International Journal of Multicultural and Multireligious Understanding

http://ijmmu.com
editor@ijmmu.com
ISSN 2364-5369
Volume 10, Issue 9
September, 2023
Pages: 66-75

Socio-Legal Review of Electronic Data Protection in Criminal Policy Formulation in the Era of Globalization

Yenny Febrianty[1]; Farahdinny Siswajanthy[1]; Priyaldi[2]

[1] Faculty of Law at Pakuan Bogor University, Indonesia

[2] Study Program of State Administration, College of Administration, Bina Nusantara Mandiri Pariaman, Indonesia

http://dx.doi.org/10.18415/ijmmu.v10i9.5047

Abstract

The threat of misuse of personal data in Indonesia is increasing, in particular since the government introduced the electronic identity card (e-KTP) program and plans for the police to use it to build the Indonesian Automatic Fingerprint Identification System (INAFIS). However, the plan was eventually canceled by the police because seen overlapping with the e-KTP program. Then the government records personal data, and the private sector such as banks and telecommunications service providers also records the data. The purpose of this paper is to analyze electronic data protection which has become a Cyber Cream in the current era of globalization as well as What is the review of the criminal policy formulation in the electronic data protection effort. With method writing normative juridical. In conclusion, writing This is b a form of legal protection that should be given to victims of criminal acts that have not yet been regulated by Law No. 11 of 2008 related to Information and Electronic Transactions in Indonesia. One of the most common crime threats today is the theft of personal information, in which other people's important data is stolen. As well as the approach to preventing and handling crime by using penal means is a "penal policy" or "penal law enforcement policy" which is carried out through several stages, namely: formulation of legislative policies, application of judicial policies, and execution of executive or administrative policies.

K*eywords:* *Socio-legal; Electronic Data; Formulation Policy Criminal*

Introduction

The development of information and communication technology in this era of globalization is very rapid, not only in one field but in various fields and sectors of life, both in developed countries and developing countries. The development of information and communication technology has changed people's behavior globally (cultural transformation) and caused the world to become borderless and significant social changes run fast. The pace of development of information and communication technology is becoming a criterion for the progress of the nation.

The development of information technology can be seen from the existence of an invention in electronic devices, namely computers that are electronic data processing devices, magnetic, optical, or

systems that carry out logic, arithmetic, and storage functions. The definition of computer not only refers to the form of a personal computer, notebook or something usually used in offices now but covers all equipment that meets the definition as well as that function, including cellphone plane. [1]The use of computer technology that continues to evolve results in the process of convergence between information technology, media, and communication until finally obtaining new facilities namely the internet, as well as its early civilization in cyberspace. Internet network is the fastest innovating media in all fields and the most adaptive to the needs of society.[2]

To the necessity of information technology that can apply past the internet for all sectors, it has become commonplace. The Internet already create a world of computer-based communication that offers a new virtual (indirect) reality as well as unreal) makes all sectors of people's lives can not be separated from to presence Internet. Through the world of the internet or cyberspace, all forms of activity and community creativity run borderless that can across the borders of the countries of the world. The development of information technology is not just can create a global world, but Already develop a new life space for community, namely the life of virtual society (cyber community).[3] In line with the development of the internet which is increasing day by day as well as shows fast speed, then the internet can contribute to an increase in welfare, progress as well human civilization. That is seen from the use of the internet which is used to make it easier for humans to run activity daily activities, for example, e-banking, e-learning, e-commerce, e-government, and others.

Currently, information plays an important role in the economic growth of a country, both developing and developed countries. The government and the private sector are responsible for managing individual information. However, with the advancement of the computer age, there has come a greater threat to the privacy of that individual. In addition, the risk of loss faced by individuals due to information leakage has also increased significantly. Advances in digital technology have fueled rapid growth in the amount of personal data being stored, as well as transmitted via computers, mobile devices, broadband connections, websites, and the media. However, these developments also threaten the privacy and security of personal information. In the legal context of telematics, data refers to the formal representation of concepts, facts, or instructions. In general, data are statements that are taken for granted in everyday use. The term "data" comes from the Latin word "datum" which means "something given ".[4] Data includes all information that is processed through devices that automatically respond to specific purposeful instructions as well as saved To use can be processed. The information included in the data may also include health records, social records, educational records, or relevant parts of the storage system.[5]

