THE POLITICS OF CRIMINAL LAW IN CYBERCRIME: AN EFFORTS TO COMBAT INFORMATION TECHNOLOGY CRIMES IN INDONESIA

Milla Mudzalifah
Universitas Diponegoro
mileasiregar@gmail.com

Pujiyono
Universitas Diponegoro
pujifhundip@yahoo.com

Abstract

This article aims to analyze the politics of criminal law in cybercrime and its efforts to overcome information technology crimes from cybercrime. This article used a normative juridical approach. This study concludes that legal politics has a significant role in enforcing the Information and Electronic Transaction Law because it is related to the existence of political will in enforcing the Aquo Law, where there is a structure that is very closely related to legal politics. Efforts to deal with information technology crime, as stated in the Preamble to the 1945 Constitution paragraph 4, to date, two cyber laws of the Electronic Information and Transaction Law have been and are or are still in force in Indonesia. Changes to the cyber law of the Information and Electronic Transaction Law occur because of the influence of legal politics, which is the primary policy in determining the direction, form, and content of the law to be formed following the needs of the state at the time the law is enacted and the politics of the government's interests at the time an Act applies.

Keywords: *Cybercrime; Cyberlaw; Information; Technology.*

A. INTRODUCTION

The era of globalization influences the development of technology and the internet for human life. Globalization can be interpreted as an act of process or policy-making something around the world within the scope of application. We cannot avoid technological progress in this life because technological progress will run according to scientific advances. Technology is a tool/extension of human abilities. Technological advances produce some situations humans have never thought of before[1]. Today, it has become a force that shackles our behavior and lifestyle. With its enormous influence, because it is also supported by robust social systems and at an increasing pace, technology has become the guide of human life.

Technological advances have implications for the development of crime. Traditional crimes are now transformed into crimes in cyberspace (cybercrime) using the internet and other electronic tools. The internet

1 Besse Sugiswati, Aspek Hukum Pidana Telematika Terhadap Kemajuan Teknologi Di Era Informasi, *Perspektif*, Vol. 16, No. 1, 2011, page.59

provides opportunities for criminals in cyberspace to commit crimes more neatly, hidden, organized, and able to penetrate space and time with a broad reach. Cybercrime can be carried out as a form of crime by involving several perpetrators in several jurisdictions of different countries, with target victims in other countries as well[2].

Cybercrime is sometimes also known as cyber sabotage and extortion. This crime is committed by disrupting, destroying, or destroying data, computer programs, or computer network systems connected to the internet. Usually, this crime is carried out by injecting a computer virus or specific computer programs so that data and computer programs cannot be used, do not run as they should, or run as desired by the perpetrator[3].

A complete understanding of this relatively new crime is essential to create a comprehensive roadmap to minimize the ability of cybercrime actors to carry out attacks on networks or use computers as a medium for terror propaganda[4]. For this reason, an adequate understanding of the anatomy of cybercrime is required. This relates to how the criminal law policy in tackling cybercrime crime.

Criminal law policy is a policy from the state through authorized bodies to implement the desired regulations, which are expected to be used to express what is contained in society and to achieve what is aspired. Efforts and policies to make reasonable criminal law regulations cannot be separated from the purpose of crime prevention[5].

So the policy or politics of criminal law is also part of criminal politics. From the point of view of criminal politics, the politics of criminal law is identical to the understanding of crime prevention policies with criminal law. Meanwhile, according to Marc Ansel[6], criminal law policy is a science to formulate or formulate positive law to be better than the previous one. Based on this, it is necessary first to examine how the current provisions apply or the positive law regulating the spread of cybercrime to make future policies.

The use of legal remedies, including criminal law, as an effort to overcome social problems, including in the field of law enforcement policies. Crime prevention efforts with criminal law are essentially part of law enforcement efforts (especially criminal law enforcement). The politics of criminal law is part of law enforcement policies. This law enforcement policy is also included in social policy, namely, all reasonable efforts to achieve

2 Ismail Koto., Cyber Crime According to the ITE Law, *International Journal Reglement & Society*, Vol. 2, No. 2, 2021, page.103–110

3 Muhammad Hatta., Efforts to Overcome Cyber Crime Actions in Indonesia, *International Journal of Psychosocial Rehabilitation*, Vol. 24, No. 3, 2020, page.1761–68

