

The Sinergy of Law and Technological Development for Humankind: Cyber Crime

Haryono¹ & Suparno²

^{1,2}Muria Kudus University, Kudus, 59327 Central Java, INDONESIA

*Corresponding author: suparno@umk.ac.id

To Cite This Article: <https://doi.org/10.53797/icccmjssh.v3i3.4.2024>

Received 14 February 2024, Revised 28 February 2024, Accepted 13 March 2024, Available online 15 March 2024

Abstract: This article aims to let us learn more about cyber-crime. The development of this information technology in turn changes the social order and behavior. In fact, it does not only end there, but also changes the reality of the economy, culture, politics and law. Therefore, behind the positive benefits, internet technology also has a small negative impact. Information technology is the mother of cyber-crimes. In other word, cyber-crime is nothing more than wrongful use of computer technology. This research is a normative legal research, so according to the type and nature of the research, the data sources used are secondary data consisting of primary legal materials and secondary legal materials consisting of books, scientific journals, scientific papers and articles that can provide an explanation of the material primary law. Cybercrime actually not only uses the sophistication of computer technology but also utilizes information technology computer in its operation. The development of information technology has also formed a new world society that is no longer hindered by territorial boundaries and has turned everything that is far away from being near what is imaginary into reality. But behind this progress, has also given birth to new unrest with the emergence of sophisticated crime in the form of cybercrime. The increasing number of cybercrime cases (especially in Indonesia) has attracted the attention of the government to immediately enact laws that can be used to trap criminals in cyberspace. The Indonesian government itself has incorporated the Cybercrime Law into the ITE Law Number 11 of 2008, and hopes that the ITE Law Number 11 of 2008 can overcome, reduce, and stop the perpetrators of crime in cyberspace.

Keywords: Cyber-crime, technological development, cyber law

1. Introduction

In societal life, we often encounter changes in all aspects of life, including changes in the community itself, because there is essentially no static society. There are always changes in society dynamically. Either the changes build up in the sense of positive impact in the future for the community or instead bring a bad impact to the community. The change is a technological innovation. Technological advances are also advancing information. Information can be obtained from friends, family, print media and electronic media. Especially in today's modern era, many people are already using new media that is Internet media. Internet presence makes it easy for people to make information and data that is not necessarily found directly in the print media that can be encountered daily. Especially because the obstacles are way and costs are not small. In Indonesia, there can be internet cafes that scattered along the roadside. In addition, there are many public places, educational institutions, cafes, malls, and recreation venues that offer hotspot or Wi-Fi services to people who have laptops or notebooks. Besides, there are many types of mobile phones equipped with Internet applications. Activities based on Internet technology, is now no longer a new thing in the information society. The Internet has even been used by children of preschool age, parents, businessmen, agencies, employees to housewives (Umanailo et al., 2019a).

The development of this information technology in turn changes the social order and behavior. In fact, it does not only end there, but also changes the reality of the economy, culture, politics and law. Therefore, behind the positive benefits, internet technology also has a small negative impact. One of them is used as a means of committing crimes, hereinafter known as internet crime or cybercrime. Besides being known as cybercrime, this term is also called computer-related crime, which is a type of human crime that is committed in cyberspace or the internet through computer facilities to earn money profit as much as possible from others, either by deceiving, deceiving the public, breaking into other people's accounts, or by randomizing a country's information system. This action is carried out by a handful of people

who use it for their own interests but harm others. In fact, in some cases, this type of crime has the potential to cause greater harm to its victims than conventional or traditional types of crime. For example, theft through hacking mode (Koto, 2021).

Information technology is the mother of cyber-crimes. In other word, cyber-crime is nothing more than wrongful use of computer technology. Hence, technological innovations are the primary and perhaps most important tool to fight cyber-crime. With the development of technology, especially those that intersect with information and are connected to the internet, cyber-crime is categorized as an act within the scope of law, especially criminal law as a criminal act in cyberspace. Where the perpetrator in this case has utilized the sophistication or advancement of technology and the growth of the internet. Internet utilization is misused to commit a crime (Oates, 2001).