The threat of misuse of personal data in Indonesia is increasing, in particular since the government introduced the electronic identity card (e-KTP) program and plans for the police to use it to build the Indonesian Automatic Fingerprint Identification System (INAFIS). However, the plan was eventually canceled by the police because seen overlapping with the e-KTP program. Then the government records personal data, and the private sector such as banks and telecommunications service providers also records the data. Recently, the public was shocked by information about the possibility of leaking the personal data of 25 million cell phone subscribers. The e-KTP program was first introduced by the government in early 2011 as well be the implementation of the NIK program. The aim of the e-KTP program is to create a single identity for each resident that is valid for life, with one card containing the NIK for each resident. each individual.

[1]Widodo, " *Criminal Policy on Computer-Related Crime in Indonesia "* , Dissertation, Postgraduate University of Brawijaya, 2006, p., 235.

[2]Burhan Bungin, *Pornomedia: Sociology of Media, Social Construction of Telematics Technology, & Celebration of Sex in Mass Media* , Prenada Media, Jakarta, 2005, pp. 10-11

3. Sutan Remy Syahdeini, *Computer Crime and Crime* , PT Pustaka Utama Grafiti, Jakarta, 2009, p. 2.

[4]Purwanto, *Research on Digital Data Legal Protection* , National Legal Development Agency, Jakarta, 2007, p. 13

[5]United Kingdom, Data Protection Act 1998, Article 1 paragraph 1

After that, the government recorded population data as part of the implementation of this program. All Citizens' personal information, including identity and physical characteristics, is recorded. Recording of physical characteristics was carried out by scanning fingerprints and eye retinas, which will be used later for biometric verification of KTP holders. Based on information provided by the Ministry of Home Affairs, the results of the data recording will be stored on a chip on the KTP, after being encrypted using certain cryptographic algorithms. However, there are a number of questions that arise regarding the practice of recording e-KTP data. There are different interpretations of regulations and practices that occur in the field. For example, regarding the e-KTP security system. Based on Presidential Decree No. 67 of 2011, " the security system (biometric validation) will only be used fingerprint scanning, but in the practice of recording data, it turns out that recording is also carried out on the retina of the eye ". In accordance with Wikileaks Wire, a presentation by British company Thorpe Glen (2008), regarding surveillance methods that can be held via e-KTP, is increasing worry. Based on that information, by using the e-KTP device, citizens can whereabouts traced as well as their activities. Utilizing this method, the state can easily observe the private life of each citizen which causes civil liberties to be violated so just.

In the world of cybercrime, in general action, the first thing to do is access illegal systems or network computers, which became a step in beginning to do other cyber crimes. When you have access illegal, doer Then interfere with, change, destroy, or obstruct access data on a computer another party No legal, then action the ie data interference. When data is changed illegally That is page front (front page) of a website owned by a party else, then action namely defacing.[6] In line With the increase in cracking and defacing activities in Indonesia, the government needs to develop more effective crime control policies, either through a criminal law approach or a non-criminal approach. Business-related crime prevention criminal law approach, Indonesia actually has several laws that can be used by law enforcement officials as a basis for use prosecuting criminals against electronic data. that law namely the Criminal Code, Law no. 11 of 2008 related to Information and Electronic Transactions (UU ITE), Law no. 36 of 1999 related to Telecommunications and other laws regarding other crimes committed by criminals on electronic data.

From the explanation above, the author tries to write a paper entitled: "Socio-Legal Review of Electronic Data Protection in Criminal Policy Formulation in the Era of Globalization I". Problems that will be studied in the study This namely, How is electronic data protection becoming a Cyber Cream in the current era of globalization? And how is the criminal policy formulation reviewed in the electronic data protection effort?