4 Gazalba Saleh, Juridical Analysis of the Crime of Online Store Fraud in Indonesia, *Jurnal Hukum Dan Peradilan*, Vol. 11, No. 1, 2022, page.151–175

5 Uni Sabadina, Politik Hukum Pidana Penanggulangan Kejahatan Teknologi Informasi Terkait Kebocoran Data Pribadi Oleh Korporasi Berbasis Online, *Jurnal Lex Renaissance*, Vol. 6, No. 4, 2021, page.799–814

6 Sherly Nelsa Fitri, Politik Hukum Pembentukan Cyber Law Undang-Undang Informasi Dan Transaksi Elektronik Di Indonesia, *Jurnal Justisia : Jurnal Ilmu Hukum, Perundang-Undangan Dan Pranata Sosial*, Vol. 7, No. 1, 2022, page.104–124.

public welfare. Besides that, it aims to achieve the welfare of society in general.

This new crime significantly impacts security in carrying out activities with technology. Many consider that the existence of the Criminal Code cannot reach these new crimes, so the government initiated the birth of regulation on cybercrime[7]. Based on existing documents, the Law on Electronic Information and Transactions (UU ITE) is Act No. 19 of 2016, Amendments to Act No. 11 of 2008.

According to Widodo[8], the imposition of imprisonment for cybercrime perpetrators is an unwise move. This is due to the discrepancy between the characteristics of the perpetrators of criminal acts and the system of fostering prisoners in the Correctional Institution so that the purpose of punishment as regulated in the Correctional Law will not be achieved. According to Widodo[9], as a substitute for punishment, it is social work or supervisory crime. Because there is a match between the characteristics of cybercrime perpetrators and the paradigm of punishment in social work or criminal supervision, the purpose of punishment can be achieved. In line with Widodo's view, in anticipating cybercrime, the Draft Law on the Criminal Code (RUU KUHP) tries to broaden the term's scope to target and capture these crimes. Meanwhile, according to Barda Nawawi Arief[10], in the perspective of criminal law, cybercrime prevention efforts can be seen from various aspects, including aspects of criminalization policy (formulation of criminal acts), aspects of criminal responsibility or punishment and jurisdictional aspects.

Anticipating cybercrime problems is not only done through the Electronic Information and Transaction Law (UU ITE) but also seeks to anticipate it in preparing the Criminal Code Bill. Based on this description, this study aims to analyze the politics of criminal law in cybercrime and how to overcome information technology crimes from cybercrime.

B. RESEARCH METHODS

The research method used is a normative juridical method with a literature study. The literature study examines secondary data from primary and secondary legal materials. This study analyzes the laws and regulations related to cybercrime, namely the Criminal Code, the Telecommunications Law, the ITE Law, and the Criminal Code Bill, which will become legislation in Indonesia. The method used to analyze the data collected in this study is a qualitative analysis method. Normative juridical research that is qualitative

7 Muhammad Isnaeni Puspito Adhi and Eko Soponyono, Crime Combating Policy of Carding in Indonesia in the Political Perspective of Criminal Law, *Law Reform*, Vol. 17, No. 2, 2021, page.135–144.

8 Supanto, Perkembangan Kejahatan Teknologi Informasi (Cyber Crime) Dan Antisipasinya Dengan Penal Policy, *Yustisia Jurnal Hukum*, Vol. 5, No. 1, 2016, page.52–70.

9 Dewi Bunga, Politik Hukum Pidana Terhadap Penanggulangan, *Jurnal Legislasi Indonesia*, Vol. 16, No. 1, 2019, page.1–15

10 Dwila Annisa Rizki Amalia and Mujiono Hafidh Prasetyo, Kebijakan Hukum Pidana Dalam Upaya Penanggulangan Cyber Prostitution, *Jurnal Pembangunan Hukum Indonesia*, Vol. 3, No. 1, 2021, page.228–239.

is research that refers to legal norms contained in legislation and court decisions as well as norms that live and develop in society[11].

C. RESULT AND DISCUSSIONS

1. The Role of Legal Politics in the Formation of Law

Soerjono Soekanto, in his writing entitled Political Science and Law argues that law and politics have a reciprocal relationship. When a law is at the highest level above politics, this causes positive law to include all standards that lead to agreement in society being reached by a constitutional process. Soerjono Soekanto also said that in interpreting the law, the ruler separates himself, struggles to maintain power, and is not polluted by political influence. On the other hand, political actors can accept autonomy and legal institutions when they believe that the rules that must be obeyed are based on policies they have also adhered to since ancient times. Another opinion says that politics strongly influence the law because it is a form of political decision the authorities make[12].

