activities in cyberspace. The most effective method of preventing the proliferation of cybercrime is to encourage the government to enact regulations and legislation that can apprehend perpetrators. This should particularly focus on the stages of assistance, recovery and the provision of victims' rights. Furthermore, law enforcement must take robust action to deter cybercrime perpetrators by establishing a clear legal basis.

One of the main challenges faced by law enforcement is the rapid pace of technological change. Cybercriminals constantly evolve their tactics, using increasingly sophisticated techniques to bypass traditional methods of detection. As a result, Indonesian law enforcement has been under pressure to keep up with technological developments and adapt their investigative methods accordingly. This has led to an emphasis on digital forensics, the use of specialized software

and tools to trace digital evidence, and cyber surveillance techniques to monitor online criminal activity.

In recent years, Indonesia has made efforts to enhance the capabilities of its law enforcement agencies by providing cybercrime training to police officers and establishing collaborative networks with international law enforcement organizations such as Interpol. These efforts have improved Indonesia's ability to respond to cybercrime incidents, although there is still a significant need for additional resources and expertise.

Additionally, law enforcement faces legal and procedural challenges in the collection and handling of digital evidence. While traditional evidence, such as physical documents or witness testimony, can be easily preserved, digital evidence is more volatile and can be altered or destroyed more easily. Therefore, police must exercise caution and follow strict protocols to ensure the integrity of digital evidence.

Another important aspect of law enforcement's role is public awareness. Given that many individuals and businesses are still vulnerable to cybercrimes such as phishing, identity theft, and online fraud, law enforcement must also engage in cybersecurity education. By increasing awareness of common cyber threats and providing guidance on how to prevent them, law enforcement agencies can help reduce the overall impact of cybercrime in Indonesia. While Indonesia has taken significant steps to improve its law enforcement response to cybercrime, ongoing challenges remain. Continuous investment in specialized training, technology, and international cooperation will be essential to combat the growing threat of cybercrime.

Furthermore, there is a growing recognition of the need for victim advocacy in cybercrime cases. Victims of digital crimes often feel isolated and unsure of how to navigate the complex legal and technological landscape. Support services, including victim advocacy organizations, can help victims understand their rights, assist in filing complaints, and guide them through the legal process.

While Indonesia has made significant strides in protecting victims of cybercrime, challenges remain. There is still a need for greater public awareness about victim rights and legal processes. Additionally, victims may face difficulties accessing timely and effective legal and psychological support, especially in rural or less developed areas.

In conclusion, while Indonesia has established a legal framework for victim protection, more efforts are needed to ensure that victims of cybercrime are adequately supported. This includes improving access to legal remedies, providing psychological support, and enhancing awareness of victims' rights.

CONCLUSION

The Indonesian state is characterised by a legal system that regulates the behaviour of its citizens. The prevalence of cybercrime in the contemporary technological era is a matter of grave concern. The Indonesian legal system has established legal frameworks that address various forms of cybercrime. The regulations governing cybercrime can be found in several pieces of legislation, including the Criminal Code, Law Number 11 of 2008 concerning ITE, Law Number 44 of 2008 concerning Pornography and Law Number 36 of 1999 concerning Telecommunications. The phenomenon of cybercrime is becoming increasingly prevalent, resulting in a growing number of victims. Those who have fallen victim to cybercrime must be afforded legal protection. The protection of victims is regulated by Law Number 13 of 2006 concerning the Protection of Witnesses and Victims (UU PSK), Article 5. The importance of legal protection for victims of cybercrime, in addition to being within the framework of realizing a state of law, is twofold. Firstly, it is important to do so as a preventive measure carried out by law enforcement officers in reducing or preventing the occurrence of victims of cybercrime. Secondly, it is important to ensure that the legal protection provided is not merely a receptacle for reports, but rather that there will be real action from law enforcement officers. This is necessary in order to ensure that the community of technology users really feels safe in carrying out their activities in cyberspace.

It is recommended that law enforcement officers adopt a more assertive approach to combating the growing and diverse phenomenon of cybercrime. The existing regulatory framework requires updating, given the proliferation of cybercrime models. The expansion of cybercrime types should also enhance victim protection, with due consideration of current regulations

REFERENCES

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.

