Research Horizon

Vol. 2, no. 6, (2022), 597-606
Website: https://journal.lifescifi.com/index.php/RH/index

Legal Complexity in Dealing with Cyber Crime in Indonesia

Dijan Widijowati[1, *]

[1] *Universitas Bhayangkara Jakarta Raya*

[*] Corresponding author:
dijanwidijowati.ubharajaya@gmail.com

Received : 2 Aug, 2022
Revised : 28 Nov, 2022
Accepted : 20 Dec, 2022

Abstract

The development of criminal activities alongside technological advancements demands the evolution of law enforcement instruments to remain relevant and effective. The rampant prevalence of cybercrime in contemporary society has introduced legal complexities in its mitigation. Cybercrimes have evolved and become increasingly intricate. To address these challenges, new legal regulations with a technological approach are necessary. Indonesia has implemented such an instrument, namely the Electronic Information and Transactions Law (UU ITE). However, despite its implementation to combat cybercrime, several complexities persist. This research adopts a normative approach with a descriptive model. It aims to analyze the complexities associated with the implementation of the UU ITE in addressing cybercrime in Indonesia. In the face of rapid technological advancements, cybercrimes have become more intricate and require appropriate legal approaches. The research endeavors to contribute to the understanding and development of the implementation of the UU ITE in combating cybercrime in Indonesia. The findings of this research are expected to serve as a foundation for enhancing the effectiveness and efficiency of cybercrime management, thereby safeguarding society's digital activities. In conclusion, the growing threat of cybercrime necessitates continuous adaptation and improvement of law enforcement instruments. The research seeks to shed light on the complexities of implementing the UU ITE in Indonesia and provide valuable insights for the enhancement of its efficacy. By doing so, it aspires to contribute to the protection of individuals and communities in the digital realm.

Keywords

Cybercrime, Cyber law, legal complexity

1. Introduction

According to Nugroho, & Chandrawulan (2022) assertion, Indonesia is a country that upholds the rule of law. The actions of every human being, as legal subjects, are governed by law. Law serves as a tool for societal change for the better, straightening out previously broken situations and improving them. Although people, as legal subjects, tend to make mistakes, the presence of the law guides them towards betterment. (Febriansyah, Indiantoro, and Ikhwan, 2023)

With the advancement of information technology, human crimes are not only committed in the real world, but also in the virtual world, commonly known as Cybercrime (Bunga, 2019). The emergence of the Internet as a new communication medium is associated with conflicting claims about the emergence of new patterns of social interaction (Noerhadi, 2022). The idea of virtual communities as a precursor to social interaction on the Internet has progressed (Djanggih 2018, Pratama, Sakti, Setyadi, Ibrahim, and Hidayat, 2022.)The use of the internet is so high that it eventually leads to new and significant social problems. For example, excessive personal communication through electronic devices, which can reduce the form of interaction between personal communication relationships and is very common. It uses social media status to seek personal information about individuals who are publicly exposed, ultimately making public spaces look like private spaces (Kristiyono, 2015).

Therefore, activities conducted through electronic media need legal frameworks in order to protect the global community. Considering the growth of electronic media activities in Indonesia, legal frameworks such as cyber law, telematics law, or electronic law are necessary to support such activities. The term cyberlaw, as suggested by Saini, Rao, and Panda, (2012). is preferred by the author as translation. Internationally, cyber law refers to legal terms related to the use of information and communication technology. Other terms used include law of information technology, virtual world law, and mayantara law. Technological advancements have transformed the structure of society from local to a more global community, and this is due to the emergence of information technology. The development of information technology is combined with the use of media and computers, which have given birth to a new tool known as the internet (Wahid and Labib, 2005: 103).