Law works in a particular political situation marked by a relationship between law and legal politics itself, meaning that law is an embodiment of developing values, which are values about justice. So ideally, the law is made by considering the interests that can realize the values of justice. Where legal regulations contain orders and prohibitions, demanding compliance and sanctions, then the law that runs will create order and justice in society[13].

Etymologically, legal politics is the Indonesian interpretation of the Dutch legal term *rechtspolitiek,* which is the wording of *Recht* (regulation) and Politics (policy). According to the Big Indonesian Dictionary (KBBI), a policy is a series of ideas and rules that form the basis for plans for carrying out tasks, initiatives, and approaches to acting logically in acting. So, in short, legal politics means legal policy[14].

According to Mahfud MD, legal politics is a legal policy or an official line of policy regarding the law that will be applied to new laws, or there will be a replacement of laws in old laws. The goal is to achieve the goals of a country. Mahfud MD made it clear that the law cannot be separated from political influence when it is formulated, even the political position is more dominant in it, so it is not easy to find a legal form that is neutral from political influence. Then, legal politics has a role as an activity of selecting the means to achieve a goal in a particular legal or

11 Nuria Siswi Enggarani, Penanggulangan Kejahatan Internet Di Indonesia, *Jurnal Ilmu Hukum*, Vol. 15, No. 2, 2012, page.149–168.

12 Carolina da Cruz, Legal Aspects Of Justice In Criminal Law Enforcement, *Jurnal Pembaharuan Hukum*, Vol. VI, No. 3, 2019, page.396-405.

13 Marwin, Penanggulangan Cyber Crime Melalui Penal Policy, *Jurnal Hukum Ekonomi Syariah*, Vol. 5, No. 1, 2013, page.31–40.

14 Dian Alan Setiawan, et al., The Legal Strategy Of Treating Telematics Crimes In The Field Of Electronic Transactions In Global Trade, *Jurnal Pembaharuan Hukum,* Vol. 8, No. 3, 2021, page.374-393.

social order in a society[15]. Mahfud MD thinks that there is a unity and statutory arrangement consisting of various components that are mutually dependent on each other in the legal system in Indonesia, which is built to achieve the goals of the state and is guided by the basis and ideals of national law contained in the 1945 Constitution. Another elaboration on legal politics is that legal politics is a tool or means and steps that the government can use to create the desired national legal system. With that national legal system, the ideals of the Indonesian nation will be realized[16].

From the definitions of legal politics above, it is concluded that legal politics is a fundamental policy in the administration of the state, especially in the field of law in the context of positive law as a law that will run, is currently running, and has been in force. This stems from the values that grow and live in a society intending to achieve the goals of the state as stated in the Preamble to the 1945 Constitution of the Republic of Indonesia (UUD 1945) in paragraph 4, namely: 1) protecting the entire Indonesian nation and all spilled Indonesian blood; 2) promote the general welfare; 3) educating the nation's life; and (4) participate in carrying out world order based on freedom, eternal peace, and social justice.

Then, the role of legal politics in the formation of law. Between law and politics, which of the two has a more dominant position, legal or political power? The answer to this question depends on the perception and point of view of the people, wanting to see from various angles what we mean by law and what we mean by politics. Let us take a non-dogmatic perspective and view that law is not just a regulation made by political power. Further problems regarding the relationship between legal power and political power can still be prolonged. However, when we adopt an optimistic view, this view will view the law only as a product of political power. Law is a command of the Lawgiver (law is an order from the ruler), in the sense of an order from those who have the highest power or who hold sovereignty [17].

2. Legal Politics in Handling Information Technology Crimes

Increased crime using information technology identified since 2003, for example, carding crimes (credit card fraud), ATM/EDC skimming, hacking, cracking, phishing (internet banking fraud), malware (viruses/worms/trojans/bots), cybersquatting, pornography, online gambling, transnational crime (drug trade, mafia, terrorism, money laundering, human trafficking, underground economy). Thus, general data protection is needed which this understanding refers to protection

15 Endri Susanto and others, Politik Hukum Dalam Penegakkan Undang-Undang Informasi Dan Transaksi Elektronik (Ite), *Jurnal Kompilasi Hukum*, Vol. 6, No. 2, 2021, page.104–122.

