The Development of Law in The Digital Era Towards Globalization

Lia Yuwannita
{derahbi28@gmail.com}
Universitas Jayabaya, Jakarta, Indonesia

Abstract. Advancements in today's digital era are bounded to the movement towards the era of globalization. This era has made human activities inseparable from digitalization. An adequate legal system that adjusts to this condition is also needed. The digital globalization strongly affects the legal system of a country, because it consequently requires legal globalization. The role of law in the development of the digital world in the current era of globalization and modernization is still being questioned for the presence of law is undeniably required to regulate all aspects of social life including social, political, cultural, and educational aspects. The law also has essential roles in organizing digital activities.

Keywords: Digital Era, Globalization, Legal System

1 Introduction

In the United Nations Congressional Resolution VIII (1990) regarding Computer-related crimes, proposed several policies which, among others, urge member countries to intensify efforts to tackle computer abuse more effectively by considering the following steps: (1) Modernizing the law material crime and criminal procedural law; (2) Develop computer prevention and security measures; (3) Take steps to sensitize citizens, court officials, and law enforcement, to the importance of preventing computer-related crimes.

In the context of realizing the international call for tackling cybercrime, matters concerning substantive crimes that need to be changed are the concept of criminal responsibility. As stated above, in principle, liability in criminal law is liability based on fault. However, in relation to overcoming cybercrime, specifically the protection of computer security systems by internet service providers or officials/officers in charge of these tasks, apart from liability base on fault to the perpetrators, it is necessary to consider the possibility of strict liability.

This responsibility means that an offender can be punished solely because the elements of a criminal act have been fulfilled without further regard for the mistakes of the maker in committing the crime. In the context of cybercrime, it means that the owner of the internet service provider institution or the official/officer or the person in charge of information technology is responsible for the security of the computer system. Further consequences if internet crimes are committed through computers that are under their responsibility, then the owner or person responsible for the field of information technology can be punished.

In relation to substantive crimes, while waiting for a more comprehensive cyber law, it is necessary to add several provisions in the Criminal Code concerning theft, fraud, forgery or destruction to tackle cybercrime whose modus operandi is developing every time. Many

ICLHR 2021, April 14-15, Jakarta, Indonesia

DOI 10.4108/eai.14-4-2021.2312312

countries have done this, including the Netherlands, Canada, Denmark, Finland, Italy, Germany, France and Greece. However, there are some countries that make special laws relating to computers, such as Israel and the UK. In addition, there are those who include cybercrime in the telecommunications law, such as China.

Article 97 or Article 103 WvS, without changing the existing form. In Article 97 – the new provisions added to the WvS – states, “Hij die wederechtelijk binnendring in een daartegen beveiligd geatutomatiseerd werk voor de opslag of werking van gegevens, of in een daartegen beveiligd deel daar van, wordt gestraft met gevangeninnistraf van ten hoogste zes maanden of geldboete van de derde catagorie”. Sedangkan dalam Pasal 103 WvS dinyatakan, “Hij die opzettelijk door misdrijf uit een geautomattiseerd werk verkregen gegevens met winsttoogmerk bekend maakt of gebruikt, wordt gestraft met gevangennisstraf van ten hoogste drie jaren of geldboete van de vierde catagorie." [free translation: Anyone illegally interfering with the protected computerized work for the storage or operation of data, or any protected part thereof, shall be punished with imprisonment of up to six months or a fine of the third category.” Whereas in Article 103 WvS it is stated, “Anyone who knowingly discloses or uses data obtained from an automated work to gain profit through crime, will be punished with imprisonment of up to three years or a fourth category fine].

In compiling cyber law related to cybercrime prevention, it is advisable to compare it with the draft Cyber Crime Convention produced by the European Committee on Crime Problem (2001). Some interesting keywords to look at include Illegal access, Illegal interception, Data interference, System interference, Misuse of devices, computer-related forgery, and computer-related fraud. Electronic data as legal evidence in court. In addition, if we refer to the 5 valid pieces of evidence as described above, the only evidence that is strong enough in terms of proving in court against cybercrime cases is expert testimony.

Based on the Criminal Procedure Code, instructions can only be obtained as evidence if they come from witness statements, letters, or statements from the defendant, not including expert testimony. Therefore, in the revision of the Criminal Procedure Code or at least in the procedural law relating to cybercrime, it is necessary to add that instructions as evidence can also be obtained by judges from expert statements. In fact, it is very possible, in addition to the five pieces of evidence plus electronic data, specifically regarding cybercrime evidence, it is necessary to add evidence of the judge's knowledge.