Anggusti, M. (2022). Cybercrime change consumers' purchase intention in Indonesia: a moderating role of corporate social responsibility and business law, *International Journal of Cyber Criminology* 16(1), 20-39.

Anwary, I. (2022). The Role of Public Administration in combating cybercrime: An Analysis of the Legal Framework in Indonesia, *International Journal of Cyber Criminology*, 16(2), 216-227.

Arief, B.N. (2003). *Kapita Selekta Hukum Pidana*, Bandung: Citra Aditya Bakti.

Astariyani, N.L.G., Hermanto, B., da Cruz, R. & Wisnaeni, F. (2023). Preventive and evaluative mechanism analysis on regulatory and legislation reform in Indonesia, *Law Reform* 19(2), 248-269.

Azmi, R.H.N. (2020). Indonesian Cyber Law Formulation in The Development Of National Laws In 4.0 Era, *Lex Scientia Law Review* 4(1), 46-58.

Bunga, D. (2019). Legal response to cybercrime in global and national dimensions, *Padjadjaran Journal of Law*, 6(1), 69-89.

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

Djanggih, H. (2018). The phenomenon of cyber crimes which impact children as victims in Indonesia, *Yuridika* 33(2), 212-231.

Drew, J.M. & Farrell, L. (2018). Online victimization risk and self-protective strategies: Developing police-led cyber fraud prevention programs, *Police Practice and Research* 19(6), 537-549.

Fuady, M.E. (2015). Cybercrime : Fenomena Kejahatan melalui Internet di Indonesia, *Jurnal Mediator* 6(2), 255-264.

Gojali, D.S. (2023). Identifying the Prevalence of Cybercrime in Indonesian Corporations: A Corporate Legislation Perspective, *International Journal of Cyber Criminology* 17(1), 1-11.

Halder, D. & Jaishankar, K. (2015). "Irrational coping theory and positive criminology: A framework to protect victims of cyber crime." In: *Positive criminology*, pp. 276-291. UK: Routledge.

Hermanto, B. (2021). Discover future prospect of Indonesia criminal law reform: Questioning adat criminal law existence, Material and Formal Legislation, and Constitutional Court Decision Frameworks, *Paper* was presented at International Seminar Udayana University and University of Melbourne, 17 June 2021.

Hermanto, B. & Aryani,, N.M. (2021). Omnibus legislation as a tool of legislative reform by developing countries: Indonesia, Turkey and Serbia practice, *The Theory and Practice of Legislation* 9(3), 425-450.

Hermanto, B. (2023). Deliberate legislative reforms to improve the legislation quality in developing countries: case of Indonesia, *The Theory and Practice of Legislation* 11(1), 1-31.

Hong, Y. & Neilson, W. (2020). Cybercrime and punishment, *The Journal of Legal Studies* 49, no. 2 (2020): 431-466.

Imran, M.F. (2023). Preventing and Combating Cybercrime in Indonesia, *International Journal of Cyber Criminology* 17(1), 223-235.

Jhon, R.M. (2018). Existence of Criminal Law on Dealing Cyber Crime in Indonesia, *Indonesian Journal of Criminal Law Studies*) 3(1), 25-34.

Laksana, A.W. (2019). Pemidanaan Cybercrime Dalam Perspektif Hukum Pidana Positif, *Jurnal Hukum Unissula*, 35(1), 8-17.

Lamintang, P.A.F. (1997). *Dasar-Dasar Hukum Pidana Indonesia*, Bandung: Citra Aditya Bakti.

Manthovani, R. (2023). Indonesian Cybercrime Assessment and Prosecution: Implications for Criminal Law, *International Journal of Criminal Justice Sciences* 18(1), 439-452.

Nadriana, L. & Sukmana, P. (2022). Exploring the Applicability of Common Law Principles in Combating Cybercrime in Indonesia: An Analysis of Current Legal Framework and Challenges, *International Journal of Cyber Criminology*, 16(2), 192-204.