In responding to the challenges of globalization marked by the swift flow of information globalization has made Indonesia part of the international community that inevitably, like it or not, will face the flow of globalization. To answer these challenges, Indonesia currently has a special law in the era of information disclosure and electronic transactions. The law has been in effect since April 2008. In the legal world, this is a new step to address the development of information technology on how to behave and act in using information technology (Ejiaku, 2014). This law regulates the actions of people everywhere whose actions have legal consequences.

There is hope from all elements of society that this law is able to provide justice. The law is Law Number 11 of 2008 concerning Electronic Information and Transactions. This law was created and born to follow up on the use of information technology. In fact, this law was born as a form of government effort to ensure the security of electronic transactions. In order for this guarantee to be realized, it is not wrong then that this law is said to be a cyber law in Indonesia. As a cyber law, this law can punish the perpetrators of cyber-crime. Based on the description above, the main problem can be drawn, namely how technological developments affect the occurrence of cybercrime? And How is Cyber Crime Legal Arranged in the ITE Law?

2. Methodology

This research is a normative legal research, so according to the type and nature of the research, the data sources used are secondary data consisting of primary legal materials and secondary legal materials consisting of books, scientific journals, scientific papers and articles that can provide an explanation of the material primary law (Zainuddin & Ramadhani, 2021). In this study, researchers used the approach of literature studies. The literature study is a study used to dull information and data with the help of various materials in libraries and the Internet such as documents, books, journals, magazines, historical stories. Meanwhile, according to the literature study experts are theoretical studies, references and other scientific literature related to the culture, values and norms that develop in the social situation studied. The data analysis technique used in this study is a method of content analysis. This analysis is used to obtain valid inference and can be researched based on its context. In this analysis will be the process of selecting, comparing, combining and sorting various information and data until found the relevant (Umanailo et al., 2019b).

3. Analysis and Discussion

3.1 The Influence of Technological Development on the Occurrence of Cyber Crime

The world of internet today has become a parallel form of life and living. It has become inseparable in such a way, that life without internet is beyond imagination. Internet has enabled the use of website communication, email and a lot of anytime anywhere IT solutions for the betterment of human kind. One cannot question the significance and utility of this virtual space but at the same time one also cannot deny the threats and dangers to which we are exposed due to internet. Invention of computer and evolution of internet in modern times has almost become a parallel form of life and living. It is rightly said that development comes with a cost. Crime today remains elusive and hides itself in the face of development. Every crime leaves a social and negative impact and so does the most recently evolved crime.

In most common parlance cybercrime is defined as crimes committed on the internet using the computer as either a tool or a targeted victim. Technically – “Cyber Crime can be said to those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime.” Earlier it was very difficult to categorise these crimes into a particular specified fashion because every day a different type of crime was witnessed. Now, since have studied nature of each crime specifically we are able to categorise them. Statistics show that in 21 century cyber-crime has grown at an alarming rate owing to new innovations in Information Technology. Realising the quantum of loss and insecurity it can cause, worldwide Governments, Police Departments and Intelligence units have started to respond strictly to such happenings. Different laws have been formulated with the help of cyber world is regulated by the Information Technology Act (Karagiannopoulos et al., 2021).

Cybercrime, first occurred in the United States in the 1960s. In 1970 in the United States there was a case of manipulation of student academic grade data at Brooklyn College in New York, a case of misuse of company computers for the benefit of employees, a case of data copying for smuggling crimes for the benefit of employees, a case of data copying for the means of smuggling crimes narcotics, and credit card fraud. In addition, there was also a case of unauthorized access unauthorized access to pacific national bank's security database which resulted in a loss of \$10.2

million US in 1978. Furthermore, similar crimes also occurred in a number of countries including Germany, Australia, England, Finland, Sweden, Austria, Japan, Canada, the Netherlands and Indonesia. These crimes attack property wealth, honor of computer systems and networks (Sumarwani, 2017).

According to Raodia (2019), there are 2 (two) types of cybercrime there are 2 (two) types, namely: crimes that use information technology (IT) as a facility and crimes that make information technology (IT) systems and facilities as targets as the target. Examples of the first type are credit card fraud, banking fraud, pornography, and drug trafficking through the internet. While defecting and hacking can be classified as the second type. In this first type of case, position of the internet as a medium of information technology as a medium of advanced technology has been misused as a criminal tool misused as a tool of criminality that not only endangers the regional community, but also the global community regional community (Raodia, 2019).