This means that the judges who try these cases have control or at least know about cyberspace. In addition, training regarding cyberspace for law enforcement officers is necessary. Because it is impossible for a judge to reject a case on the grounds that it does not exist or does not know the law. It is a basic postulate in legal science known as the adage ius curia novit. That is, a judge is considered to know the law.

Based on the number of incoming police reports and the number of completed cases reported by the subagbinops ditreskrimsus throughout the Regional Police, the trend of cybercrime is as follows:

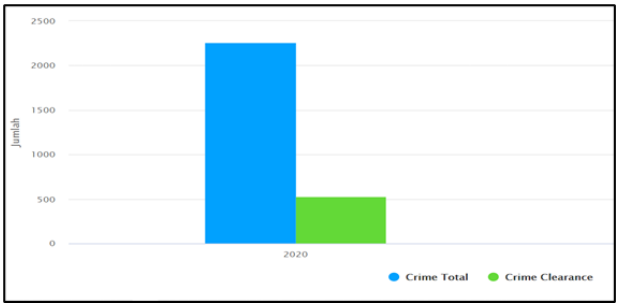

Fig 1. Trends in cybercrime in Indonesia (Directorate of Cybercrime, Police of the Republic of Indonesia, 2020)

In connection with some of these things, it requires legal globalization to be able to develop integrated and sustainable law (rechtsbeofening) in Indonesia (Sulistiyono, 2007) in accordance with the national legal order (Indonesian legal system) based on the values contained in the substance of Pancasila and the 1945 Constitution. Legal development is a job as old as the work of developing the state and nation (Wignjosoebroto, 2002). The presence of law as written law through legislation and in the judicial process as jurisprudence (judge-made law) has also long been known in the legal world, as well as parts of Indonesian law that are currently increasingly important and influential.

Based on the above, the development of digital globalization requires the legal world to continue to develop with the aim that there is no legal vacuum in the event of legal problems related to the digital world that have global effects. One of the things that most often occurs is related to criminal acts of fraud carried out through digital activities, besides that, what often happens is also defamation carried out by misuse of social media.

Cybercrime

According to Van Hamel, the definition of a criminal act (strafbaar feit) is the behavior of a person (menselijke gedraging) which is formulated in the law (wet), which is against the law, which deserves to be punished (strafwaardig) and is done wrong (Sudaryono, & Surbakti, 2017). Crime in the field of information technology or can be called cybercrime is increasingly prevalent in Indonesia. The definition of cybercrime is human activity in cyberspace that makes computers a target of crime (eg illegal access, site destruction, illegal interception), and human activities that use computers as targets for crime (eg credit card counterfeiting, pornography via the internet). The provisions of criminal law that regulate crimes in the field of information technology are commonly called cybercrime law (Widodo, 2013).

Cybercrime in Indonesia occurs with various motives and is carried out by various actors ranging from teenagers to the elderly, male or female. Cybercrime (Wisnubroto, 2010) is a crime based on telematics technology, hereinafter referred to as a telematics crime in various sources, often referred to as Computer Misuse or Computer Crime (computer crime; computer-related crime; computer-assisted crime); Mayantara crime (cybercrime), computer crime (cyber computer).

The Indonesian National Police (cybercrime unit) uses parameters based on UN congressional documents on The Prevention of Crime and The Treatment of Offenders in Havana, Cuba in 1999 and Vienna, Austria in 2000, stating that there are 2 known terms:

1. Cybercrime in a narrow sense is called computer crime: any illegal behaviour directed by means of electronic operation that target the security of computer system and the data processed by them.
2. Cybercrime in a broader sense is called computer related crime: any illegal behaviour committed by means on relation to, a computer system offering or system or network, including such crime as illegal possession in, offering or distributing information by means of computer system or network.

Cyber Crime

Cybercrimes are all criminal acts that use facilities or with the help of electronic systems. That means that all conventional criminal acts in the Criminal Code if they use the help or means of electronic systems such as murder, trafficking in persons, can be included in the category of cybercrimes in a broad sense. Likewise, criminal acts in Law Number 3 of 2011 concerning Fund Transfers as well as criminal acts of banking and money laundering in Law Number 8 of 2010 concerning Prevention and Eradication of the Crime of Money Laundering. However, in a narrower sense, the regulation of cybercrimes is regulated in Law Number 11 of 2008 concerning Information and Electronic Transactions as amended by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions are the same as the Convention on Cybercrimes.