Cyber law is a multidisciplinary law that relates to other branches of science such as criminal law, civil law, consumer protection, economics, and administration with a technological, sociocultural (ethical), and legal approach. The development of information technology, especially the internet, has brought many benefits to society. However, like two sides of a coin, along with the benefits, the internet can also have negative impacts and can be a means for certain individuals to commit crimes (Reyns, 2017) Nevertheless, in principle, computer technology or information technology is neutral. This means that within itself, there is no intention to harm human beings. It is only humans who, in using it, sometimes seek to exploit its weaknesses for malicious purposes or engage in illegal activities. Crime is closely related and even a part of human creation itself. This means that the higher the level of culture and the more modern a nation, the more modern crime will be in its form, nature, and methods of execution (Ersya, 2017). According to Jewkes, and Yar (2010), what is interesting about cybercrime is the motivation

behind the act. The perpetrator of computer crimes does not do it solely for material gain but for the challenge. What they are thinking about is not what they will gain from their actions, but rather outsmarting a computer system and enjoying the results of their actions.

Based on data from the Indonesian National Police (POLRI), between April 2020 to July 2021, there were at least 937 reported cases. Out of these 937 cases, three types of cases had the highest number of reports, namely provocative cases, hate content, and hate speech with around 473 cases. This was followed by online fraud with 259 cases and pornography content with 82 cases.

In several literatures, cyber crime is often equated with computer crime. The U.S Department of Justice provides the definition of computer crime as "...any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution". Another definition is given by the Organization of European Community Development, which states that "any illegal, unethical, or unauthorized behavior relating to the automatic processing and/or the transmission of data" (www.interpol.go.id, January 2nd, 2013). Meanwhile, Barda Nawawi Arief (2003: 255) uses the term mayantara criminality to refer to this type of crime uses the term cyber crime with computer crime, in which the crime in the computer field generally means illegal usage.

In the constellation of Indonesian criminal law, cybercrime falls under the category of special crimes, even though its primary elements can be equated with several articles in the Indonesian Criminal Code (KUHP). However, it is committed in new ways or modes, which requires a more complex legal instrument in combating such crimes. As mentioned by Soerjono Soekanto (2007:8), one of the factors that influences law enforcement is the means and resources that support law enforcement efforts. For this reason, to address the development of crimes through information technology, the Indonesian House of Representatives passed the Electronic Information and Transactions (ITE) Law in late March 2008. This regulation, which had been designed since 1999, can be a good legal instrument in responding to the development of cybercrime. However, this law still has some problems from both non-legal and legal aspects. Legal issues that are often encountered are related to the delivery of information, communication, and/or electronic transactions, especially in terms of proof and legal actions carried out through electronic systems. Therefore, based on the background above, a problem can be formulated, which is how to address legal issues in combating cybercrime in Indonesia?

2. Research Methods

The author employed a normative research method with a descriptive approach to investigate the legal regulations related to cybercrime. The objective of this research is to contribute to a deeper understanding of legal issues surrounding cyber law in Indonesia. The normative research method was utilized to analyze and interpret the existing legal regulations and provide an explanation of their context within the field of cybercrime. With a descriptive approach, the author explored the characteristics of the existing legal regulations and elucidated their implications in the legal context concerning cybercrimes. This research is expected to offer a more comprehensive understanding of legal issues pertaining to cyber law in Indonesia, thus serving as a crucial reference for stakeholders involved in the handling of cybercrime cases, policy formulation, or the development of laws in this field.

3. Cyber Crime In The Context Of Criminal Law

3.1 Forms of Cybercrime Action

In combating Cybercrime, there is a need for Cyber Law or the aspect of law whose term originates from the Cyberspace Law, which encompasses every aspect related to individuals or legal subjects utilizing and making use of internet/electronic technology from the time they initiate "online" and enter the cyber or virtual world. In countries that have progressed in using the internet/electronics as a tool to facilitate every aspect of their lives, the development of Cyber Law is already highly advanced (Hawdon, Parti, and Dearden, 2020).

Jonathan Rosenoer (1997) has classified Cyber Law into various categories such as Copyright, Trademark, Defamation, Hate Speech, Hacking, Viruses, Illegal Access, The Regulation Internet of Resource, Privacy, Duty Care, Criminal Liability, Procedural Issues, Electronic Contract, Pornography, Robbery, Consumer Protection, E-Commerce, and E-Government. These categories cover a wide range of topics including intellectual property rights, cybercrime, online transactions, online privacy, and consumer protection. The Cyber Law also focuses on the regulation and management of the internet resources, jurisdiction, and investigation procedures related to cyber-crimes. Cybercrime can be classified into various categories based on the nature of the act and the target of the criminal activity. Some of the common types of cybercrime include hacking, phishing, malware attacks, identity theft, cyberstalking, and online fraud.