Technological advances have changed the structure of society from a local society to a global society. It has shifted the structure of society from a local society to a globally structured society. This change caused by the presence of information technology. The development of information technology is combined with media and computers, which then gave birth to a new technology called the internet (Coccia, 2019). New thing called the internet. The presence of the internet has given rise to a new paradigm in human life. Life has changed from a virtual reality to a new virtual reality (real) to a new reality that is virtual. This second reality is usually associated with the internet and cyberspace. This second reality is usually associated with the internet and cyberspace.

Of all the developments in technology, the Internet is one of the most significant inventions to date Over the years there is no doubt that the Internet has developed immensely, providing billions of individuals and organizations across the world with digital communication. Hence individuals and organizations are more dependent on it, as individuals use it for shopping and online transactions and organizations use the Internet to support their business process. However, even though the Internet offers various advantages, it is always threatened by many risks such as cybercrime. Cyber criminals use the Internet as a platform to grow and it is easy for them to go unpunished because of the difficulties involved in tracing the origins of such crime. The main reason for cybercrime is the exploitation of personal information. Therefore, Internet users are at the risk having their personal information leaked. Most of the Internet users are unaware of the concept of protecting information (Anshari et al., 2021).

Cybercrime is one of the new forms or dimensions of contemporary crime caused by the rapid development of technology that is very rapid. This crime has even become an international concern international attention. Cybercrime is one of the dark sides of technological advancement that has a negative impact on the world of technological advances that have a very broad negative impact on all areas of modern life today all areas of modern life today.

Cybercrime is an unlawful act committed by using the internet that is based on the sophistication of the internet using the internet which is based on the sophistication of computer technology and telecommunications telecommunication technology. Cybercrime actually not only uses the sophistication of computer technology but also utilizes information technology computer in its operation (Roadia, 2019). The development of information technology has also formed a new world society that is no longer hindered by territorial boundaries and has turned everything that is far away from being near what is imaginary into reality. But behind this progress, has also given birth to new unrest with the emergence of sophisticated crime in the form of cybercrime (Laksana, 2018).

The state of cyberlaws and processes vary widely around the world, often paralleling the general level of online technology used in a nation. Some countries have developed advanced laws and techniques for addressing cybercriminals. Others have few-to-no laws. Most countries, having noted the rise of cybercrime affecting their populations or those of other nations, fall somewhere in the middle. The following section showcases how countries from varied geographic regions address cybercrimes, based on what they view as a cybercrime and how serious those crimes affect them and their allies. Although the cases may vary, they show that cybercrime is a real problem around the world.

3.2 Cyber Crime Legal Arranged in the ITE Law

Crimes that occur in cyberspace are born due to the negative impact of technological development, crimes that occur from various forms and types. This has consequences for the legal protection of its users. This is important considering that every human being must be protected in accordance with their dignity as human beings. One form of responsibility of the state for the protection of its citizens is by legal guarantees and concrete actions that protect the community from all forms of crime or acts of violence. From all forms of crime or other deviant acts that may be experienced by the community both in the world of either in the real world or in cyberspace.

The term 'cybercrime' is derived from the term "cybernetics" which implies the science of communication and control over machine and man. The new horizon called cyberspace which means anything that is moderated by machine for information and communication between societies across the planet. Wherefore, crime committed in cyberspace in relation to machines or devices or cyber technology affiliated to crimes which are to be known as cybercrime. In broader way it is a crime on the internet that includes: hacking, cyber theft, forgery, flowing of viruses, and cyber pornography (Kumari & Bushan, 2021).

Any unlawful activity that happens through digital means is other kind of cybercrime. In facts data theft is one of most common types of cybercrime, but cybercrime includes a variety of vicious activities likely to be known as a) cyber bullying; and b) planting worm or virus.

Indonesia is a state of law as stated in the constitution, as a state of law, of course, the state is obliged to protect every citizen from every action that can harm, let alone these actions can damage the order of the life of the nation and state. Such as crimes that occur in cyberspace or commonly referred to as cybercrime (Widijowati, 2022). This crime that does not recognize space and time has experienced rapid development lately, the sophistication of technology that is misused by irresponsible people for personal gain has made it difficult for developing countries to take action against computer criminals, especially the police, besides the need for a set of rules governing the misuse of this information, human resources and supporting facilities and infrastructure are also needed (Wahyudi, 2013).