Mayantara's Crime Characteristics

Clifford (2001) describes the characteristics of cybercrime as follows: Computers as targets of criminal activity. For example: breaking through a computer system without access rights/permits (hacking), hacking followed by other actions such as illegally taking/copying information or data (cracking), hacking followed by damaging the computer system or the information contained therein (sabotage); Computer as a tool/means to do evil deeds. Examples: fraud (fraud), theft (theft), embezzlement (embezzlement), forgery (forgery), and other crimes that use computers as a means; Computers as an incidental aspect of malicious behaviour. Example: drug dealing business when the accounting system and transactions use computers or use computers to write threats/terror letters.

The Convention on Cybercrime (Budapest, 23.XI.2001) does not define cybercrimes, but provides provisions that can be classified into:

Title 1	–	Offences against the confidentiality, integrity and availability of computer data and systems
Title 2	–	Computer-related offences
Title 3	–	Content-related offences
Title 4	–	Offences related to infringements of copyright and related rights
Title 5	–	Ancillary liability and sanctions Corporate Liability

2 Research Methods

This type of research is normative legal research that uses a combination of sociological approach, and statutory approach, as well as media law approach (media of law), as well as changes in the culture of digital technology in digital media (the change of culture). technology in digitizing media). This is applied to deepen and investigate the development of legal norms and legal institutions that take policies on changes in the use of media technology with internet-

based digital systems, which are related to the impact of the emergence of legal problems in the digital era society or more popular with the term society disruption.

The impact of legal problems that occur is an attempt to violate legal actions related to criminal acts. Approach to legislation (statute approach) by reviewing all laws and regulations related to the substance of this research problem. Then the researcher also uses secondary data materials in the form of textbooks related to the problem, while tertiary legal materials are instructions or explanations for primary legal materials and secondary legal materials such as information and communication technology literacy, legal dictionaries, and encyclopaedias.

The collection of these materials is carried out through a literature study by collecting and analysing library materials; thus, the author also analyses legal research materials using the inductive analysis method.

3 Results and Discussion

Readiness of Legal Infrastructure or Legal Instruments to Face Digital Problems

The digital era has brought various good changes as positive impacts are used as well as possible. However, apart from bringing a positive impact, the digital era can also have a negative impact, so that it becomes a new challenge in human life in this digital era. Challenges in the digital era have also entered various fields such as politics, economy, socio-culture, defence, security, and information technology itself. The digital era was born with the emergence of digital, internet networks, especially computer information technology. The new media of the digital era has the characteristics of being able to be manipulated, network, or internet. The mass media switch to new media or the internet because there is a cultural shift in the delivery of information.

The ability of this digital era media makes it easier for people to receive information faster. With the internet, the mass media have moved in droves. The more sophisticated digital technology today makes big changes to the world, the birth of various kinds of increasingly advanced digital technology has emerged. Various groups have been facilitated in accessing information through many ways and can enjoy the facilities of digital technology freely and in control. The digital era has also made the realm of people's privacy seem lost. Personal data recorded in the computer's brain makes internet residents easy to track, both in terms of surfing habits and hobbies. The digital era is not a matter of being ready or not, nor is it an option, but a consequence. Technology will continue to move like ocean currents that continue to run during human life. So, there is no other choice but to master and control technology properly and correctly to provide the maximum benefit.

Based on the above, legal infrastructure or legal instruments are needed that will be used in the real world in the event of adequate cybercrimes or digital crimes. Whereas what is meant by infrastructure, in this case, is all types of facilities needed by the public to support various community activities in daily life. Based on this, what is meant by legal infrastructure according to the researcher is all legal facilities or facilities that are formed to prevent or become signs for all community activities in daily life so that they remain controlled and do not violate the law and all applicable regulations. While what is meant by legal instruments according to the Big Indonesian Dictionary, there are two meanings, the first means law, and the second means constitution.