Hacking refers to the unauthorized access to computer systems or networks, with the intent to gain sensitive information, cause damage or disrupt operations. Phishing involves tricking users into revealing sensitive information such as login credentials, credit card numbers or other personal data by posing as a legitimate entity, typically via email.

Malware attacks involve the deployment of malicious software or code on a system or network, with the intent to breach security, steal data or cause damage. Identity theft involves stealing personal information and using it for fraudulent purposes, such as opening accounts or making purchases in someone else's name.

Cyberstalking involves using technology to harass or intimidate someone, such as sending threatening messages or posting personal information online. Online fraud involves engaging in financial fraud or other criminal activities on the internet, such as scams, phishing, or other types of fraud.

If reviewed using conventional legal regulations, cybercrime can be categorized as an illegal act. According to Article 1365 of the Civil Code (KUHPerdata), an illegal act is defined as "an act that causes harm to others and requires the perpetrator to be responsible for compensating for the harm." Based on this criterion, cybercrime can be prosecuted using conventional criminal law regulations. Some of these regulationsis is Article 378 of the Indonesian Criminal Code stipulates that said “anyone who, with the intention of benefiting themselves or others, violates the rights of others by using a false name or false identity, using deception or fraud, or using lies to persuade others to give something, incur a debt, or release a debt, shall be punished for fraud with a maximum imprisonment of four years.”

Article 372 of the KUHP on theft, Article 372 of the Criminal Code states that with regard to embezzlement, anyone who intentionally possesses, either completely or in part, someone else's property in a manner that violates their rights and the property is held not as a result of committing

a crime, shall be punished for the act of embezzlement, with a maximum prison sentence of four years.

Article 310 paragraph 2 of the KUHP on falsifying documents, that said “if the act in question is conducted through written or pictorial means that are disseminated, displayed or affixed in a public place, the offender shall be subject to a maximum imprisonment of one year and four months, or a maximum fine of four thousand five hundred Indonesian rupiah for written defamation.

Article 311 of the Indonesian Criminal Code states that Article 311 paragraph 1 of the Criminal Code reads as follows: "Whoever commits the crime of defamation or defamation in writing, if allowed to prove their accusation, but unable to do so and if the accusation is known to be untrue, shall be punished for false accusation with imprisonment for a maximum of four years."

3.2 Cybercrime Offenses under the Electronic Information and Transactions Law (UU ITE)

The regulation of cyber crime in Indonesia is governed by Law Number 11 of 2008 on Information and Electronic Transactions (ITE), as well as Law Number 19 of 2016 which amends Law Number 11 of 2008. The ITE Law contains nine articles which outline the various forms of criminal activities. Cyber crimes under the ITE Law include:

1. Violations of decency, as stipulated in Article 27 section (1)
   “Every individual intentionally and without right distributes and/or transmits and/or enables access to electronic information and/or electronic documents that contain content that violates morality.”
2. Gambling, as stipulated in Article 27 section (2).
   "Every person who intentionally and without right disseminates information aimed at causing hatred or hostility toward individuals or certain groups based on ethnicity, religion, race, or intergroup differences, or encourages others to commit acts of violence or discrimination against them, shall be sentenced to imprisonment of up to six years and/or a fine of up to one billion rupiahs."
3. Defamation or slander, as stipulated in Article 27 section (3).
   “Every person intentionally and without right distributes and/or transmits and/or enables access to electronic information and/or electronic documents that contain defamatory content and/or defamation of character.”
4. Extortion or coercion, as stipulated in Article 27 section (4).
   “Every person who intentionally and without right distributes and/or transmits and/or enables access to electronic information and/or electronic documents that contain extortion and/or threats as referred to in Article 27 paragraph (4) shall be subject to imprisonment for a maximum of 6 (six) years and/or a fine of up to one billion rupiahs.”
5. Spreading false and misleading news to deceive or defraud consumers, as stipulated in Article 28 section (1).
   “Every person intentionally and without authority disseminates false and misleading news that causes consumer losses in Electronic Transactions."

6. Inciting hatred based on race, ethnicity, religion, or societal group, as stipulated in Article 28 section (2)
   "Every individual intentionally and without authority disseminates information aimed at inciting hatred or hostility towards individuals and/or specific groups within society based on ethnicity, religion, race, and inter-group relations (commonly referred to as SARA)."
7. Sending threatening messages or intimidation directed at individuals, as stipulated in Article 29.
   "Every person intentionally and without authority sends Electronic Information and/or Electronic Documents containing violent threats or intimidating content directed personally"
8. Illegal access to any computer system, network or data, as stipulated in Article 30.
   Section 1 :
   ""Every individual intentionally and without authority or against the law accesses the computer and/or electronic systems belonging to others by any means."
   Section 2 :
   "Every individual intentionally and without authority or in violation of the law accesses a computer and/or electronic system by any means, with the purpose of obtaining Electronic Information and/or Electronic Documents."
   Section 3 :
   "Every individual intentionally and without authority or in violation of the law accesses a computer and/or electronic system by any means, through breaching, circumventing, exceeding, or bypassing security systems."
9. Illegal interception of electronic information, documents, or networks, as stipulated in Article 31.
   Section 1 :
   "Every individual intentionally and without authority or in violation of the law engages in interception or eavesdropping on electronic information and/or electronic documents within a specific computer and/or electronic device belonging to someone else."
   Section 2 :
   ""Every individual intentionally and without authority or in violation of the law engages in interception of non-public electronic information and/or electronic documents, transmitted to, from, or within a specific computer and/or electronic device belonging to someone else, whether without causing any changes or causing alterations, removals, and/or disruptions of the electronic information and/or electronic documents being transmitted."

3.3 Legal Complexity in dealing with Cyber Crime in Indonesia

There are several complexities in handling cybercrime in Indonesia. This is because, in the judge's decision-making process, at least 2 valid pieces of evidence are required and they must be absolutely certain that the crime has indeed occurred and was committed by the defendant.

This is referred to as the negative system according to the law (Subekti, 1991). The meaning of the negative system according to the law is as follows:

1. A minimum level of evidence established by laws is needed in order to question a defendant.
2. The judge's conviction of the defendant's guilt is necessary. Even if the evidence exceeds the limits prescribed by the law, if the judge lacks conviction of the defendant's guilt, he or she cannot impose punishment.

Therefore, it can be concluded that the meaning of negative proof according to the law is a theory between the positive system of proof according to the law and the system of proof according to the judge's conviction or conviction in time (Wardani, Eka, and Soewondo, 2020). The negative system according to the law means that someone is presumed innocent until proven validly and convincingly guilty. In cybercrime cases, it is often difficult to gather valid evidence because perpetrators can hide their digital tracks or use disguise techniques. Moreover, cybercrime often involves foreign perpetrators who are difficult to pursue or extradite.

3.4 Electronic evidence

According to Article 1, paragraph (1) of the Electronic Information and Transactions Law (ITE Law) in Indonesia, electronic information refers to one or a collection of electronic data, including but not limited to text, sound, images, maps, designs, photos, electronic data interchange (EDI), electronic mail (email), telegram, telex, telecopy, or similar forms of communication. It also encompasses letters, signs, numbers, access codes, symbols, or perforations that have been processed and carry meaning or can be understood by individuals capable of comprehending them.

Currently, aside from the evidence tools outlined in Article 184, paragraph (1) of the Indonesian Criminal Procedure Code (KUHAP), there has been the emergence of electronic evidence as a new form of evidence. This electronic evidence includes electronic information and documents, which represents a progression and broadening of the existing evidentiary framework. Article 44 of the Electronic Information and Transactions Law (UU ITE) acknowledges the presence of electronic evidence, encompassing electronic information and/or documents as defined in Article 1, paragraphs (1) and (4), as well as Article 5, paragraphs (1), (2), and (3) of the UU ITE, in addition to the provisions already established in the KUHAP.

In Article 5, the existence of electronic evidence is reinforced as a valid form of evidence, outlined as follows:

1. Electronic information and/or electronic documents and/or their printed results are recognized as legally valid evidence.
2. Electronic information and/or electronic documents and/or their printed results, as mentioned in paragraph (1), constitute an extension of valid evidence according to the applicable procedural law in Indonesia.
3. Electronic information and/or electronic documents are deemed valid when utilizing electronic systems in accordance with the provisions set forth in this law.
4. The recognition of electronic evidence is not only stipulated in the Electronic Information and Transactions Law (UU ITE), but it has also been established

previously in Law No. 8 of 1997 concerning Company Documents. In Article 15, paragraph (1), it states that company documents stored in microfilms or other media, as mentioned in Article 12, paragraph (1), and/or their printed results, are considered valid evidence.

4. Legal Complexity In Dealing With Cyber Crime In Indonesia

The expansion of conventional evidentiary tools mentioned in Article 184, paragraph (1) of the Indonesian Criminal Procedure Code (KUHAP) introduces a new form of evidence that is progressive and responsive to the changing times. However, in its application as evidence, electronic data or electronic evidence faces several challenges:

The issue of locus delicti (the scene of the crime): In cybercrime cases, investigators may encounter difficulties in determining the precise location or place where the crime occurred. Perpetrators can alter or erase the digital traces on their devices used to commit cybercrimes or manipulate the location to be different from the actual scene. In addition, the limited capacity of law enforcement, particularly the Indonesian National Police investigators, in handling cybercrimes is evident in both human resources and equipment limitations. The dedicated cybercrime unit within the Indonesian National Police's Criminal Investigation Division (Direktorat Reserse Kriminal Polri) was established on February 3, 2017 (source: www.kompas.com, February 3, 2017). Previously, cybercrime cases were handled by the Special Economic Crime Investigation Division (Direktorat Tindak Pidana Ekonomi Khusus - DIT TIPPID EKSUS), specifically Subdivision V, which dealt with offenses related to cybercrime, information crimes, and electronic transactions.

In addition, the issue of evidence also poses its own challenges for law enforcement agencies. The sought-after evidence in cybercrime cases is often related to everything used to prepare, commit, and produce the results of the offense. Tracking such evidence proves difficult due to the sophistication of internet networks, which provide opportunities for skilled individuals to manipulate or forge their identities in the virtual world. Moreover, information technology is an open system technology susceptible to illegal hacking or cloning, allowing individuals with expertise in the field to manipulate and alter data, including transforming fake data into authentic data.

Furthermore, cybercrime exhibits characteristics where it is typically carried out by a single individual in a closed room. This makes it challenging for investigators to obtain direct witnesses to observe the perpetrator in the act of committing the cybercrime. As a result, the available witnesses are often limited to the victims themselves. In cases related to banking, financial institutions may be inclined to conceal instances of cyber-attacks, as such incidents can damage public trust and the confidence of depositors in the bank.

Finally, the recognized jurisdiction of a country under conventional international law is based on geographical boundaries, while multimedia communication is international, multi-jurisdictional, and borderless. Consequently, it remains uncertain how a country's jurisdiction can be applied to multimedia communication as one of the uses of information technology. Thus, the issue of legal authority (jurisdiction) in enforcing cybercrime laws can give rise to serious challenges due to the borderless nature of the internet. This may lead to jurisdictional disputes among countries that feel aggrieved by cybercrime activities and seek to enforce their own laws.

5. Conclusion

The process of proving and presenting evidence holds a crucial and key role in the judicial proceedings. With the emergence of new criminal activities utilizing novel media and methodologies (modus operandi), it becomes imperative to establish new regulations that can effectively respond to these evolving offenses. One such development in Indonesian criminal law, through the Information and Electronic Transactions Act, is the extension of evidentiary provisions beyond what was previously stipulated in Article 184(1) of the Criminal Procedure Code. This extension includes the inclusion of electronic evidence in the form of electronic information and documents (as outlined in Article 44 of the Electronic Information and Transactions Act).

However, the practical implementation of electronic evidence as valid and admissible evidence within the Indonesian criminal justice system encounters several challenges. These challenges encompass issues surrounding the locus and tempus delicti (the place and time of the offense), the authentication of electronic data, the availability of witnesses, jurisdictional complexities, and the capacity of law enforcement authorities to effectively address these concerns. These complexities render the utilization of electronic evidence in the Indonesian criminal justice system vulnerable and subject to obstacles that necessitate careful consideration and resolution.

To enhance the efficacy of electronic evidence in criminal proceedings, it is crucial to address these challenges through the development and implementation of appropriate legal mechanisms. This may include measures to ensure the integrity and authenticity of electronic data, establishing protocols for the collection and preservation of electronic evidence, enhancing the expertise of law enforcement personnel in handling cybercrimes, and fostering international cooperation to address jurisdictional issues in cross-border cybercrime cases. By addressing these challenges, the Indonesian criminal justice system can effectively adapt to the evolving landscape of criminal activities and promote the fair and just adjudication of cases involving electronic evidence.

References

Badrulzaman, M. D., Sjahdeini, S. R., Soepraptomo, H., Djamil, F., & Soenandar, T. (2001). Kompilasi hukum perikatan.

Bunga, D. (2019). Politik hukum pidana terhadap penanggulangan cybercrime. Jurnal Legislasi Indonesia, 16(1), 1-15.

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

Ersya, M. P. (2017). Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia. *Journal of Moral and Civic Education*, *1*(1), 50-62.

Febriansyah, F. I., Indiantoro, A., & Ikhwan, A. (2023). Model Kejahatan Dunia Maya (Cybercrime) Sebagai Upaya Pembentukan Hukum Nasional. *Legal Standing: Jurnal Ilmu Hukum*, *7*(2), 183-196.

Hawdon, J., Parti, K., & Dearden, T. E. (2020). Cybercrime in America amid COVID-19: The initial results from a natural experiment. *American Journal of Criminal Justice*, *45*(4), 546-562.

Hua, T. K., & Biruk, V. (2021). *Cybersecurity as a Fishing Game: Developing Cybersecurity in the Form of Fishing Game and What Top Management Should Understand*. Partridge Publishing Singapore.

Jewkes, Y., & Yar, M. (2010). Introduction: the Internet, cybercrime, and the challenges of the 21st century.

Koto, I. (2021). Cyber crime according to the ITE law. *International Journal Reglement & Society (IJRS)*, *2*(2), 103-110.

Kristiyono, J. (2015). Budaya internet: Perkembangan teknologi informasi dan komunikasi dalam mendukung penggunaan media di masyarakat. *Scriptura*, *5*(1), 23-30.

Noerhadi, C. C. (2022). Cybercrimes and Alternative Settlement of Intellectual Property (IPR) Disputes in Indonesia. *International Journal of Cyber Criminology*, *16*(1), 89-109.

Nugroho, A., & Chandrawulan, A. A. (2022). Research synthesis of cybercrime laws and COVID-19 in Indonesia: lessons for developed and developing countries. *Security Journal*, 1-20.

Pratama, Y., Sakti, K. I., Setyadi, F., Ibrahim, N. A. A., & Hidayat, A. M. N. (2022, September). Cybercrime: the phenomenon of crime through the internet in Indonesia. In *Proceeding International Conference Restructuring and Transforming Law* (pp. 294-301).

Reyns, B. W. (2017). Routine activity theory and cybercrime: A theoretical appraisal and literature review. *Technocrime and criminological theory*, 35-54.

Rosenoer, J. (1997). *CyberLaw: The law of the Internet*. Springer Science & Business Media.

Saini, H., Rao, Y. S., & Panda, T. C. (2012). Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications*, *2*(2), 202-209.

Soekanto, S. (2004). *Faktor-faktor yang mempengaruhi penegakan hukum. Jakarta: Raja Grafindo.*

Subekti, R. (2016). Kebijakan Pemberian Ganti Kerugian Dalam Pengadaan Tanah Bagi Pembangunan Untuk Kepentingan Umum. *Yustisia Jurnal Hukum*, *5*(2), 376-394.

Wahid, A., & Labib, M. (2005) *Kejahatan Mayantara (Cyber Crime*), Jakarta: Refika Aditama.

Wardani, K., Eka, D., & Soewondo, S. S. (2020). Electronic evidence in criminal procedural law. *JL Pol'y & Globalization*, *104*, 1.