The increasing number of cybercrime cases (especially in Indonesia) has attracted the attention of the government to immediately enact laws that can be used to trap criminals in cyberspace. The Indonesian government itself has incorporated the Cybercrime Law into the ITE Law Number 11 of 2008, and hopes that the ITE Law Number 11 of 2008 can overcome, reduce, and stop the perpetrators of crime in cyberspace (Habibi & Liviani, 2020). Cybercrime is a crime committed through the use of information technology and computer networks. Cybercrimes can be committed for commercial, political or personal purposes and often cost victims financially or threaten their privacy. Some types of cybercrime include hacking, phishing, malware, and cyberstalking. Indonesia has Law No. 11/2008 on Electronic Information and Transactions (ITE Law) that regulates cybercrime and information technology. Some of the crimes regulated in the ITE Law include: 1) transmission or loading of information containing insults (Article 27 paragraph 1 of the ITE Law). This crime involves the act of sending or posting information that contains insults or defamation of a person through electronic media such as the internet or social media. Perpetrators who are proven to have committed the act of disseminating this crime may be subject to criminal sanctions; and 2) fraud and embezzlement through electronic networks (Article 46 of ITE Law) (Husak, 2005). This crime involves committing fraud or embezzlement through electronic networks such as the internet or social media. Perpetrators who are proven to have committed this crime may be subject to criminal sanctions. In Indonesian criminal law, cybercrime and information technology are considered serious criminal offenses that harm many people.

Prior to the Electronic Transaction Information (ITE) Law, there was no legislation in Indonesia that specifically regulated cybercrime. Therefore, in handling cases related to cybercrime in the period before the existence of the ITE Law, many laws and regulations were used that could be related to cybercrime, both from the Criminal Code (KUHP) and from outside the KUHP. The ITE Law can be said to be the cyber law in Indonesia (Sari, 2018). The following acts of cybercrime (cybercrime) are regulated in Law no. 11 of 2008 concerning Information and Electronic Transactions and Law no. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Information and Electronic Transactions, as follows:

- a. In Article 27 paragraph (1) of Law no. 11 of 2008 it is stated that "Every person intentionally and without rights shares or distributes or makes accessible Electronic Information or Electronic Documents that have contents that violate decency". However, the act of sharing/distributing/creating content of electronic information/electronic documents that violates decency (decency) is not explained by itself in Law no. 11 of 2008. Violation of ethics/decency through internet media itself refers to the Criminal Code. In the context of acts that violate decency through electronic media, Article 27 paragraph (1) of Law Number 11 of 2008 regulates information and electronic transactions, including online pornography and online prostitution. If this crime is committed against children, it will become even more serious. One of the problems caused by the development of information technology through the internet is the number of sites that display pornographic scenes. It seems that nowadays, it is very difficult to protect the Internet from the interference of entertainment dealers who sell pornography.
- b. Online gambling is regulated in Article 27 paragraph (2) of the Electronic Information and Transaction Law. The same regulation also states that: "Everyone intentionally and without rights shares/distributes/make accessible electronic information/electronic documents containing gambling content".
- c. Defamation or humiliation in cyberspace is a prohibition regulated in Article 27 paragraph (3) of Law no. 11 of 2008, which reads: "Everyone intentionally, and without rights, shares/distributes/make accessible electronic information/electronic documents that contain insults or defamation contents." Lawmakers equate humiliation and defamation. Humiliation itself is an act, while one form of humiliation is pollution.
- d. In Article 27 paragraph (4) of Law no. 11 of 2008 prohibits extortion or threats in cyberspace. In the article it is explained: "Anyone who knowingly and without rights distributes and/or transmits and/or makes accessible electronic information and/or electronic documents containing extortion and/or threats". Article 368 (1) of the Criminal Code includes qualifications acts that count as extortion or threats, namely: "Every person who intends to benefit himself or another person unlawfully (illegally), forces someone to give something belonging to that person or another person in whole or in part with violence or threats of violence or creates debt or write off a debt, will be punished with extortion and can be sentenced to up to 9 years in prison."
- e. Law No. 11 of 2008 Article 29 stipulates that: "Any person who intentionally and without rights sends Electronic Information or Electronic Documents containing threats of violence or intimidation aimed at personally". The provisions regarding electronic information and transactions in Article 29 regulate acts of harassment, threats, or other actions taken to cause fear, including certain words or actions. These provisions are similar to cyberstalking arrangements in the United States, Canada, the United Kingdom and other countries. This action is carried out by