16 Sy. Hasyim Azizurrahman, Pembaharuan Kebijakan Penegakan Hukum Pidana Di Era "Cyber", *Masalah-Masalah Hukum*, Vol. 41, No. 2, 2012, page.298-305.

17 Ida Musofiana, Aji Sudarmaji, and Ira Alia Maerani, Aspects Of Legal Protection For Children From Cybercrime, *Jurnal Pembaharuan Hukum,* Vol. 7, No. 3, 2020, page.201-210.

practices and a binding rule, which is further enforced to protect personal information and ensure that data subjects remain in control of their information. In this case, the data owner must be able to decide if he wants to share some information or not, who has access, for how long, and for what reason. Data is the plural form of datum, derived from the Latin word meaning something given. Data is formed from characters in the form of alphabets, numbers, or special symbols. Data is processed through data structures, file structures, and databases[18].

Privacy protection for personal information is growing due to internet users and many transactions through e-commerce, resulting in much personal information that can be processed, profiled, and distributed to other parties. Based on Article 79 paragraph (1) of Act No. 24 of 2013 concerning Amendments to Act No. 23 of 2006 concerning Population Administration (from now on referred to as the Population Administration Law), Article 58 of Government Regulation Number 37 of 2007 concerning Implementation of Act No. 23 of 2006 concerning Population Administration (from now on referred to as PP on Population Administration), and Article 26 paragraph (1) of Act No. 19 of 2016 concerning Amendments to Act No. 11 of 2008 concerning Information and Electronic Transactions (from now on referred to as UU ITE)[19].

These regulations automatically require certainty over the management of data and information, especially in the management of personal data, because without proper and proper data management, it will lead to abuse and cybercrime attacks. Therefore, risk management analysis is needed in dealing with cybercrime attacks[20]. Because this cybercrime crime can potentially lose data information, such problems are still difficult to overcome. Crimes regarding personal data are often found in a company because, in this case, they need to learn how the data is managed and secured properly and correctly. In this case, the company should understand the regulations, principles, and practices regarding protecting personal data. So that irresponsible parties do not misuse someone's data and information.

Nevertheless, there is no regulation regarding protecting personal data, causing many crimes of misuse of information systems and personal data. Therefore a system is needed that can overcome this. As is well known, until now, Indonesia does not have a law that can protect personal data from a person. So far, it is still contained separately in several laws and regulations, so it is necessary to have a law that regulates comprehensively, clearly, and firmly related to the misuse of

18 Haingo Rabarijaona and Devina Arifani, Legal Protection Of Employees / Workers Who Experienced Employment Relationship Impact Digitalization, *Jurnal Pembaharuan Hukum,* Vol. 7, No. 3, 2020, page.211-221.

19 Besse Sugiswati, Aspek Hukum Pidana Telematika Terhadap Kemajuan Teknologi Di Era Informasi, *Perspektif*, Vol. 16, No. 1, 2011, page.59

20 Angga Dewanto Basari, Muhammad Syauqillah, and Asep Usman Ismail, Study on the Implementation of the Regulations of Terrorism Activities in Social Media, *Journal of of Strategic and Global Studies*, Vol. 3, No. 2, 2020, page.1–21

personal data. Currently related to the protection of personal data contained in several laws and regulations, including 1) Act No. 19 of 2016 concerning Amendments to Act No. 11 of 2008 concerning Information and Electronic Transactions; 2) Government Regulation Number 82 of 2012 concerning Electronic System and Transaction Operators.

In essence, politics or criminal law policy is how criminal law can be adequately formulated, provide legislators guidance, and implement criminal law. Legislative policy is decisive in the following stages because when criminal legislation is about to be made, the objectives to be achieved have been determined. The scope of the legislative policy is 1) Replacement of colonial heritage legislation and national laws that are no longer following the development of society; 2) Improving the existing laws and regulations but not following the demands and needs of the community; 3) Forming new laws and regulations that are following the demands and meet the legal needs of the community[21].

