International Journal of Social Science And Human Research

ISSN (print): 2644-0679, ISSN (online): 2644-0695

Volume 06 Issue 12 December 2023

DOI: 10.47191/ijsshr/v6-i12-39, Impact factor- 6.686

Page No: 7514-7517

Analysis of International Law Regarding Technological Advancements and Cybersecurity in Indonesia

Widia Utami[1], Dr. Joko Setiyono, S.H., M.Hum[2]

[1,2] Master of Laws, Faculty of Law, Diponegoro University, Indonesia

ABSTRACT: The progress of technology and its applications always has various implications, both for the order of social life, the development of the business world, and the advancement of moral, ethical, and legal values. The following will provide an overview of some technologies considered capable of transforming life globally in all its dimensions. Through multimedia technology, telecommunications have become highly advanced, encompassing basic telecommunications and including other value-added technologies. The widespread penetration of the internet, if not used wisely, can give rise to cybercrimes, a term used to refer to crimes committed in the virtual world or cyberspace. Cybercrime is considered a more advanced development of computer crime. Crimes in the field of information technology are relatively new compared to conventional forms of crime. Information technology crimes emerged concurrently with the advent of the information technology revolution. Additionally, it is characterized by social interactions that minimize physical presence, marking another feature of the information technology revolution. Law enforcement's efforts to counter cybercrime are heavily affected by existing legislation; several laws related to information technology, especially crimes associated with the internet, are regulated under national regulations.

KEYWORDS: Policy, Cyber Law, Cyber Handling in Indonesia, International Cyber Law

INTRODUCTION

The current era's advancements have significantly changed the fabric of human life. Human civilization has gradually shifted towards modernization, impacting every aspect of human life. One of the hallmarks of contemporary development is the progress in technology and information, which humans have applied to simplify their tasks. The internet is a product of this technological and informational advancement. Many conveniences are experienced as a result of this progress, and one of the applications can be seen in the field of national defense as a supportive component in its implementation. The speed of accessing information, connectivity between subsystems, and the modernization of infrastructure are benefits that can be developed in the defense field based on technology and information. The war paradigm has shifted; war is no longer just about armed conflict but also involves modern warfare such as trade wars, information warfare, cyberwar, proxy wars, and other asymmetric warfare. In the realm of defense, the utilization of information technology can enhance the capabilities of a nation's components, both in terms of facilities and human resources, in the effort to achieve national goals and counter any threats, challenges, obstacles, and disruptions from both internal and external sources (Sanjaya, 2022).

The phenomenon of information technology crimes is a relatively new form of criminal activity when compared to other conventional forms of crime. Information technology crimes emerged concurrently with the birth of the information technology revolution. Additionally, it is characterized by social interactions that minimize physical presence, marking another feature of the information technology revolution. The extensive internet penetration, if not used wisely, can give rise to cybercrimes, a term used to refer to crimes committed in the virtual world or cyberspace. Cybercrime is considered a more advanced development of computer crime. The cyberspace (virtual world) is currently vulnerable to criminal behavior. For example, practices of virus implantation that harm computers worldwide have been observed, leading to significant financial losses for banks and financial institutions. Advanced nations like the United States, the United Kingdom, and several others have reported breaches in national security data, which has been accessed and downloaded by unauthorized individuals. Other criminal activities also take place through the internet, such as child pornography, attacks on someone's privacy, illegal trade, or the presence of sites that disturb society. Another example is for those who enjoy gambling, as they can engage in it from home or the office (Nitibagaskara, 2011).

The numerous threats to cybersecurity in the digital world indicate that the utilization of digital technology in financial service institutions positions systems, data, networks, and programs (software) as significant assets that must be protected. Vulnerabilities of systems, data, networks, and programs to hacking are fundamental issues that should not be overlooked to ensure freedom from cybersecurity threats and to avoid harm to the public as users of these services. Financial institutions can take measures

to anticipate cybersecurity threats by strengthening risk management in the utilization of digital services. This is done to enable financial institutions to seize opportunities and significant benefits in the digital realm while minimizing potential risks associated with crimes in the digital world. This approach aims to minimize losses and maintain the security of funds and the convenience of financial services for users (Kurniawan, 2022).

PROBLEM FORMULATION

1. What do technological advancement and cybersecurity mean?
2. How is the current overview of technological advancement and cybersecurity in Indonesia?