Pane, M.D. & Situmeang, S.M.T. (2011). Penegakan Hukum Cyber Crime dalam Upaya Penanggulangan Tindak Pidana Teknologi Informasi, *Jurnal Loyalitas Sosial* 3(2), 93-105.

Purwani, S.P.M.E. & Dewi, P.M.L. (2022). Judicial Pardon in Update of the Criminal System Against Middle Crimes, *Yustisia* 10(3), 415-430.

Rahmanto, T.Y. (2019). Penegakan Hukum Terhadap Tindak Pidana Penipuan Berbasis Transaksi Elektronik, *Jurnal Penelitian Hukum DE JURE*, 19(1), 31-52.

den Bergh, R-v., Carin MM, & Junger, M. (2018). Victims of cybercrime in Europe: a review of victim surveys, *Crime science* 7(1), 1-15.

Robalo, T.L.A.S. & Rahim, R.B.B.A. (2023). Cyber victimisation, restorative justice and victim-offender panels, *Asian journal of criminology*, 18(1), 61-74.

Setiawan, D. (2005). *Sistem Keamanan Komputer*, Jakarta: PT Elex Media Komputindo.

Siregar, G. & Sinaga, S. (2021). The law globalization in cybercrime prevention, *International Journal of Law Reconstruction*, 5(2), 211-227.

Suartha, I.D.M., Martha, I.D.A.G.M. & Hermanto, B. (2022). Between Mental Illness, Criminal Policy Reform, and Human Rights: Discourse on Reformulation of The Article 44 Indonesia Criminal Code, *International Journal of Criminal Justice Sciences*, 17(1), 1-21.

Sudiarawan, K.A., Tanaya, P.E. & Hermanto, B. (2020). Discover the legal concept in the sociological study, *Substantive Justice International Journal of Law*, 3(1), 94-108.

Sugama, I.D.G.D. & Hariyanto, D.R.S. (2021). Politik Hukum Pemberantasan Prostitusi Online Terkait Kriminalisasi Pekerja Seks Komersial dan Pengguna, *Kertha Wicaksana*, 15(2), 158-168.

Sumarwani, S. (2014). Tinjauan Yuridis Pemidanaan Cybercrime Dalam Perspektif Hukum Pidana Positif, *Jurnal Pembaharuan Hukum* 1(3), 287-296.

Subawa, M. & Hermanto, B. (2023). Despite Complicated Portraits and Policy Orientation: Struggle to Articulate Right to Education Based on the Indonesia Constitutional Court Decisions, *Revista de Direito Internacional* 20(2), 611-629.

Swardhana, G.M. (2021). Discover Crimes against Humanity as Gross Violations of Human Rights: International and Indonesia Perspectives, *Substantive Justice International Journal of Law*, 4(2), 115-133.

Swardhana, G.M., Anggarita, N.K. & Kurniawan, I. (2022). Criminal Policy against Children Who Committed Cyber Bullying: Indonesia Laws Perspective, *J. Legal Ethical & Regul. Isses*, 25(1): 1-9.

Wahid, A. & Labib, M. (2005). *Kejahatan Mayantara (Cybercrime)*, Bandung: Refika Aditama.

Wijaya, M.R. & Arifin, R. (2020). Cyber Crime in International Legal Instrument: How Indonesia and International Deal with This Crime?, *Indonesian Journal of Criminal Law Studies*, 5(1), 63-74.

Yudha, K.P.S.W.B., Parsa, I.W., Swardhana, G.M. & Suartha, D.M. (2023). International Standards in Inter-Country Cooperation Regarding the Crime of Money Laundering, *Telematique* 22(1), 197-205.

Yusa, G. (2017). The Authority of Government in Clearing Hatefull and Hostilities, *International Journal of Electrical and Computer Engineering*, 7(6), 3735-3744.

Yusa, I.G. et.al.. (2021). Law Reform as the Part of National Resilience: Discovering Hindu and Pancasila Values in Indonesia's Legal Development Plan, *Proceedings of International Conference For Democracy and National Resilience (ICDNR 2021)*, 1-10. Atlantis Press.

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET