Realizing An Effective Legal System in Handling Mayantara Crime (Cybercrime) in The Society 5.0 Era

Nopit Ernasari[1], Azis Budianto[2], Rineke Sara[3]
nopiternasari694@gmail.com[1], azis_budianto@borobudur.ac.id[2], rineke_sara@borobudur.ac.id[3]

Universitas Borobudur[1, 2, 3]

Abstract. In the era of Society 5.0, information and communication technology has brought significant changes to global society. In the concept of human-centered and technology-based society 5.0, the main drivers of this industry are technology and modern society. The rapid development of technology and digitization has impacted all aspects of human life in the era of society 5.0. One of these is an aspect of security in the form of cybercrime threats. The use of this technology also opens loopholes for cybercrimes. Therefore, an effective legal system is needed in dealing with cybercrime. It is important to maintain the security and stability of digital society in dealing with cybercrime.

Keywords: Legal System, Mayantara Crime, Society 5.0

1. Introduction

Period Society 5.0 is one piece of the ongoing turns of events, this time is an improvement in the area of innovation, innovation made by people that is developing quickly. One of them is Society 5.0 which was started by the Japanese state. The idea of society 5.0 permits people to utilize current science-based like Man-made consciousness (artificial intelligence), Robots, and the Web of Things (IoT) which are human requirements to go for the gold live serenely. Society 5.0 seemed quite a while back, on January 21, 2019, and was made as a goal to industry 4.0 goal.

Society 5.0 becomes a character value that must be developed and becomes a tolerance that must be fostered along with the development of competencies that think innovatively, creatively, and critically. Society 5.0 has a goal to integrate cyberspace and physical space into a single unit that can make everything easier by being equipped with artificial intelligence. In this era, work and human activities were focused on human-centered, which was based on technology. It appears to be hard to do in an emerging nation like Indonesia, however that doesn't mean it isn't possible in light of the fact that right now Japan has shown off itself abilities as a country with the most trend setting innovation, this era is also capable of creating new jobs and causing other impacts, namely in the form of cybercrime. (cybercrime) which is an effective means of unlawful acts (onrecht matigedaad) due to the rapid development of technology.

Thus the law should also protect internet users who have good intentions and take firm action against perpetrators of internet crimes that cause a lot of harm to other people. As a result of the Covid-19 pandemic hitting the world, threat actors are getting like a windfall. Never imagined, there are new opportunities to carry out cyber threats, to individual users, governments, and companies. The pandemic has blurred the lines between work and personal

ICLSSEE 2023, May 06, Salatiga, Indonesia

DOI 10.4108/eai.6-5-2023.2333461

life. At the same time, enterprises and education must compete with hybrid work styles, while companies are also trying to accelerate their migration to the cloud. Governments around the world are also confounded by data and privacy issues.

Mayantara wrongdoing (cybercrime) is another type of danger that has never existed before in the public eye. Hacking, breaking, damaging, sniffing, checking, phishing, spamming, or tricks are a progression of hazardous web wrongdoings that can likewise enter government-possessed public foundation, causing many national losses and disturbing the wider community. Cybercrime is known as a modern conventional crime. Public law in the form of jurisdiction, ethics of online activities, consumer protection, regulatory bodies, data protection, and private law (HAKI, E-commerce, Insurance) are part of the basic strength of the state to fight these crimes.

The development of technology certainly brings various implications that must be anticipated and also watched out for. This effort has produced a legal product in the form of Law Number 19 of 2016 in conjunction with Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE). The basic thing about the ITE Law is an effort to accelerate the benefits and functions of law (regulations) within the framework of legal certainty. [1]

In the era of Society 5.0, cyber crimes are increasing and difficult to handle because criminals can hide behind complex computer networks and are difficult to trace. Therefore, an effective legal system is needed in dealing with Mayantara crime to reduce the level of crime in protecting the public from cybercrime.

Realizing an effective legal system for handling cybercrime in the era of society 5.0 needs to be supported by adequate legal instruments. This remembers regulations and guidelines by improvements for data and correspondence innovation. In addition, it is also necessary to form law enforcement agencies and a team of experts who are trained and capable of dealing with various types of cybercrimes.

Based on the background described above, the research problem can be formulated as follows: How effective is Law No. 19 of 2016 Jo Law No. 11 of 2008 in dealing with cybercrime in the era of society 5.0? and What are the obstacles in handling cybercrime in the era of society 5.0?

2. Methodology

The exploration utilized recorded as a hard copy is regulating juridical. The wellsprings of legitimate materials utilized in this exploration are essential lawful materials and optional legitimate materials. The primary materials used are legal science books. [2] The types of approaches used in this study are statutory approaches, case, and legal concept analysis approach. The data processing method used is the analytical method which is then outlined in descriptive-analytical writing.

3. Result and Discussion

Mayantara wrongdoing (Cybercrime) is a crime that uses the improvement of PC innovation, particularly the web. Cybercrime is an unlawful demonstration in light of the advancement of web innovation and the utilization of PC innovation. Cybercrime has turned

into another structure or aspect of wrongdoing today that has gotten the consideration of the more extensive worldwide local area, the dark side of technological progress in the era of society 5.0 which has such a broad negative impact on today's modern life. [3]

The period of society 5.0 is a continuation of the time of the modern transformation 4.0. In the era of 4.0, society has its characteristics, namely that people will want to know more about information or what can be called the term information society. Whereas in the era of society 5.0, an era where society is built in such a way by connecting the cyber world and the real world so that it becomes human-centric by considering many aspects of the humanities, if faced with a social problem it can solve it sustainably.

Industry 4.0 is otherwise called the term society 4.0, beforehand there was additionally society 1.0, society 2.0, and society 3.0 until the phase of society 5.0 as human civilization, every one of which has its personality. Society 2.0 is agribusiness where people have begun to know cultivating. Society 3.0 began to enter the modern time, to be specific when people began utilizing machines to help their regular routine exercises, then, at that point, Society 4.0 is right now being capable, in particular people who are know all about PCs to the web as well as its application in individuals' lives.[4]

The inherent character of society in the era of society 5.0 is that people rarely interact with each other because most people in the era of society 5.0 are people who live in a virtual world. Another well-known character in the era of society 5.0 is the existence of artificial intelligence or what is called Artificial Intelligence (AI) and also robotics.

The idea of society 5.0 and industry 5.0 arose in this development not as a basic sequential continuation or as an option in contrast to the business 4.0 worldview. Society 5.0 has the objective of setting people at the focal point of advancement, using the effect of innovation and the aftereffects of industry 4.0 with mechanical uprightness to work on personal satisfaction, social obligation, and manageability.

Society 5.0 and Industry 5.0 can mirror a crucial change in the public eye and the economy towards another worldview to offset monetary improvement with tackling social and ecological issues to defeat a test connected with human collaboration. The European Commission announced that industry 5.0 has differences from industry 4.0 which is considered to be driven by technology, while industry 5.0 has special value in the welfare of society. [5]

Indonesia as a constitutional state always prioritizes all state and social activities by the law. Thus, Indonesia is trying to reform criminal law, one of which is the enactment of Law no. 19 of 2016 Jo Law No. 11 of 2008 concerning Electronic Information Technology. Because activities in the field of computer-based technology are very important for society and can easily violate human rights.

Legal instruments provide the basis and guidelines for law enforcement officials who are enforced by perpetrators of cybercrimes. The enactment of Law no. 19 of 2016 Jo Law No.11 of 2008 is the latest chapter for the government of the Republic of Indonesia in fighting crime based on communication and information technology. The existence of these provisions opens the way for law enforcers to take action and prosecute the perpetrators of cybercrimes. The faster the technology is used, the more vulnerable it is to existing crimes committed by parties who are not responsible for fraud, theft, and defamation via the internet.