RESEARCH METHODOLOGY

Research is a systematic process, a framework of steps conducted, planned, and systematically executed to obtain solutions to specific problems or respond to particular statements. Research is fundamentally an effort to search, not just an observation carried out casually on an easily accessible object. This is because research aims to systematically, methodologically, and consistently uncover the truth. Analysis and construction were carried out through this research process in relation to the collected and processed data. To achieve the best results, the research method used was normative juridical, consisting of the primary legal basis deeply examined in this research, which was the Regulations of Resolution 57/239, 2002, on the "Creation of a Global Culture of Cybersecurity" in the UN Agreement.

DISCUSSION

1. Technological Advancements in Indonesia

Information Technology is a technology used to process data, including processing, obtaining, organizing, storing, and manipulating data in various ways to generate high-quality information. This information is relevant, accurate, timely, used for personal, business, and government purposes, and is strategically important for decision-making. This technology employs a set of computers to process data, network systems to connect one computer to another as needed, and telecommunication technology to distribute and access data globally. The role provided by this information technology application is to acquire information for personal aspects such as health, hobbies, recreation, and spirituality. Then, for professions such as science, technology, trade, business news, and professional associations, there is a means of collaboration between individuals or groups without knowing the limits of distance and time, countries, race, economic class, ideology, or other factors that may hinder the exchange of ideas. The development of Information Technology drives a new way of life, from the beginning to the end, known as e-life, meaning that this life is already affected by various electronic needs. Moreover, now, it is vibrant with various terms that start with the prefix 'e,' such as e-commerce, e-government, e-education, e-library, e-journal, e-medicine, e-laboratory, e-biodiversity, and others, all based on electronics (Wardiana, 2002).

In addressing cybercrime, the existence of Cyber Law is essential. Cyber Law is a legal aspect whose term originates from Cyberspace Law, encompassing every aspect related to individuals or legal entities using and utilizing internet/electronic technology that starts when they go "online" and enter the cyber or virtual world. In countries that have advanced in the use of the internet/electronics as a tool to facilitate every aspect of their lives, the development of cyber law has already progressed significantly.

Cyber Law is highly essential concerning efforts to prevent and address criminal activities. It serves as the legal foundation in law enforcement processes against crimes committed through electronic and computer means, including money laundering and terrorism. The enforcement of Cyber Law in Indonesia is crucial due to the evolution of the times. Proponents of Cyber Law argue that Indonesia should adopt it as traditional laws are incapable of anticipating the rapid developments in the virtual world. A case in point is the cybercrime experienced by Lukman Hakim Saifuddin, the Deputy Chair of the People's Consultative Assembly (MPR) from 2009 to 2014, where his email was hacked by someone aiming to benefit financially by sending letters to contacts in his email. Lukman Hakim Saifuddin has rights as regulated in Article 26 paragraph
(2) of Law Number 11 of 2008 concerning Electronic Information and Transactions, amended by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions ("ITE Law"). It states that "any person whose rights are violated as referred to in paragraph (1) may file a lawsuit for losses incurred based on this Law." With the rights mentioned above, Lukman Hakim Saifuddin has the right to file a lawsuit based on Article 28 paragraph (1) of the ITE Law, which stipulates, "any person who intentionally and without the right disseminates false and misleading information resulting in consumer losses in Electronic Transactions," which is a prohibited act. In line with this, the perpetrator may be subject to criminal penalties under Article 45A of the ITE Law, which states, "Any person who intentionally and without the right disseminates false and misleading information resulting in consumer losses in Electronic Transactions" as referred to in Article 28 paragraph (1) shall be punished by imprisonment for a maximum of 6 (six) years and/or a fine of up to IDR 1,000,000,000.00 (one billion rupiahs)."

2. Impact of Technological Advancements and Cybersecurity and Legal Certainty

Based on various incidents in recent years, Indonesia has been identified as a country with weak cybersecurity. This is evident from the prevalence of various events, such as hacking customer debit card data from a bank, where hackers attempted to infiltrate the bank's customer card security system in mid-May 2014. This incident highlights the inadequacy of cybersecurity in Indonesia. One surprising fact comes from the internet monitoring company Akamai, revealing that internet crimes in Indonesia have doubled. This figure places Indonesia in the top position as a potential target for hackers, surpassing China. Out of 175 investigated countries, Indonesia contributes as much as 38 percent of the total targets for hacking traffic on the internet. This number has increased in tandem with the rising internet speed in Indonesia (Ardiyanti, 2016).

According to David Belson from Akamai Research, internet speed is not directly related to the significant potential of internet crimes threatening Indonesia. Hacking activities are more attributed to the weaknesses in the internet and computer security systems in Indonesia. The losses caused by cybercrime in the cyber world in Indonesia, as indicated by CIA data, have reached 1.20% of the global cybercrime loss rate, as shown in the table below. The estimated losses due to cybercrime, compared to the estimated losses in Indonesia of USD 895 billion, have reached 1.20% of the total estimated global losses due to cybercrime, reaching USD 71,620 billion.

In the policy realm, addressing cybercrime differs from handling other forms of crime. Governments can generally easily control and enforce laws within the sovereignty of their territories. However, this is not the case for online activities, whose physical locations can change at any time and sometimes can only be imagined. The issue arises when determining legal choices and jurisdictions, leading to various considerations for approaching the problem. One emerging thought is positioning the internet as the fourth international space, similar to Antarctica, outer space, and the oceans (Golos, 2007).

The cyber-security policy in Indonesia, specifically, has been initiated since 2007 with the issuance of the Minister of Communication and Informatics Regulation No. 26/PER/M.Kominfo/5/2007 concerning the Security of Utilizing Telecommunication Network Based on Internet Protocol. Subsequently, the regulation was revised through the Minister of Communication and Informatics Regulation No. 16/PER/M.KOMINFO/10/2010, updated again with the Minister of Communication and Informatics Regulation No. 29/PER/M.KOMINFO/12/2010. One of the regulations stipulates the establishment of ID-SIRTII (Indonesia Security Incident Response Team on Internet Infrastructure), which stands for Indonesia Security Incident Response Team on Internet Infrastructure. It is a team the Minister of Communication and Informatics (*Kominfo*) assigned to supervise the security of internet protocol- based telecommunication networks. According to Hasyim Gautama, the legal framework for cyber-security in Indonesia is currently established, in part, based on the Electronic Information and Transactions Law No. 11 of 2008, Government Regulation on the Organization of Electronic Systems and Transactions No. 82 of 2012, as well as ministerial circulars and regulations. In efforts to ensure legal certainty in the development of cybersecurity, various programs have been implemented. These include initiating legislation related to cybersecurity, such as the Information and Electronic Transactions Law No. 11 of 2008, Government Regulation on the Organization of Electronic Systems and Transactions No. 82 of 2012, and developing a national cybersecurity framework (Nasrullah, 2023).

However, the legality of handling crimes in the cyber world is still weak. Despite existing regulations prohibiting attacks or destruction of electronic systems in the Information and Electronic Transactions Law No. 11 of 2008, no specific legislation regulates cybercrime and its handling. On the other hand, cybercrime is on the rise, and its patterns are evolving rapidly, making it challenging for law enforcement authorities to address (Kurniawan, 2022).

The suboptimal enforcement of laws against cybercrimes is due to the inadequate tools and facilities for law enforcement. Enforcing the law against cybercrimes is crucial because the nature of these crimes involves using both tangible and intangible tools. Determining the time and place of cybercrimes depends on when the tools are effectively operational. Therefore, telematics analysis is highly necessary to uncover these crimes. To investigate, detect, and mitigate these crimes, Onno W. Purbo explains that the approach depends significantly on the applications and network topologies used. Some of the applications can be found in gnacktrack and backtrack. This illustrates that adequate tools and facilities are crucial in the law enforcement process. Without specific tools or facilities, law enforcement cannot proceed smoothly. These tools or facilities include educated and skilled human resources, well-organized organizations, adequate equipment, sufficient finances, etc. If these elements are not fulfilled, it is impossible for law enforcement to achieve its goals.

To enhance efforts in combating the increasing cyber crimes, the Indonesian National Police (*Polri*), specifically the Criminal Investigation Department, Indonesian National Police Headquarters (*Bareskrim Mabes Polri*), has endeavored to conduct awareness campaigns regarding cybercrimes and their handling procedures for units in different regions (Regional Police or *Polda*). This awareness campaign involves training sessions (vocational education) and improving the investigative skills of Polri members by sending them to various courses related to cybercrime. The deployment of *Polri* personnel is not only limited to national scope but also includes sending them to attend courses in advanced countries to apply and implement the knowledge gained in Indonesia.

The legal awareness of the community is crucial in the technological era, and the low legal awareness among internet users hampers the optimal enforcement of laws against cybercrimes. The lack of legal awareness among internet users is evident in the

misuse of the internet for various criminal activities, including the trading of sexual services and other forms of criminal behavior. The legal awareness of victims to report the crimes they experience remains very limited. Until now, the legal awareness of the Indonesian community in responding to cybercrime activities is still perceived as insufficient. This is caused, among other things, by a lack of understanding and knowledge (lack of information) among the public regarding the various types of cybercrimes. This lack of information hinders efforts to combat cybercrime, particularly in terms of legal compliance and the monitoring process of the public towards any activities suspected to be related to cybercrime. Therefore, it is right to say that optimal law enforcement requires legal awareness and moral consciousness from the public.

CONCLUSION

Technological advancement refers to the development and innovation in the field of technology that influences various aspects of human life. Cybersecurity is an effort to ensure the achievement and maintenance of security features for organizations and user assets against relevant security risks in the cyber environment. The general security objectives consist of availability integrity, which includes authenticity and the possibility of reducing repudiation; and the final is confidentiality.

In relation to developing a national strategy for building cybersecurity in Indonesia in the future, it will be conducted by fulfilling four foundations that support the development of information technology, including the development of cybersecurity. These foundations are the development of software, such as systems and applications, and the development of hardware; the development of information technology facilities and infrastructure; content management; telecommunication and networking; the development of the internet; and online or internet-based commerce. Apart from fulfilling the four main foundations of cybersecurity development, another crucial step involves organizing the utilization of information technology systems by considering four key aspects: firstly, information systems; secondly, organizational competition; thirdly, information systems and organizational decision-making; and fourthly, the organizational use of information systems.

REFERENCES

1) Ardiyanti, H. (2016). Cyber-security dan tantangan pengembangannya di indonesia. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*.
2) Daniel H Purwadi, Belajar Sendiri Mengenal Internet Jaringan Informasi Dunia, PT Elex Media Komputindo, Jakarta 1995, Edmon, Makarim,. Komplikasi Hukum Telematika. Jakarta: RajaGrafindo. 2003.
3) Golos P. R, "Penegakan Hukum Cybercrime dalam sistem Hukum Indonesia dalam seminar Pembuktian dan Penanganan Cybercrime di Indonesia". 2007.
4) Huala Adolf, Hukum Penyelesaian Sengketa internasional, Sinar Grafika, Jakarta: 2014. Kurniawan, F. A., & Solihin, K. (2022). Penguatan Manajemen Risiko Lembaga Keuangan
5) Syariah Non-Bank dalam Menghadapi Ancaman Cyber Security. *JIOSE: Journal of Indonesian Sharia Economics*, *1*(1), 1-20
6) Mauna, Boer. 2013. Hukum Internasional : Pengertian, Peranan, dan Fungsi dalam Era Dinamika Global. Bandung : Penerbit Alumni.
7) Muhammad, Abdulkadir. 2004. Hukum dan Penelitian Hukum. Bandung: PT. Citra Aditya Bakti.
8) Nasrullah, Sepintas Tinjauan Yuridis Baik Aspek Hukum Materil Maupun Formil Terhadap Undang-undang Nomor 15/2003 Tentang Pemberantasan Tindak Pidana Terorisme. Makalah Pada Semiloka tentang "Keamanan Negara" yang diadakan oleh Indonesia Police Watch bersama Polda Metropolitan : Jakarta Raya.,2003
9) Nitibaskara, Tubagus Ronny Rahman. Ketika kejahatan berdaulat: sebuah pendekatan kriminologi, hukum dan sosiologi. 2011
10) Sanjaya, B. R., Efrianti, D., Ali, M., Prasetyo, T., Mukhtadi, M., Widasari, Y. K., & Khumairoh,
11) Z. (2022). PENGEMBANGAN CYBER SECURITY DALAM MENGHADAPI CYBER WARFARE DI INDONESIA. *Journal of Advanced Research in Defense and Security Studies*, *1*(1), 19-34.
12) Wardiana, W. (2002). Perkembangan teknologi informasi di Indonesia.