utilizing information and communication technology, such as mail bombs, unsolicited hate mail, obscene or threatening email, and others.

- f. The spread of fake news is regulated in Law no. 11/2008 Article 28 paragraph (1), reads: "Everyone intentionally and without rights spreads false/false and misleading news, which results in consumer losses in Electronic Transactions."
- g. Article 28 paragraph (2) of Law Number 11 of 2008 concerning Information and Electronic Transactions regulates the crime, which reads: "Everyone intentionally and without rights disseminates information designed to cause hatred or hostility to certain individuals/community groups based on ethnicity, religion, race, and inter-group (SARA)" (Habibi & Liviani, 2018).
- h. Law No. 11 of 2008, Article 30 stipulates as follows: 1) anyone who knowingly, without rights or against the law (illegally) accesses another person's Computer or Electronic System in any way; 2) anyone intentionally, without rights or against the law (illegal) accesses (opens) a Computer or Electronic System in any way with the intention of obtaining Electronic Information or Electronic Documents; and 3) anyone who violates, breaks through, exceeds, or breaks into the security system intentionally, without rights or against the law (illegal) accessing a Computer or Electronic System."

Law Number 11 of 2008 concerning Information and Electronic Transactions (IET). The rules of criminal acts committed in it are proven to threaten internet users. Since the enactment of Law no. 11 of 2008 concerning Information and Electronic Transactions on April 21, 2008, has caused many victims. Recently, the first amendment was made. Together with the government, the parliament approved about some revision of ITE Law in October 27, 2016 (Revision UU No. 11/2008 about Information and Electronic Transaction). IET law can be used to defeat all cybercrime activities on the internet without exception.

4. Conclusion

Cybercrime is one of the new forms or dimensions of contemporary crime of contemporary crime caused by the rapid development of technology that is very rapid. This crime has even become an international concern international attention. Cybercrime is one of the dark sides of technological advancement that has a negative impact on the world of technological advances that have a very broad negative impact on all areas of modern life today all areas of modern life today. Cybercrime is an unlawful act committed by using the internet that is based on the sophistication of the internet using the internet which is based on the sophistication of computer technology and telecommunications technology. Cybercrime actually not only uses the sophistication of computer technology but also utilizes information technology computer in its operation. The development of information technology has also formed a new world society that is no longer hindered by territorial boundaries and has turned everything that is far away from being near what is imaginary into reality. But behind this progress, has also given birth to new unrest with the emergence of sophisticated crime in the form of cybercrime.

Prior to the Electronic Transaction Information (ITE) Law, there was no legislation in Indonesia that specifically regulated cybercrime. Therefore, in handling cases related to cybercrime in the period before the existence of the ITE Law, many laws and regulations were used that could be related to cybercrime, both from the Criminal Code (KUHP) and from outside the KUHP. The ITE Law can be said to be the cyber law in Indonesia. The increasing number of cybercrime cases (especially in Indonesia) has attracted the attention of the government to immediately enact laws that can be used to trap criminals in cyberspace. The Indonesian government itself has incorporated the Cybercrime Law into the ITE Law Number 11 of 2008, and hopes that the ITE Law Number 11 of 2008 can overcome, reduce, and stop the perpetrators of crime in cyberspace. Law Number 11 of 2008 concerning Information and Electronic Transactions (IET). The rules of criminal acts committed in it are proven to threaten internet users. Since the enactment of Law no. 11 of 2008 concerning Information and Electronic Transactions on April 21, 2008, has caused many victims. Based on the monitoring that the alliance has done there are at least four people who are called the police and become suspects because they are suspected of committing criminal acts regulated in the ITE Law.