That if it is seen from the readiness of legal infrastructure or legal instruments to face digital problems in Indonesia, which is related to digital technology, it can encourage various advances, especially in Indonesia. In terms of infrastructure and laws that regulate activities in the digital world, Indonesia is ready to live in the digital era. Indonesia's readiness for digital progress can be seen from the internet connection which is currently getting better in the digital era of Information and Electronic Transactions (ITE). The internet-based digital world makes all the activities of its residents unlimited by space and time.

The legal umbrella to regulate all forms of these activities, such as the Electronic Information and Transactions Law (UU ITE) in 2008 must continue to be refined because the development of the digital era in Indonesia, including the mass media in Indonesia, has changed in conveying information. Even though Indonesia is late in adopting communication technology, especially the internet, compared to other countries such as America, Europe, and Singapore. However, the digital culture of the Indonesian people is very quick to accept these technological developments. Globally, Indonesia is included in the digital culture that is needed to achieve positive growth in accordance with the progress of the era itself.

Legal policies must have strengthened law enforcement to provide legal certainty on legal rights and obligations for everyone as legal subjects who carry out all transaction activities in the living space of social institutions with internet media. The development of modern society will also experience forms of crime that are different from their nature and form, it can be said that it is getting more complicated with patterns of criminal behaviour that are intentionally made more diverse by using internet-based media, this is related to proving the crimes committed in the cyberspace.

However, the law must not stop and be static, but as crime develops from technological developments, the law must follow its movements dynamically according to the theory of Law as a tool of social engineering, which is a theory put forward by Roscoe Pound, which means the law as a tool of renewal in society. In this term, the law is expected to play a role in changing social values in society. Based on this, the law continues to develop following developments in society. The point is that the law must not go backward, it must not be out of date but must continue to develop following the developments of the present and future times and the law must contain ius constituendum which is the law that is aspired to in the future. "The law will apply in the future and this can be interpreted as in the case of the Draft Law (RUU) which is being discussed between the DPR and the government or other draft laws and regulations. The rules are not yet in effect but are planned to apply in the future.

Whereas based on the above, the agreement of the legal experts and all of this is intended for one purpose to create order and justice, peace for the community. The law that moves dynamically will give serious attention to following the development of society with various forms of crime and the nature of the crime that changes according to the development of the era. Of course, this has a positive legal purpose, there is no legal vacuum (rechtsvacuum), to provide legal protection and certainty to legal subjects as victims (victim) of crimes due to the impact of digital-based crimes. Referring to the protection function on the function of the nature of the law, dynamic law is strongly influenced by legal aspects in legal reform.

Indonesia already has a national regulation in resolving legal issues related to cybercrime (cybercrime) for such unlawful acts, such as manipulating data, hacking, and fraud by using internet media facilities. Law number 19 of 2016 on amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions is expected to be able to unravel legal problems resulting from unlawful acts with various forms of existing crimes. Of course, it is expected to confirm the strengthening of the use of electronic evidence that has been recognized as one of the provisions of evidence based on the provisions of electronic evidence contained in

Article 5 Paragraph (1) of the ITE Law which stipulates that Electronic Information and/or electronic documents and/or results in the print is a piece of valid legal evidence.

This legal evidence in the form of electronic evidence meets material and formal requirements, in line with the provisions of Article 184 Paragraph (1) of the Criminal Procedure Code due to the expansion of strengthening of the existence of electronic documents that are binding and recognized as legal evidence. to provide legal certainty for the operation of the electronic system, especially in terms of evidence relating to legal actions carried out through the electronic system.

In addition, other digital-based legal regulations, namely the Job Creation Law, amend and add several provisions in 3 (three) laws, namely, Law no. 36 of 1999 concerning Telecommunications, Law no. 32 of 2002 on Broadcasting, and Law No. 38 of 2009 on Post. The material for the Job Creation Act is a follow-up to President Joko Widodo's directives on digital transformation which, based on information and communication technology, Job Creation Law also encourages national economic recovery and enters a new era of the global economy, to create a prosperous, prosperous society. and the fair relationship we aspire to together.

What has been said above, it seems that the protection aspect of digital problems for human resources is very important in accelerating the technological revolution in order to place the function of truth and uphold the truth of their rights as the owner of the truth, and to give definite punishment to someone who intentionally commits an act. against the law with proper evidence and create a deterrent effect as the purpose of the law is to provide justice and public order, and the development of this era requires experts to form legal rules that are ius constituendum so that there is no blemish at all to be outdated If the development of digital law in Indonesia is good, it means that Indonesia is ready to face the digital world towards globalization which is full of complicated problems, and with the readiness of legal infrastructure to prevent all cybercrimes or digital crimes.

The Development of Criminal Law in Facing the Development of Information Technology in the Era of Globalization

The law is not a purely empirical phenomenon, but also shows normative characteristics. In a legal context, "sein" and "sollen" cannot be sharply separated from one another. Law is the atmosphere of "das sein" in which "das sollen" takes its form. Facts and rules in law always go hand in hand: law is fact and rule at the same time. From this it appears that legal philosophy is not satisfied with the conclusions of legal theory (Gunarsa & Sidharta, 2013).

Among legal theorists, the latest legal theory is now known to answer the reality of today's globalized world, namely the Triangular concept of legal pluralism (the triangular concept of legal pluralism). The theory was introduced in 2000 and then modified in 2006 by Werner Menski, a law professor at the University of London. Legal experts in the field of law of Asian and African nations who highlight the character of culture and law. Then Menski introduced his legal theory, which is indeed very relevant for the laws of Asian and African nations, as well as for western nations (Ali, 2009).

The Development of Criminal Law in Facing the Development of Information Technology in the Era of Globalization

The law is not a purely empirical phenomenon, but also shows normative characteristics. In a legal context, "sein" and "sollen" cannot be sharply separated from one another. Law is the atmosphere of "das sein" in which "das sollen" takes its form. Facts and rules in law always go

hand in hand: law is fact and rule at the same time. From this it appears that legal philosophy is not satisfied with the conclusions of legal theory (Gunarsa & Sidharta, 2013).

Among legal theorists, the latest legal theory is now known to answer the reality of today's globalized world, namely the Triangular concept of legal pluralism (the triangular concept of legal pluralism). The theory was introduced in 2000 and then modified in 2006 by Werner Menski, a law professor at the University of London. Legal experts in the field of law of Asian and African nations who highlight the character of culture and law. Then Menski introduced his legal theory, which is indeed very relevant for the laws of Asian and African nations, as well as for western nations (Ali, 2009).

Menski's legal theory combines modern natural law theory, positivism, and legal sociology to discuss legal pluralism, which is the reality of the global world, through the triangular concept of legal pluralism. That the concept of law is not only an instrument of legitimacy, but also social engineering. As social engineering, law is a means intended to change the behaviour of citizens in accordance with predetermined goals. If law is the chosen means to achieve certain goals, then the process does not only stop at choosing law as a means and it is hoped that the law can serve the needs of an increasingly complex and diverse modern society. However, the law does not necessarily go hand in hand with the development of society and the technology that follows it. The law may be used as a tool by agents of change, or a pioneer of change is a person or group of people who gain the trust of the community as the leader of one or more social institutions. A social change that is desired or planned is always under the control and supervision of the proprotor of the change. Ways to influence society with an orderly and pre-planned system are called social engineering or social planning. Law has a direct or indirect influence in encouraging social change.

That the concept of law that has a direct influence that can encourage development in the era of globalization, one of which is Menski's theory using the approach of three main types of law, namely the law created by the community, the law created by the state and the law that arises through values and ethics. If this concept of legal pluralism is associated with the three elements of the legal system from Friedman (1969), it can be said that legal plurality does not only concern its substance or structure, but also has an even higher level of plurality in the element of "legal culture" which includes the plurality of existing habits. , the plurality of existing opinions, the plurality of existing beliefs, as well as the plurality of ways of thinking and acting in the field of law. So that this component was developed into the concept of the Menski triangle.

The development of the world of digital technology is also inseparable from the emergence of a crime better known as cybercrime so that the pursuit of knowledge of criminal law becomes more developed, this is marked by the emergence of the Pornography Law or perhaps the Information and Electronic Transaction Law (UU ITE) for example, which aims to tackle the rise of pornography, pornoaction. Of course, this condition also affects the process of making and enforcing laws in Indonesia, which has entered the digital era. Laws that are too formal, rigid, and inflexible, and apply nationally have difficulty accommodating the rapid development of information technology. Laws that have been built so far with the construction of legality principles, territorial principles, and actions are physical. The law is also increasingly pragmatic with the aim of if accommodating all problems in society or containing the goals of the political economy of the rulers, all of which are temporary and local (sectoral locality).

Modern law with its characters and doctrines that have been accepted as legal metanarrative, is now experiencing powerlessness when dealing with the development of information technology. According to Raharjo (2009) technological developments greatly affect

the pattern of public relations. Moreover, Sudarto (1983) clearly states that technological advances have a major influence on crime patterns.

Then Arief (2006) mentions more explicitly that Cybercrime is one of the dark sides of technological progress which has a very broad negative impact on all areas of modern life today. In public relations that have been carried out, including making it a crime media.

The various impacts of the development of telematics technology above are a challenge for how we make laws in the digital era that knows no national borders. How is modern law flexible to be able to continue to adapt to its rapid development. The law is required to be able to protect the rights of its citizens in cyber activities, such as fraud in e-commerce, guarantee the protection of Intellectual Property Rights and avoid all forms of misleading and pornographic content. The context of the application of sectoral national laws requires a global reorientation because the internet does not only connect people or people to countries within one country but throughout the world.

The inability of modern law to reach the problems above makes the virtual world considered a world without law. Onno W. Purbo stated that the internet is seen by most people, users, and social observers as a world without boundaries, without rules, a world of freedom. This is what causes various forms of crime and violations in cyberspace (Wahid & Labib, 2005). Whereas in principle, the virtual world cannot be separated from the reality of the real world, because the people or corporations involved live in the real world. They only present themselves and engage in activities in cyberspace. So, the virtual world is a media, and the cyber community is bound by law. if viewed from the point of criminal policy, efforts to overcome digital or cybercrime (including cybercrime and cyberporn) must be carried out with an integral (systemic) approach, namely a penal approach (criminal law), a technological approach (techno prevention) because cybercrime is a form of from hit-tech crime, cultural approach (cultural), moral approach (educational) and global approach (international cooperation).

Although our country already has regulations and laws that regulate all forms of cybercrime, in concrete the implementation is still not optimal, one of which is the lack of understanding of certain actions where the actions turn out to be included in the cybercrime category, for example, the theft of the customer's cell phone number database in the banking world, which is in fact a lot of marketing that offers its products, one of which is a type of insurance product. The confidentiality of customers should be strictly adhered to by the banking people, even though the person requesting the customer database is the bank itself with a marketing position because this is considered very vulnerable because, for today's era of globalization, technology is increasingly sophisticated even though it is only in the form of a customer's cell phone number, this can become a cybercrime. by hacking applications on mobile phones ranging from WhatsApp applications to be able to hack customers' E-Banking applications.

Therefore, this is very dangerous because it can result in account burglary, even though initially it is only a cell phone number. Due to the continuous development of the digital world of technology that demands the development of criminal law, which now has its lex specialist which is required, there must be continuous improvements, changes, and must continue to develop to balance the development of cybercrime that often occurs today. Because according to researchers, the current regulations governing cybercrime are still not optimal.

4 Conclusion

The latest digital-based legal regulations are contained in the Job Creation Act which amends and adds several provisions in 3 (three) laws, namely, Law no. 36 of 1999 concerning Telecommunications, Law no. 32 of 2002 on Broadcasting, and Law No. 38 of 2009 on Post. The material for the Job Creation Act is a follow-up to President Joko Widodo's directives on digital transformation which, based on information and communication technology, Job Creation Law also encourages national economic recovery and enters a new era of the global economy, to create a prosperous, prosperous society. and the fair relationship we aspire to together.

What has been said above, it seems that the protection aspect of digital problems for human resources is very important in accelerating the technological revolution to place the function of truth and uphold the truth of their rights as the owner of the truth, and to give definite punishment to someone who intentionally commits an act. against the law with proper evidence and create a deterrent effect as the purpose of the law is to provide justice and public order, and the development of this era requires experts to form legal rules that are ius constituendum so that there is no blemish at all to be outdated If the development of digital law in Indonesia is good, it means that Indonesia is ready to face the digital world towards globalization which is full of complicated problems, and with the readiness of legal infrastructure to prevent all cybercrimes or digital crimes.

Indonesia already has regulations and laws that regulate all forms of cybercrime, but in concreto, the implementation is still not optimal, one of which is the lack of understanding of certain actions which turn out to be included in the cybercrime category, for example, the theft of a database of cell phone numbers belonging to customers in the banking world, which In fact, many marketing companies offer their products, one of which is insurance-type products. The confidentiality of customers should be strictly adhered to by the banking people, even though the person requesting the customer database is the bank itself with a marketing position because this is considered very vulnerable because, for today's era of globalization, technology is increasingly sophisticated even though it is only in the form of a customer's cell phone number, this can become a cybercrime.