Forms of cybercrime that have a close relationship with the use of computer-based technology and telecommunications networks, namely:

1. Unauthorized Admittance to PC Frameworks and Administrations is the wrongdoing that is placed into a PC network framework wrongfully without consent or the information on the proprietor of the PC network framework. Hoodlums (programmers) do this by undermining or taking significant and classified data,

however some do it since they feel tested to attempt their abilities by infiltrating a framework that has an elevated degree of security. This sort of wrongdoing is progressively inescapable with the improvement of web innovation. One instance of programmers specifically:

   a. In 2016, Tiket.com and Citilink were attacked by hackers. A group of teenagers managed to hack the online ticket buying and selling site, tiket.com on the Citilink server. The loss suffered by Tiket.com was 4.1 billion, while Citilink was 2 billion.
   b. In 2020, there was a DDoS attack on the DPR RI website, the official dpr.go.id website had an error and could not be accessed. The site displays a white page with the message "An error occurred while processing your request" in tracing, the attack is categorized as DDoS.

2. Illegal Substance, which is a wrongdoing by entering information or data into the web about some falsehood.
3. Data Fabrication, specifically the wrongdoing of adulterating information on significant records put away as scriptless archives through the web.
4. Cyber Surveillance, which is a wrongdoing that uses the web organization to do spying exercises against different gatherings, by entering the PC network framework (PC network arrangement) of the objective party of this wrongdoing is displayed against business rivals with significant reports or information put away in a framework modernized.
5. Cyber Harm and Blackmail, in particular wrongdoings carried out by upsetting, harming, or obliterating information, PC projects, or PC network frameworks associated with the web. This wrongdoing is perpetrated by invading a rationale bomb, PC infection, or a specific program, with the goal that information, and PC programs can't be utilized as expected.
6. Offense Against Protected innovation, which is property focused on protected innovation freedoms possessed by somebody on the web. One model is emulating the presence of a website page of a webpage having a place with someone else wrongfully, communicating data on the web which ends up being another person's proprietary innovation.
7. Infringement of Protection, a wrongdoing coordinated at somebody's data that is exceptionally private and secret. The wrongdoing is typically coordinated against an individual's very own data that is put away in a mechanized way, which whenever known by others, can hurt the individual tangibly or unimportantly, for instance ATM Pin Number and Charge card Number.

To respond to Mayantara crime there must be harmonious cooperation between the government, law enforcement, and the community. As long as cybercrime cases occur in the community, it can be revealed if there are reports from the public, in this case, "victims". The law is needed by society to be the main opponent of crime or law to be a special weapon in dealing with crimes that are developing and developing in society. In this case it must function, if it fails to function itself in tackling or fighting crime, then the image will fall no longer as a sacred norm but a norm of impotence.

Endeavors to expand the world's obligation to network safety have been completed with the positioning of the Worldwide Online protection Record (GCI) by the Global Telecom Association (ITU) for 193 part nations. The rating is given in view of 5 points of support, namely:

1. Legal/legal,
2. Technical and procedures,
3. Organizational structure
4. Capacity building, and
5. International cooperation

Based on the GCI score in 2020, Indonesia is ranked 77th out of 193 countries.[6] What is worrying about the GCI report is the fact that the development of cyber security policies in Indonesia is at 0% when one considers how many cyber attacks Indonesia has suffered over the past 5 last years.

The government's challenges in the era of society 5.0 in strengthening cyber security include the insufficient availability of technology experts and security technical experts to design and implement cyber security strategies. The risks that occur due to the cross-border nature of cyber security, which makes a country with a weak cyber security crime strategy can disrupt the cyber security of other countries. The use of anonymization tools, for example, blockchain currencies or encryption, in crimes that use the internet further complicates policy making.

The emergence of new technologies and systems from time to time requires periodic updating of the monitoring system. New forms of cybercrime such as ransomware, identity theft, sexual advances (grooming), and sexual harassment through cyberspace. The need to deal with cyber-attacks and forms of conflict between other countries due to the absence of applicable international norms and regulations governing state behavior. Pressure to assist governments in enforcing cyber security and fighting cybercrime and terrorism, which can include creating policies and reporting content, shutting down networks, blocking services, and even compromising the security of their products to aid government surveillance. The need to build internal capacity to maintain information and network security. And in the form of incentives to maintain the confidentiality of data that can pose risks and cyber attacks in the name of data privacy and potential defamation.

3.1 Effectiveness of the Implementation of Law no. 19 of 2016 Jo Law No. 11 of 2008 concerning Electronic Information Technology

The effectiveness of the implementation of criminal aspects in the ITE Law can be seen through the substance and legal structure aspects which include law enforcement, law enforcement apparatus resources, and community participation in the context of law enforcement and must also be supported by facilities and infrastructure so that law enforcement is realized.

In reality, in the era of globalization, people feel the convenience and great benefits of the results of the convergence between telecommunications, information, and computers, which people call the information technology revolution. One of the results of this convergence is a cyber activity that has broad implications for all aspects of life and is not impossible in various activities regarding existing legal issues.

The advancement of data innovation doesn't give most extreme advantages to society. Advanced innovation permits simple abuse of data, so the issue of data framework security is vital. The data security approach should be done comprehensively, accordingly there are three ways to deal with keep up with security in the internet:

1. Technological approach
2. Socio-cultural approach
3. Legal approach.[7]

To deal with security disturbances, a technological approach is necessary, because without network security it is very easy to infiltrate, intercept or access illegally and without rights. as a form of protection for the entire community in the context of ensuring legal certainty, which previously was a concern for all parties, especially concerning the emergence of various electronic-based activities.

Efforts to guarantee legal certainty in the development of cyber-security have been carried out, among others, by implementing a series of programs that have started to run including initiating legislation related to cyber-security such as Law no. 19 of 2016 Jo Law No. 11 of 2008 concerning Electronic Information Technology and PERPRES No. 95 of 2018 concerning Electronic-Based Government Systems.

In Indonesia In Indonesia itself, there is already a law that regulates cybercrime, namely the ITE Law. In this law several issues stand out, namely:

1. Regarding the evidence related to legal actions carried out through
2. electronic system.
3. Relating to the interpretation of legal principles and norms when confronted
4. intangible material issues.

Cybercrime is not something simple, because its activities are no longer limited by the territoriality of a country. Losses can occur both to the perpetrator of the transaction and to other people who have never made a transaction, such as theft of credit card funds through shopping on the internet (carding). In cybercrime in proving. [8] is a vital component thinking about that electronic data has not been obliged in the Indonesian criminal procedural regulation framework.

The verification is an issue that assumes a part in the preliminary court assessment process, with this confirmation the destiny of the not entirely set in stone. Assuming that the consequences of the proof utilizing the proof determined by regulation are not adequate to demonstrate the culpability accused of the litigant, the respondent is let out of discipline, then again on the off chance that the litigant can be demonstrated with the proof alluded to in Article 184 of the Criminal Strategy Code, the litigant should be proclaimed blameworthy and he will be condemned. Hence, judges should be cautious, cautious, and mature in surveying and taking into account proof issues. [9]

In terms of regulations in Indonesian positive law, cybercrime is equated with criminal acts related to information technology. In this regard, Donn B. Parker expressed in his opinion, namely "Computer abuse is broadly defined to be any incident associated with computer technology in which a victim suffered or could suffer loss and a perpetrator by intention made or could have gained". Incorrect use of computers can be broadly defined as 'any incident that has relevance to technology where the perpetrator does it intentionally and has the potential to make a profit, while on the other hand, the victim will suffer a loss as a result of the perpetrator's actions. [10]

The ITE Law is a special characteristic or lex specialis of the Criminal Code. One of the efforts to expand jurisdiction that is effective in dealing with cybercrime cases is the promulgation of Law no. 19 of 2016 Jo Law No. 11 of 2008 concerning Electronic Information Technology occurred in Indonesia. In practice, crime using a computer has always been a type of crime that tends to be difficult to classify as a crime, said Maskun. 22 Forms of cybercrime related to the misuse of information technology by violating the law as well as causing harm to others, for example, incitement, fraud, defamation, pornography, and so on.[11]

In addition, acts of disrupting data communication traffic and stealing other people's data are also included in the category of cybercrime.[12] In the ITE Law itself, acts that are prohibited or that can be categorized as cybercrime are contained in Chapter VII in detail in

Articles 27 to 37 of the ITE Law. For example is the pornographic delict contained in "Article 27 Paragraph (1) of the ITE Law which reads "Every person intentionally and without rights distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents that have content that violates decency." “Previously, this provision was contained in the Pornography Law, but in the ITE Law, the jurisdiction over the act of distributing such moral material is clarified, that spreading it on the internet can also be punished. "Article 27 Paragraph (2) of the ITE Law reads "Every person intentionally and without rights distributes and/or transmits and/or makes Electronic Information and/or Electronic Documents that have gambling content accessible."

Criminal liability in the criminal offenses of the ITE Law is regulated in CHAPTER XI, namely "Articles 45-52 of the ITE Law". Criminal responsibility is a form of someone's responsibility because of the crime he committed. Criminal responsibility is a system formed by criminal law in response to a violation based on consensuality to jointly make a refusal.[13] Based on the above understanding, a new person can be held accountable depending on two things, as follows:

1. The objective element is that the act was committed against the law or there is an element against the law that must be fulfilled.
2. The subjective element is the existence of a mistake either intentional (dolus) or negligence (culpa) to hold accountable those who violate the law.

Criminal liability arises from the existence of someone who commits an offense. Regarding "criminal responsibility, Roeslan Saleh defines it as the fulfillment of the objective elements inherent in criminal acts" and the subjective element means that it can be imposed on the perpetrator according to his actions.[14] Indonesia adheres to a system of criminal responsibility based on the principle of legality by "Article 1 of the Criminal Code" and the principle of guilt.[15] Criminal liability is born as a result of an error, namely a crime committed, and regarding this crime, there are already regulations governing it.

3.2 Obstacles in Handling Mayantara Crime (Cybercrime) in the era of Society 5.0

Law enforcement against cybercrime requires tools because the characteristic of this crime is that it is carried out with both tangible and intangible tools. Deciding when and where a cybercrime happens is resolved when the device works successfully, subsequently telematics examination is required in reveal this wrongdoing.

To research, identify and handle this wrongdoing, Onno W. Purbo made sense of that the technique relies upon the application and organization geography utilized. A portion of the applications are in gnacktrack and backtrack. This outlines that satisfactory method and offices are significant in the policing. Without specific means or offices, policing occur without a hitch. These offices or offices incorporate among others, instructed and talented HR, great association, and sufficient gear.

Counteraction and control of cybercrime requires a reformatory and non-corrective methodology that is essential and requires incorporation. Discussing society is a need or commitment connected to conversations about the law. Regulation and society are cut out of the same cloth. So without examining society in advance, really discussing an unfilled regulation.[16]

The lack of legal awareness in the community has implications for their understanding and disobedience to the law. For several reasons formulated by Dikdik M. Arief Mansur and Elisatris Gultom, up to this point the lawful consciousness of the Indonesian public is as yet missing, in particular: the legitimate attention to the Indonesian public in answering cybercrime exercises is as yet felt to need. This is expected, in addition to other things, to the absence of

understanding and information (absence of data) of general society in regards to this kind of cybercrime wrongdoing. This lack of information causes cybercrime countermeasures to encounter obstacles, in this case, constraints related to law enforcement and the community's control over any activity that is suspected to be related to cybercrime. Thus, it is appropriate to say that optimal law enforcement requires legal awareness and moral awareness from society.

The UN Congress Resolution VIII/1990 has called on member states to deal with Cybercrime by penal means, but, it is not easy. This is caused by several things, namely:

a. The evil deeds committed are in the electronic environment. Therefore dealing with Cybercrime requires special expertise, investigative procedures, and legal force/base which may not be available to law enforcement officials in the country concerned.
b. Cybercrime transcends national boundaries, while investigations and law enforcement efforts have so far been limited within the territory of their own country.
c. The open structure of international computer networks allows users to choose a legal environment (country) that has not criminalized cybercrime.[17] The occurrence of data havens (countries where data is sheltered/stopped, namely countries that do not prioritize preventing misuse of computer networks) can hinder other countries' efforts to eradicate this crime.

4. Conclusion and Suggestion

4.1 Conclusion

Based on these descriptions, the authors conclude that cybercrime is a crime that has a very big chance to occur in the development of the digital era. To overcome this, a strong legal basis is needed regarding cybercrime regulation, namely the ITE Law as a special regulation or *"lex specialis* of similar crimes which has been accommodated by the Criminal Code as a *lex generali."*

Impediments and hindrances tracked down in endeavors to examine cybercrime connected with the ITE regulation, among others, connect with issues of lawful instruments, the capacity of specialists, proof, and PC criminological offices. Endeavors that can be made to conquer the snags found in doing cybercrime examinations incorporate working on lawful instruments, teaching agents, building legal processing offices, expanding analytical endeavors and public and global participation, as well as completing preventive countermeasures.

4.2 Suggestion

In this case, so that the government can increase commitment to national strategies or priorities, it needs to be done, for example by forming a cyber task force from the center to the regions. Thus, there is a special task force that handles cybercrime cases such as cases of corruption, terrorism, drugs, and so on. Bearing in mind that cybercrime jurisdiction is global and is often carried out transnationally, handling this crime can utilize the internet (via e-mail or messenger) and digital signatures as a means of inspection to save time, costs, and distance and it is necessary to increase moral commitment in law enforcement against transnational crimes utilizing outreach and training.

References

[1] Sudikno Mertokusumo dan A Pitlo, Bab-bab Tentang Penemuan Hukum, Bandung: Citra Aditya Bakti, 1993.

[2] B. J. Nasution, Metode Penelitian Hukum, Bandung : Mandar Maju.

[3] B. N. Arief, Tindak Pidana Mayantara, Perkembangan Kajian Cybercrime di Indonesia, Jakarta: Rafa Grafindo Persada.

[4] Y Puspita, Y Fitriani, S Astuti, & S Novianti, "Selamat Tinggal Revolusi Industri 4.0, Selamat Datang Revolusi Industri 5.0. 122–130," in *Prosiding Seminar Nasional Pendidikan,*, 2020.

[5] J. Morowka-Jancelewicz, "The Role of Universities in Social Innovation Within Quadruple/Quintuple HelixModel: Practical Implications from Polish Experience," *Journal of Knowledge Economy, Springer US,* 2021.

[6] Global Cybersecurity Index 2020. International Telecommunication Unit Indonesia's data accessible and downloadable on https://ncsi.ega.ee/country/id/., 2020.

[7] A. Romli, "Cyberlaw dan HAKI Dalam Sistem Hukum di Indonesia," Jakarta , Refika Aditama, 2004, p. 3.

[8] A. Hamzah, Pengantar Hukum Acara Pidana Indonesia, Jakarta: Sinar Grafika, 1983.

[9] M. A. Yustia, Pembuktian Dalam Hukum Pidana Indonesia Terhadap Cyber Crime, Jakarta: Pranata Hukum, 2010.

[10] A. Hamzah, Hukum Pidana Yang Berkaitan Dengan Komputer, Jakarta: Sinar Grafika, 1993.

[11] H Sutarman, I Gede Widiana, dan Ihsan Amin, Cyber Crime: Modus Operandi dan Penanggulangannya, Yogyakarta: Laksbang Pressindo, 2007.

[12] A. Raharjo, Cybercrime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi, Bandung: Citra Aditya Bakti, 2002.

[13] C. Huda, Dari Tiada Pidana Tanpa Kesalahan Menuju Kepada Tiada Pertanggungjawaban Pidana Tanpa Kesalahan, Jakarta: Kencana, 2006.

[14] Hanafi Amrani dan Mahrus Ali, Sistem Pertanggungjawaban Pidana Perkembangan dan Penerapan, Jakarta: PT Rajawali Press, 2015.

[15] President of the Republic of Indonesia, "Law No. 1 of 1956 Concerning Criminal Law Regulations", 1956.

[16] S. Rahardjo, Hukum dan Perilaku: Hidup Baik adalah Dasar Hukum yang Baik, Jakarta: Kompas, 2009.

[17] B. N. Arief, Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan, Jakarta: Kencana, 2007.

[18] Law No.19 of 2016 in conjunction with Law No.11 of 2008 concerning Electronic Information Technology.

[19] The Criminal Procedure Code.