When viewed in Article 26, paragraph (2) of the ITE Law, this kind of thing does not provide criminal sanctions to the perpetrator. In this case, the victim only sued civilly. Apart from that, Article 26 of the ITE Law is only about essential protection. Information technology experts consider Article 26 of the ITE Law to have weaknesses. The downside is that there is no user protection whose personal data is used to obtain certain company benefits. Data security is intended to improve data security and serves to 1) Protect data so that unauthorized persons cannot read it; 2) Prevent unauthorized people from inserting or deleting data[22].

Apart from that, the urgency regarding the protection of personal data can be seen with the protection of personal data as part of human rights regulated in Article 12 of the Universal Declaration of Human Rights (UDHR), which provides a legal basis for member countries in terms of the state's obligation to protect and respect the personal rights of their respective citizens. In 2017 the Draft Law on Personal Data Protection (RUU PDP) began to be ratified as a National Legislation Program (*Prolegnas*) and became a Priority *Prolegnas* in 2018 and 2019. And at this time, the PDP Bill is still in the stage of harmonization under the auspices of the Sub Directorate of Research and Technology, Directorate of Harmonization of Legislation II, Directorate General of Legislation, Ministry of Law and Human Rights.

3. Cybercrime Crime Formulation Policy

Cybercrime prevention policies with criminal law include the field of penal policy, which is part of criminal policy. From the point of view of criminal policy, crime prevention efforts (including overcoming cybercrime) cannot be carried out solely partially with criminal law (penal

means). However, they must also be taken with an integral/systemic approach[23]. The operationalization of the penal policy includes criminalization, decriminalization, penalization, and depenalization. Criminal law enforcement is highly dependent on the development of legal, criminal, and social politics. Therefore, law enforcement does not only pay attention to autonomous law but also pays attention to social problems and the science of social behavior. As a form of high-tech crime that can transcend national borders (transnational), it is natural that cybercrime prevention efforts must also be taken with a technological approach (techno prevention). In addition, a cultural/cultural approach, a moral/educational approach, and even a global approach through international cooperation are needed[24].

The criminalization policy is a policy in determining an act that was initially not a crime (not punished) to become a criminal act (a criminal act). According to Bassiouni[25], the decision to criminalize and decriminalize must be based on specific policy factors that take into account various factors, including 1) The balance of the means used concerning the results to be achieved; 2) Cost analysis of the results obtained concerning the objectives sought; 3) Research or interpretation of the goals sought concerning other priorities in the allocation of human resources; 4) The social influence of criminalization and decriminalization related to or viewed from their secondary effects.

Sudarto[26] states that in criminalizing an act, the following four things need to be considered: 1) The use of criminal law needs to pay attention to the national development goals, namely to create a just and prosperous society that is evenly distributed both materially and spiritually based on Pancasila; 2) Actions that are attempted to be prevented or overcome by criminal law should be undesirable acts, namely actions that cause harm (material or spiritual) to members of the community; 3) The use of criminal law needs to consider the cost and benefit principle; 4) The use of criminal law should also pay attention to the capacity or working power of criminal law enforcement agencies so that there is no overload of duties (overbearing).

Concerning the policy of criminalizing acts in cyberspace (cyber), in a workshop on computer-related crime held at the X United Nations congress in April 2000, it was stated that member countries should try to

23 James Popham, Mary McCluskey and Michael Ouellet., Exploring Police-Reported Cybercrime In Canada Variation And Correlates, *Policing: An International Journal*, Vol. 43, No. 1, 2020, page.35-48.

24 Michael Levi and Matthew Leighton Williams, Multi-Agency Partnerships In Cybercrime Reduction Mapping The UK Information Assurance Network Cooperation Space, *Information Management & Computer Security*, Vol. 21, No. 5, 2013, page.420-443.

25 Babayo Sule, Usman Sambo, and Muhammad Yusuf, Countering cybercrimes as the strategy of enhancing sustainable digital economy in Nigeria, *Journal of Financial Crime*

26 Sri Hartati, Hadi Karyono, and Hudi Karno Sabowo, Implementation of The Law on Information and Electronic Transactions and Pancasila Law Enforcement Related to Cybercrimes in Indonesia, *International Journal of Educational Research & Social Sciences*, Vol. 3, No. 1, 2022, page.425–436.

harmonize provisions related to criminalization, proof of, and procedures (states should seek harmonization of the relevant provisions on criminalization evidence and procedure). This means that the criminalization policy on cybercrime is not solely a matter of Indonesian national policy but is also related to regional and international policies (John, 2018). So the problem is not just how to make criminal law policies in the field of cybercrime prevention but how there is a harmonization of penal policies in various countries.

Five things need to be considered by legislators to criminalize cybercrime, namely: 1) Criminalization must be an effort that supports the ultimate goal of criminal policy, namely protecting and prospering the community; 2) The community denounces the act that will be criminalized; 3) It is necessary to take into account the advantages and disadvantages of criminalization; 4) Efforts should be made to prevent over-criminalization which may have a secondary effect on the public interest; 5) Need to be adjusted between the ability of law enforcement and law enforcement.[27]

The criminalization policy or formulation of criminal law in Indonesia related to cybercrime issues so far can be identified as follows:

a. In the Criminal Code

   The formulation of criminal acts in the Criminal Code is mostly still conventional and has yet to be directly related to the development of cybercrime. Besides that, there are also various weaknesses and limitations in dealing with technological developments and high-tech crime, which vary widely. For example, the Criminal Code has difficulties in dealing with credit card counterfeiting and electronic fund transfers because there are no special rules regarding these matters. The existing provisions only concern: a) oath/false statement (Article 242); b) shying away from currency and banknotes (Article 244-252); c) counterfeiting stamps and marks (Articles 253-262); and (d) falsification of letters (Articles 263-276).[28]

b. Laws outside the Criminal Code
   1) Act No.36 of 1999 concerning Telecommunications threatens criminal acts against 1) Manipulating access to telecommunications networks (Article 50 jo.22); 2) Causing physical and electromagnetic disturbances to telecommunications operations (Article 55 jo.38); 3) intercepting information through telecommunications networks (Article 56 jo.40);
   2) Article 26A of Act No. 20 of 2001 concerning Amendments to Act No. 31 of 1999 concerning the Eradication of Criminal Acts of

27 Massulthan Rafi Wijaya and Ridwan Arifin, Cyber Crime in International Legal Instrument: How Indonesia and International Deal with This Crime?, *Indonesian Journal of Criminal Law Studies*, Vol. 5, No. 1, 2020, page.63–74

28 Nurianto Rachmad Soepadmo, Impact Analysis of Information and Electronic Transactions Law (Law No. 19 Year 2016) on the Level of Cyber-Crime in Social Media, *International Journal of Innovation, Creativity and Change*, Vol. 12, No. 8, 2020, page.485–500.

Corruption; Article 38 of Act No. 15 of 2002 concerning the Crime of Money Laundering; and Article 44 paragraph (2) of Act No. 30 of 2002 concerning the Corruption Eradication Commission; recognize electronic records as valid evidence;

3) Act No. 32 of 2002 concerning Broadcasting, among others, regulates criminal acts: 1) Article 57 jo. 36 paragraph (5) threatens punishment for broadcasts that: a) are slanderous, inciting, misleading, or lying; b) highlight elements of violence, obscenity, gambling, narcotics, and drug abuse; or c) opposing ethnicity, religion, race, and between groups; 2) Article 57 jo. 36 paragraph (6) threatens to punish broadcasts that ridicule, demean, harass, or ignore religious values, Indonesian human dignity, or damage international relations; 3) Article 58 jo. 46 paragraph (3) threatens to punish commercial advertisement broadcasts which contain: a) promotions related to the teachings of a religion, ideology, individual, or group, which offends feelings or demeans other people, other ideologies, other individuals, or other groups; b) promotion of liquor or the like and addictive substances or substances; c) promotion of cigarettes that demonstrate the form of cigarettes; d) things that are contrary to public decency and religious values; or e) exploitation of children under the age of 18;[29]
4) Act No.11 of 2008 concerning Information and Electronic Transactions (UU-ITE), Chapter VII Prohibited Acts, contains criminal provisions for any person who intentionally and without rights or unlawfully distributes or transmits or makes information accessible Electronic documents or electronic documents containing: 1) Violating decency; having a gambling charge; contains insults or defamation; has a charge of extortion or threats (Article 27); 2) Spreading false and misleading news that results in consumer losses in electronic transactions; disseminating information aimed at causing feelings of hatred or hostility to specific individuals or community groups based on ethnicity, religion, race, and inter-group (SARA) (Article 28); 3) Sending information containing threats of violence or intimidation aimed at personally (Article 29); 3) Accessing other people's computers or electronic systems; accessing computers or electronic systems to obtain electronic information or electronic documents; accessing computers or electronic systems by violating, breaking through, exceeding, or breaking into the security system (Article 30); 4) Interception or wiretapping of electronic information or electronic documents; conduct an electronic interception of the transmission of electronic information or electronic documents that are not public (Article 31); 5) Change, add, reduce, transmit, destroy,