Discussion

A. Electronic Data Protection as a Cyber Creame in the Era of Globalization

The development of global computer networks, namely the Internet, has created a new world that is cyberspace. Cyberspace is a world of computer-based communication, which brings the concept of virtual reality. The development of computer technology has also presented various kinds types of computer crimes in the cyberspace environment, which are then known by terms such as cybercrime, internet fraud, and the like.[7] Then Volodymyr Golubev said it was the new form of antisocial behavior '. [8] Cybercrime can interpret to be against the law using the internet based on the sophistication of computer technology and telecommunications. Andi Hamzah said cybercrime becomes computer crime or Illegal computer use. Cybercrime (cybercrime) is a term regarding criminal activities that involve the use of computers as a tool, target, or place of crime. Although in general based on the crime committed use the

[6]Widodo, *Criminal Legal Aspects of Mayantara Crime, Aswaja Pressindo* , Yogyakarta, 2013, p. 72.
[7]See http://azamul.files.wordpress.com/2007/06/thesis-cybercrime-di-indonesia.pdf, uploaded on Thursday April 27 2017 at 22.29
[8]Barda Nawawi Arief, *Law Enforcement Issues and Criminal Law Policies in Crime Control,* Kencana, Jakarta, 2007, p. 237.

finished computer main element, this term is also used for conventional criminal activities where computers are used to facilitate the commission of the crime.

There are 3 approaches to use in maintaining security in cyberspace, namely: 1. Technological approach. 2. Social, cultural, and ethical approaches. 3. legal approach. In order to overcome security disturbances, a technological approach is absolutely necessary, because No the existence of network security can make it easy breach is intercepted, or accessed illegally. Cybercrime can look at of 2, namely:

1. The crime of wearing an existing information technology facility

Examples: piracy, pornography, credit card forgery, fraud via email (fraud), online gambling, terrorism, issues of Sara, and others.

2. Crimes that make information technology systems become targets. Examples: theft of personal abstracts, computer virus creation, website breaches, cyber war, Denial of Service (DoS), crimes related to domain names, and others. Crimes involving the use of computer-based technology and telecommunications networks are classified into several forms based on the running mode is:

   a. Unauthorized Access

   Namely, the crime experienced when someone infiltrates a computer network system illegally, without permission from the owner of the computer network system for example probing and port.

   b. Illegal Contents

   Crimes are committed through entering data to the internet regarding things that are not right, unethical, as well can violate the law, for example, the distribution of pornography.

   c. Intentional Spread of Viruses

   This is usually held via e-mail. Many people whose e-mail systems have viruses do that just. This virus is past sent elsewhere in the email.

3. Data Forgery

This type of crime is the goal to falsify data on important documents on the internet. This document is generally institutions that have web-based database sites.

4. Cyber Espionage, Sabotage, and Extortion

Cyber Espionage is a crime that takes advantage of the internet network to spy on the other side, pass Enter the target party's computer network system.

Sabotage and Extortion are types of crimes committed by causing interference, destruction, or destruction of data, connected to computer program Internet.

5. Cyberstalking

This type of crime is committed passing by interrupting someone passing by a computer use, generally using e-mail as well as repeatedly. This crime is like terrorizing someone via the internet. This can be experienced because of the ease of creating an email with a specific address without the need to Include your true identity.

6. Carding

It's a crime committed to steal other people's credit card numbers as well used for trading transactions on the internet.

7. Hacking and Crackers

Hackers in general based on someone who has a keen interest in learning computer systems with details and how to increase their capabilities. Then those who often carry out acts of destruction

on the internet are generally crackers, which uses its ability to do negative things. Cracking activities on the internet have a very broad scope, ranging from hijacking other people's accounts, website hijacking, probing, spreading viruses, and arriving at target disablement. The last action is DoS (Denial Of Service), which is an attack whose goal is to paralyze the target (hang, crash) so it cannot provide services.

8. Cybersquatting and Typosquatting

Cybersquatting is a crime committed past registering the domain name of someone else's company and then trying to sell it to that company at a higher price.

Typosquatting is a passing crime that creates a play on domains, namely domains that are similar to other people's domain names, which become domain names of rival companies.

9. Hijacking

This is the crime of pirating the work of many other people experienced namely Software Piracy (software piracy).

10. Cyber Terrorism

An act of cybercrime is classified as cyberterrorism when it threatens the government or citizens.