Acknowledgement

The authors would like to thank the fellow authors and organizations whose intellectual properties were utilized for this study.

Conflict of Interest

The authors declare no conflicts of interest.

References

- Anshari, M., Almunawar, M. N., & Masri, M. (Eds.). (2021). *FinTech Development for Financial Inclusiveness*. IGI Global.
- Coccia, M. (2019). Why do nations produce science advances and new technology?. *Technology in Society*, 59, 101124.

<https://doi.org/10.1016/j.techsoc.2019.03.007>

Ejiaku, S. A. (2014). Technology adoption: Issues and challenges in information technology adoption in emerging economies. *Journal of International Technology and Information Management*, 23(2), 59-68. <https://doi.org/10.58729/1941-6679.1071>

Habibi, M. R., & Liviani, I. (2020). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam*, 23(2), 400-426. <https://doi.org/10.15642/alqanun.2020.23.2.400-426>

Husak, D. (2005). Criminal law theory. *The Blackwell Guide to the Philosophy of Law and Legal Theory*, 107-121. <https://doi.org/10.1002/9780470690116>

Karagiannopoulos, V., Kirby, A., Ms, S. O. M., & Sugiura, L. (2021). Cybercrime awareness and victimisation in individuals over 60 years: A Portsmouth case study. *Computer Law & Security Review*, 43, 105615. <https://doi.org/10.1016/j.clsr.2021.105615>

Koto, I. (2021). Cyber crime according to the ITE law. *International Journal Reglement & Society (IJRS)*, 2(2), 103-110. <https://doi.org/10.55357/ijrs.v2i2.124>.

Kumari, A., & Bhushan, S. (2021). Cybercrime: the high criminals and technology. *UGC Care Journal*, 44(1), 24-28.

Laksana, A. W. (2018). Cybercrime Comparison Under Criminal Law In Some Countries. *Jurnal Pembaharuan Hukum*, 5(2), 217-226.

Oates, B. (2001). Cyber crime: How technology makes it easy and what to do about it. *Information systems management*, 18(3), 92. <https://doi.org/10.1201/1086/43298.9.6.20010102/30989.8>

Raodia, R. (2019). Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (Cybercrime). *Jurisprudentie: Jurusan Ilmu Hukum Fakultas Syariah Dan Hukum*, 6(2), 230-239. <https://doi.org/10.24252/jurisprudentie.v6i2.11399>

Sari, N. W. (2018). Kejahatan cyber dalam perkembangan teknologi informasi berbasis komputer. *Jurnal Surya Kencana Dua: Dinamika Masalah Hukum Dan Keadilan*, 5(2), 577-593. *Scribbr*. <https://core.ac.uk/reader/337609060>

Sumarwani, S. (2014). Tinjauan Yuridis Pidana Cybercrime Dalam Perpektif Hukum Pidana Positif. *Jurnal Pembaharuan Hukum*, 1(3), 287-296. *Scribbr*. <https://jurnal.unissula.ac.id/index.php/PH/article/view/1489>

Umanailo, M. C. B., Yulisvestra, M., Oki, K. K., Mulyasari, W., & Ridwan, R. (2019a). The Thought of Emile Durkheim in the Contestation of Development in Indonesia. *Int. J. Sci. Technol. Res*, 8(8), 1881-1885.

Umanailo, M., Fachruddin, I., Mayasari, D., Kurniawan, R., Agustin, D. N., Ganefwati, R., ... & Hallatu, T. G. R. (2019b). Cybercrime case as impact development of communication technology that troubling society. *International Journal Of Scientific & Technology Research*, 8(9), 1224-1228.

Wahyudi, D. (2013). Perlindungan Hukum Terhadap Korban Kejahatan Cyber Crime Di Indonesia. *Jurnal Ilmu Hukum Jambi*, 4(1), 43295.

Widijowati, D. (2022). Legal Complexity in Dealing with Cyber Crime in Indonesia. *Research Horizon*, 2(6), 597-606. <https://doi.org/10.54518/rh.2.6.2022.597-606>

Zainuddin, Z., & Ramadhani, R. (2021). The Legal Force Of Electronic Signatures In Online Mortgage Registration. *Jurnal Penelitian Hukum De Jure*, 21(2), 243-252.