29 Muhammad Isnaeni Puspito Adhi and Eko Soponyono, Crime Combating Policy of Carding in Indonesia in the Political Perspective of Criminal Law, *Law Reform*, Vol. 17, No. 2, 2021, page.135–144.

remove, transfer, hide electronic information or electronic documents belonging to other people or the public; move or transfer electronic information or electronic documents to the electronic system of another person who is not entitled; result in the disclosure of an electronic information or electronic documents of a confidential nature become accessible to the public with improper data integrity (Article 32); 6) Disruption of the electronic system or resulting in the electronic system not working correctly (Article 33); 7) Produce, sell, procure for use, import, distribute, provide, or possess: a) hardware or software designed or specifically developed to facilitate acts as referred to in Article 27-33; b) password via computer, access code, or other similar things that are intended to make the electronic system accessible to facilitate the actions in Articles 27-33 (Article 34); 8) Manipulating, creating, changing, deleting, and destroying electronic information or electronic documents with the aim that the electronic information or electronic documents are considered as if the data is authentic (Article 35); 9) Performing the acts as referred to in Article 27-34 which cause harm to other people (Article 36); 10) Performing prohibited acts as referred to in Article 27-36 outside the territory of Indonesia against electronic systems located in the territory of the Indonesian Jurisdiction (Article 37)[30].

Cybercrime criminalization in Indonesia, especially in the ITE Law, can be divided into two categories: acts that use computers as a means of crime and acts that make computers target crime. A crime that uses computers as a means is any action that utilizes computer data, computer systems, and computer networks as tools to commit crimes in cyberspace, not real space. A crime that targets a computer is any activity using a computer that is directed at computer data, computer systems, computer networks, or all three together. The act is carried out in cyberspace, not real space, so all activities prohibited by laws and regulations occur in cyberspace.

D. CONCLUSION

Legal politics has a significant role in the process of legal renewal in order to keep pace with the rapid development of the times. The legal renewal reflects efforts to realize the mandate of the fourth paragraph of the 1945 Constitution and other provisions contained therein. In dealing with social change, when there is a change in patterns of legal behavior, it is guided to be a guideline in managing society. The law should follow preambles from the initial formation of the Electronic Information and Transaction Law and the revision of the Electronic Information and

30 Sri Hartati, Hadi Karyono, and Hudi Karno Sabowo, Implementation of The Law on Information and Electronic Transactions and Pancasila Law Enforcement Related to Cybercrimes in Indonesia, *International Journal of Educational Research & Social Sciences*, Vol. 3, No. 1, 2022, page.425–436.

Transaction Law. And law enforcement also pays attention to the application of the principles of justice, equality, and legal certainty because, for now, the Information and Electronic Transaction Law has been formed to follow political will and developments whose content and interpretation are more pro-government and limit the rights of the Indonesian people.

BIBLIOGRAPHY

Adhi, Muhammad Isnaeni Puspito, and Eko Soponyono., Crime Combating Policy of Carding in Indonesia in the Political Perspective of Criminal Law', *Law Reform*, Vol. 17, 2021;

Amalia, Dwila Annisa Rizki, and Mujiono Hafidh Prasetyo., Kebijakan Hukum Pidana Dalam Upaya Penanggulangan Cyber Prostitution, *Jurnal Pembangunan Hukum Indonesia*, Vol. 3, 2021;

Azizurrahman, Sy. Hasyim.,Pembaharuan Kebijakan Penegakan Hukum Pidana Di Era "Cyber", *Masalah-Masalah Hukum*, Vol. 41, 2012;

Basari, Angga Dewanto, Muhammad Syauqillah, and Asep Usman Ismail., Study on the Implementation of the Regulations of Terrorism Activities in Social Media, *Journal of of Strategic and Global Studies*, Vol. 3, 2020;

Bunga, Dewi., Politik Hukum Pidana Terhadap Penanggulangan, *Jurnal Legislasi Indonesia*, Vol. 16, 2019;

Cruz, Carolina da., Legal Aspects Of Justice In Criminal Law Enforcement, *Jurnal Pembaharuan Hukum*, Vol. VI, No. 3, 2019;