Legal actions that occur in cyberspace are legal actions carried out by humans who exist in real life but are carried out through internet facilities. The interactions that occur in legal actions in cyberspace are actually interactions between people in real life but only use the internet as the medium. Therefore, if there is a violation of the rights that are exercised by humans in real life and the rights that are violated are also human rights in real life, then the applicable law that needs to be applied is the law in real life.[9]

Generally, cybercrime is attempting to use computer network facilities without permission and against the law with or without causing changes to the computer facilities entered.[10]

So The conclusion is that there is a business to enter someone else's computer network without that person's knowledge aims to know the nature of things privacy that can cause changes to the computer. Computer crime activity can be classified into 2 (two), namely data fraud and program fraud.[11]

Data fraud, namely data that is not valid enters the system or data that is valid and should be entered and then changed so it's not valid anymore. This form refers to the act of falsifying and/or destroying input data with the aim of changing output. A form of program fraud is when someone changes a computer program, either through direct access to that computer or through a remote data communication network.

Personal data that is directly related to electronic data Law no. 11 of 2008 related to Information and Electronic Transactions (" UU ITE") be main reference answer questions about protecting personal information on the internet.

ITE Law does not specifically cover personal data protection rules. However, implicitly, the law regulates a new understanding related to this protection of electronic data is good in nature public or private. Furthermore, a description of the protection of personal electronic data regulated PP No. 82 of 2012 regarding the Implementation of Electronic Systems and Transactions, which became the implementation of the ITE Law.

[9] Niniek Suparni, *CYBERSPACE Problems & Anticipation of Arrangements* , Sinar Graphic, Jakarta, 2009, p.36.
[10] Merry Magdalena & Maswigrantoro Roes Setiyadi,2007,*Cyberlaw,No Need to Be Afraid* ,Andi Offset, Yogyakarta,2007,p., 37.
[11]Ibid., p. 38

Protection of personal data on electronic systems, such as regulated in the ITE Law, covers several aspects, including protection against unauthorized use, protection for electronic system operators, and protection against illegal access and interference. Article 26 of the ITE Law confirms that the use of personal data in electronic media is necessary to obtain approval from the relevant data owner. Violation of this provision can result in lawsuits for losses incurred. So the ITE Law provides a legal basis regarding the protection of personal data in electronic systems and stipulates obligations for the wearing party that data To use get permission from the data owner as well as avoid using illegitimate ones can make loss to the data owner.

Article 26 of the ITE Law reads as follows:

" *1) The use of any information through electronic media that concerns a person's personal data must be carried out with the consent of the person concerned.*
2) Every person whose rights are violated as referred to in paragraph (1) can file a lawsuit for losses incurred under this Law "

In its elaboration, Article 26 of the ITE Law states, personal data is part of a person's personal rights. Then the definition of personal data is in Article 1 PP PSTE namely, " *certain individual data that is stored, cared for, and kept true and protected by confidentiality ".*

Now there is no attention to the victims of crimes which becomes a sign of the absence of justice and prosperity in the condition of that society.

Here the victim of a crime is someone who has suffered losses due to a crime. [12]As a victim of a crime, a person has the right to obtain legal protection. This legal protection is necessary given optimally, especially for victims who belong to economically vulnerable groups. Legal protection can be in the form of compensation, restitution, and legal assistance, which are regulated in PP No. 44 of 2008 regarding the Provision of Compensation, Restitution, and Assistance to Witnesses and Victims.

In terms of cyber crimes, it is more appropriate for victims to obtain restitution. Based on Article 1 number 5 " Restitution is compensation given to victims or their families by perpetrators or third parties, which can be in the form of returning property, paying compensation for loss or suffering, or reimbursing costs for certain actions. Theft of personal information is a threat of the most common crime today, which is carried out by stealing other people's important data. Important data here includes personal data (name, address, email, cellphone number, etc.), then financial data such as bank data (account numbers), ATM data, and credit card data.

Perpetrators of theft of personal information Can caught the original sanction of 30 paragraphs of Law no. 11 of 2008 Relating to Information and Electronic Transactions, namely " Every person intentionally and without rights or unlawfully access Computers and/or Electronic Systems in any way with the aim of obtaining Electronic Information and/or Electronic Documents ". Through this article, the perpetrators of the theft of information have fulfilled the elements of Article 30 paragraph (2) of the ITE Law, whatever method it takes. namely by infiltrating a computer security system using either certain software or not, the purpose of which is to do so to steal someone's data.