By hacking applications on mobile phones ranging from WhatsApp applications to be able to hack customers' E-Banking applications. Therefore, this is very dangerous because it can result in account burglary, even though initially it is only a cell phone number. Due to the continuous development of the digital world of technology that demands the development of criminal law, which now has its lex specialist which is required, there must be continuous improvements, changes, and must continue to develop to balance the development of cybercrime that often occurs today. Because according to researchers, the current regulations governing cybercrime are still not optimal.

References

[1] Abdul Wahid & Mohammad Labib. (2005). Kejahatan Mayantara (Cybercrime). Bandung: Refika Aditama.

[2] Ali, A. (2009). Menguak Teori Hukum (Legal Theory) dan Teori Peradilan (Judicialprudence). Jakarta: Kencana Prenada Media Grup.

[3] Arief, B. N. (2006). Tindak Pidana Mayantara. Jakarta: Raja Grafindo Persada.

[4] Clifford, R. D. (2001). Cybercrime: The investigation, prosecution and defense of a computer-related crime. Prosecution and Defense of a Computer-Related Crime.

[5] Direktorat Tindak Pidana Siber Kepolisian Republik Indonesia. “Jumlah Laporan Polisi yang masuk dan jumlah kasus selesai yang dilaporkan oleh Subagbinops Ditreskrimsus seluruh Kepolisian Daerah.” Tersedia Pada: https://patrolisiber.id/statistic
[6] Friedman, L. M. (1969). “Legal culture and social development.” Law and society review, 29-44.
[7] Gunarsa, A., & Sidharta, B. A. (2013). Meuwissen tentang pengembanan hukum, ilmu hukum, teori hukum, dan filsafat hukum. Bandung: Refika Aditama.
[8] Rahardjo, S. (2009). Penegakan Hukum: Suatu Tinjauan Sosiologis. Genta Pub.
[9] Republik Indonesia. (1918). Kitab Undang-undang Hukum Pidana (Wetboek van Stafrecht).
[10] Republik Indonesia. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. LN.2008/No.58, TLN No.4843.
[11] Republik Indonesia. Undang-Undang Nomor 11 Tahun 2020 tentang Cipta Kerja. LN.2020/No.245, TLN No.6573.
[12] Republik Indonesia. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. LN.2016/No. 251, TLN No. 5952.
[13] Republik Indonesia. Undang-undang Nomor 3 Tahun 2011 tentang Transfer Dana. LN.2011/No. 39, TLN No. 5204.
[14] Republik Indonesia. Undang-Undang Nomor 32 Tahun 2002 tentang Penyiaran. LN. 2002/ No. 139. TLN. No. 4252.
[15] Republik Indonesia. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi. LN. 1999/ No. 154, TLN. No. 3881.
[16] Republik Indonesia. Undang-Undang Nomor 38 Tahun 2009 tentang Pos. LN. 2009/ No. 1146, TLN. No. 5065.
[17] Republik Indonesia. Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang. LN. 2010/ No. 122, TLN. No. 5164.
[18] Soetandyo, W. (2002). Hukum, Paradigma, Metode dan Dinamika Masalahnya. Jakarta: Huma.
[19] Sudarto. (1983). Hukum Pidana dan Perkembangan Masyarakat. Bandung: Sinar Baru.
[20] Sudaryono, S., & Surbakti, N. (2017). Hukum Pidana Dasar-Dasar Hukum Pidana Berdasarkan KUHP dan RUU KUHP. Surakarta: Muhammadiyah University Press.
[21] Sulistiyono, A. (2007). “Pembagian Hukum Ekonomi untuk mendukung pencapaian visi Indonesia 2030.” Pidato Pengukuhan Guru Besar Hukum Ekonomi Fakultas Hukum Universitas Sebelas Maret. Surakarta: Universitas Sebelas Maret.
[22] The European Committee on Crime Problems. (June, 2001). 50th Plenary session Convention on Cyber-crime. Strasbourg.
[23] United Nations. (Aug – Sept, 1990). The Eighth Congress on the Prevention of Crime and the Treatment of Offenders. Havana, Cuba.
[24] Widodo. (2013). Aspek Hukum Pidana Kejahatan Mayantara. Yogyakarta: Aswaja Pressindo