Enggarani, Nuria Siswi., Penanggulangan Kejahatan Internet Di Indonesia, *Jurnal Ilmu Hukum*, Vol. 15, 2012;

Fitri, Sherly Nelsa., Politik Hukum Pembentukan Cyber Law Undang-Undang Informasi Dan Transaksi Elektronik Di Indonesia, *Jurnal Justisia : Jurnal Ilmu Hukum, Perundang-Undangan Dan Pranata Sosial*, Vol. 7, 2022;

Hartati, Sri, Hadi Karyono, and Hudi Karno Sabowo., Implementation of The Law on Information and Electronic Transactions and Pancasila Law Enforcement Related to Cybercrimes in Indonesia, *International Journal of Educational Research & Social Sciences*, Vol. 3, 2022;

Hatta, Muhammad, Efforts to Overcome Cyber Crime Actions in Indonesia, *International Journal of Psychosocial Rehabilitation*, Vol. 24, 2020;

Koto, Ismail., Cyber Crime According to the ITE Law, *International Journal Reglement & Society*, Vol. 2, 2021;

Levi, Michael and Matthew Leighton Williams., Multi-Agency Partnerships In Cybercrime Reduction Mapping The UK Information Assurance Network Cooperation Space, *Information Management &*

Computer Security, Vol. 21, No. 5, 2013;

Marwin., Penanggulangan Cyber Crime Melalui Penal Policy, *Jurnal Hukum Ekonomi Syariah*, Vol. 5, 2013;

Musofiana, Ida, Aji Sudarmaji, and Ira Alia Maerani, Aspects Of Legal Protection For Children From Cybercrime, *Jurnal Pembaharuan Hukum,* Vol. 7, No. 3, 2020;

Rabarijaona, Haingo, and Devina Arifani., Legal Protection Of Employees / Workers Who Experienced Employment Relationship Impact Digitalization, *Jurnal Pembaharuan Hukum,* Vol. 7, No. 3, 2020;

Popham, James, Mary McCluskey and Michael Ouellet., Exploring Police-Reported Cybercrime In Canada Variation And Correlates, *Policing: An International Journal*, Vol. 43, No. 1, 2020;

Sabadina, Uni., Politik Hukum Pidana Penanggulangan Kejahatan Teknologi Informasi Terkait Kebocoran Data Pribadi Oleh Korporasi Berbasis Online, *Jurnal Lex Renaissance*, Vol. 6, 2021;

Saleh, Gazalba., Juridical Analysis of the Crime of Online Store Fraud in Indonesia, *Jurnal Hukum Dan Peradilan*, Vol. 11, 2022;

Setiawan, Dian Alan, et al., The Legal Strategy Of Treating Telematics Crimes In The Field Of Electronic Transactions In Global Trade, *Jurnal Pembaharuan Hukum,* Vol. 8, No. 3, 2021;

Soepadmo, Nurianto Rachmad., Impact Analysis of Information and Electronic Transactions Law (Act No. 19 Year 2016) on the Level of Cyber-Crime in Social Media, *International Journal of Innovation, Creativity and Change*, Vol. 12, 2020;

Sule, Babayo, Usman Sambo, and Muhammad Yusuf., Countering Cybercrimes As The Strategy Of Enhancing Sustainable Digital Economy In Nigeria, *Journal of Financial Crime*;

Sugiswati, Besse., Aspek Hukum Pidana Telematika Terhadap Kemajuan Teknologi Di Era Informasi, *Perspektif*, Vol. 16, 2011;

Supanto., Perkembangan Kejahatan Teknologi Informasi (Cyber Crime) Dan Antisipasinya Dengan Penal Policy, *Yustisia Jurnal Hukum*, Vol. 5, 2016;

Susanto, Endri, Hariadi Rahman, Nurazizah, Lisa Aisyah, and Ema Puspitasari., Politik Hukum Dalam Penegakkan Undang-Undang Informasi Dan Transaksi Elektronik (Ite), *Jurnal Kompilasi Hukum*, Vol. 6, 2021;

Wijaya, Massulthan Rafi, and Ridwan Arifin, 'Cyber Crime in International Legal Instrument: How Indonesia and International Deal with This Crime?', *Indonesian Journal of Criminal Law Studies*, Vol. 5, 2020.