Based on the provisions of Article 46 paragraph (2), " the perpetrator can be subject to imprisonment for a maximum of 7 years and/or a maximum fine of Rp. 700,000,000.00 " .

One additional problem lies in the absence of provisions regarding legal protection for victims in Law No. 11 of 2008 concerning Information and Electronic Transactions. Cyber crime perpetrators such

[12] Rena Yulia, *Victimology of Legal Protection for Crime Victims* , Graha Ilmu, Yogyakarta, 2010, p.51.

as theft should be required to use provide compensation to victims as a form of their responsibility. The amount and type of compensation received by the victim must be determined by The judge on his verdict. The compensation can be in the form of returning property (material). Therefore, it is important to formulate a criminal policy that regulates victim protection, especially in cases of theft of personal information through cyber media, in order to update the ITE Law.

B. Review of Criminal Policy Formulations in Electronic Data Protection Efforts

The term " policy' ' from "policy" in English or " politick" in Dutch. So the term "criminal law policy" can be called " criminal law politics". In foreign literature, the term "criminal law politics" is also known in various ways terms "penal policy", "criminal law policy" or "strafrechtspolitiek ".[13]

The policy formulation stage is the initial step and the basis for stage implementation of the next criminal law, namely the application and implementation stages. There are The policy formulation stage shows the prevention and handling of crime as the responsibility of legislators, not those of the law the duties of law enforcement officers. The formulation stage is also a strategic stage because errors at this stage can be business obstacle prevention and handling at the application and implementation stages.

According to Barda Nawawi Arief, [14]policy formulation is the most strategic stage of " penal policy " because of that stage The legislature has the authority in terms of determining what actions can be punished which are problem-oriented The main points of criminal law include acts that are against the law, mistakes, criminal liability and what witnesses can be imposed.

So crime-fighting efforts do not It is not only the duty of law enforcement officials but also the duty of law-making apparatus (legislative apparatus). Then Barda Nawawi Arief said, " Criminalization policy is not just a policy of determining what crimes can be punished (including criminal sanctions) but covers issues such as whether the formulation policy is compiled in 1 unitary criminal law system (legislative policy) that is harmonious and integrated ".[15]

Technological cybercrime prevention policies are spelled out at the IIIC (International Information Industry Congress), namely: [16]" *The IIIC recognizes that government action and international treaties to harmonize laws and coordinate legal procedures are key in the fight against cybercrime, but warns that these should not be relied upon as the only instruments. Cybercrime is enabled by technology and requires a healthy reliance on technology for its solution. "* In accordance explanation In this case, efforts to overcome criminal acts in the field of information technology are carried out Using the means of "penal" (criminal law), it is necessary to study the material /substance (legal substance reform) of current information technology crimes. In countermeasures through criminal law (penal policy) must be considered as follows What formulate (legislative policy) a regulation p Law that is appropriate for tackling criminal acts in the information technology sector in the future, as well as whether to apply the legislative policy by law enforcement officials.

Related Law No. 8 of 1997 Company Documents have begun to regulate the direction of proof of electronic data.[17] Through this law, the government is trying to regulate the recognition of microfilm and other media, for example, non-paper information storage devices as well as have a level of security that

[13] Barda Nawawi Arief, *Anthology of Criminal Law Policy*, Kencana Prenada Media Group, Bandung, 2008, page 22.

[14] Barda Nawawi Arief, Law Enforcement Issues and Criminal Law Policies in Crime Control, Kencana Prenada Media Media Group, Jakarta, 2008, pp. 78-79

[15]Barda Nawawi Arief, *Kapita Selekta Criminal law*, PT Citra Aditya Bakti, Bandung, 2003,
page 259

[16]ITAC, "IIIC Common Views Paper On Cybercrime", IIIC 2000 Millennium Congress, September 19th, 2000, p1.5. See in Barda Nawawi Arief, *Law Enforcement Issues and Criminal Law Policies in Crime Control*, Kencana Prenada Media Group, Jakarta, 2007, p1m.240.

[17]Isis Ikhwansyah, *Universal Principles for Contact Through E-Commerce and Civil Proof Legal Systems in Information Technology, in Cyberlaw: An Introduction*, ELIPS, Bandung, 2002, p. 36.

can guarantee the authenticity of the transformed documents, such as Compact DiskRead Only Memory (CD-ROM) and WriteOne-Read-Many (WORM) became valid evidence, regulated in Article 12 of the Company Documents Law. Electronic information and data arrangements exist in several special laws such as Article 38 of Law no. 15/2002 related to the Crime of Money Laundering, Article 27 of Law no. 16/2003 in conjunction with Law no. 15/2003 related to the Eradication of Criminal Acts of Terrorism, and Article 26 (a) of Law no. 20/2001 regarding Amendments to Law no. 31/1999 regarding the Eradication of Corruption Crimes.

are many applications of electronic information and data evidence in legislation result in multitasking like specialized law enforcement officers' path when trial. This is because there are no clear signs of the acknowledgment of the evidence. The concept of the 2000 Criminal Code Draft Law, where this concept underwent changes until 2008, has regulated electronic evidence, namely:[18] In Book I ("General Provisions ") related Provisions are made evidence:

1. Definition ' goods ' (Article 174/178) which includes intangible objects such as data and computer programs, telephone or telecommunication services, or computer services
2. Definition of' keys ' (Articles 178/182) which include secret codes, computer entry keys, magnetic cards, silly & programmed to open things. Based on Agus Raharjo, [19]the meaning of this key is probably certain codes such as private or public key infrastructure.
3. Definition ' letters ' (Article 188/192) include data written or stored on diskettes, magnetic tapes, computer storage media, and others.
4. The definition of ' space ' (Article 189/193) includes a computer terminal that can be accessed in a certain way. The meaning of this space also includes cyberspace or cyberspace or virtual reality.
5. The definition of ' login ' (Article 190/194) includes accessing a computer. In accordance Agus Raharjo entered the global information network system, namely the internet, then entered something that included servers and computers that were included in site management. So there are 2 meanings of entry, namely entering the internet and entering the site.
6. Definition ' telephone ' network (Article 191/195) includes computer networks or computer communication systems.

With the rise of electronic activity, important for evidence that can be worn legally to include electronic information or documents to facilitate legal proceedings. Then the printout of the document also needs to have valid evidence based on law. To facilitate the consumption of electronic evidence (either in electronic form or print), then electronic evidence can be considered to be an expansion of valid evidence, in accordance with procedural law in Indonesia, as regulated in Article 5 of the ITE Law:

1. Electronic Information and/or Electronic Documents and/or printouts are valid legal evidence.
2. Electronic Information and/or Electronic Documents and/or printouts such as the purpose of paragraph (1) is the expansion of legal evidence in accordance with Indonesian procedural law.
3. Electronic Information and/or Electronic Documents are declared valid when using Electronic Systems in accordance with the provisions stipulated in this law.[20]

But electronic evidence cannot be used for specific matters such as those in Article 5 paragraph (4) of the ITE Law stating that Provisions related to Electronic Information and/or Electronic Documents as in paragraph (1) do not apply to:

a. a letter based on the law must be made & in written form; And
b. the letter and its documents in accordance with the law must be drawn up in the form of a notarial deed by the official who made the deed.[21]

[18]Barda Nawawi Arief, *Criminal Law Reform in the Perspective of Comparative Studies,* PT. Citra Aditya Bakti, Bandung, 2005, pp. 131-133.
[19]Agus Raharjo,*Understanding CyberCrime and Technology Crime Prevention Efforts*,PT Citra Aditya Bakti, Bandung,2002,p. 236
[20]Article 5 paragraph (1),(2) and (3) of Law No.11 of 2008 concerning Information and Electronic Transactions, promulgated on 28 April 2008, State Gazette No.58.

Letters that are required by law to be made in writing, such as in the process of marriage and divorce, documents that must be in written form according to law, agreements related to immovable property transactions, documents regarding ownership rights, and documents other regulations regulated by laws that require approval by a notary or authorized official. Electronic evidence will only be considered valid if it uses an electronic system that complies with regulations in Indonesia. Electronic evidence can have the force of law if the information can Guaranteed integrity, yes accountability, is accessible, and can be shown. So the person submitting electronic evidence must be able to disclose the information it has from a trusted electronic system. In accordance with Article 5 paragraph (1) of the ITE Law, electronic information has the power of law become valid evidence, if this electronic information is made using an electronic system that can be accounted for according to developments in information technology. In fact, Article 6 of the ITE Law stipulates "Against all legal provisions that require that information needs to be in a written or original form other than what is stipulated in Article 5 paragraph (4), that requirement has been fulfilled in accordance with this Law if the electronic information guaranteed integrity as well can be accounted for, can be accessed, can be displayed then explains a condition ".

Conclusion

From the description above, then in conclusion:

1. The form of legal protection that should be given to victims of criminal acts has not yet been regulated on Law No. 11 of 2008 related to Information and Electronic Transactions in Indonesia. One of the most common crime threats today is the theft of personal information, in which other people's important data is stolen. This important data includes personal information such as name, address, email, and mobile number, as well as financial information such as bank account numbers, ATM data, and credit card data. Because there are no related settings of legal protection for victims in Law No. 11 of 2008 related to Information and Electronic Transactions, a criminal policy is needed that regulates victim protection, especially in case of theft of personal information through cyber world media. One form of that protection Can shape material compensation that must be regulated in the renewal of the ITE Law.
2. In simple terms, there is a difference between crime prevention efforts through "penal" and "non-penal" channels. The "penal" approach focuses more on "repressive" actions or suppression after the crime has occurred, then The "nonpenal" approach places more emphasis on "preventive" actions or prevention before a crime occurs. Penal policy (criminal law policy) is a science and art that has the purpose to improve the formulation of positive legal regulations and provide guidelines for legislators, courts, and executors of court decisions. Pe use of penal policy in handling crime is not a strategic policy. But it's also not a viable policy move simplified by taking an extreme attitude to use abolish criminal law altogether. The problem lies in the policy of its use. Become a policy problem, the use of penal policies can not be carried out in absolute terms, because there is no absolute thing in the field of policy. The approach to preventing and handling crime by using penal means is a "penal policy" or "penal law enforcement policy" that is implemented through several stages, namely: formulation of legislative policies, application of judicial policies, and execution of executive or administrative policies.

References

Agus Raharjo, *Understanding CyberCrime, and Technology Crime Prevention Efforts*, PT Citra Aditya Bakti, Bandung, 2002.

[21]Article 5 paragraph (4) Law No.11 of 2008 concerning Information and Electronic Transactions, promulgated on 28 April 2008, State Gazette No.58.

Barda Nawawi Arief, *Law Enforcement Issues and Criminal Law Policies in Crime Control*, Kencana, Jakarta, 2007.

Barda Nawawi Arief, *Kapita Selekta Criminal Law*, PT Citra Aditya Bakti, Bandung, 2003.

Barda Nawawi Arief, *Anthology of Criminal Law Policy*, Kencana Prenada Media Group, Bandung, 2008.

Barda Nawawi Arief, *Criminal Law Reform in the Perspective of Comparative Studies*, PT. Citra Aditya Bakti, Bandung, 2005.

Burhan Bungin, *Pornomedia: Sociology of Media, Social Construction of Telematics Technology, & Celebration of Sex in Mass Media*, Prenada Media, Jakarta, 2005.

Cameron G. Shilling, *"Privacy and Data Security: New Challenges of The Digital Age* ", New Hampshire Bar Journal, 2011.

Isis Ikhwansyah, *Universal Principles for Contact Through E-Commerce and Civil Proof Legal Systems in Information Technology, in Cyberlaw: An Introduction*, ELIPS, Bandung, 2002.

Sutan Remy Syahdeini, *Computer Crime and Crime*, PT Pustaka Utama Grafiti, Jakarta, 2009.

Shinta Dewi, *Privacy Protection for Personal Information in E-Commerce According to International Law*, Widya Padjajaran, Bandung, 2009.

Paul Marrett, *Information Law in Practice: 2nd Edition*, MPG Books Ltd., Cornwall 2002.

Widodo, *Criminal Policy on Computer-Related Crime in Indonesia*, Dissertation, Postgraduate University of Brawijaya, 2006.

http://azamul.files.wordpress.com/2007/06/thesis-cybercrime-diindonesia.pdf.

Law No. 11 of 2008 concerning Information and Electronic Transactions.

Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (http://creativecommons.org/licenses/by/4.0/).