SALAM
Jurnal Sosial dan Budaya Syar-i
P-ISSN: 2356-1459. E-ISSN: 2654-9050
Vol. 8 No. 4 (2021), pp. 975-986
DOI: **10.15408/sjsbs.v8i4.21795**
http://journal.uinjkt.ac.id/index.php/salam/index

The Process and Performance of Combating Cyber Crimes In Indonesia*

Sefitrios,[1] Tofik Yanuar Chandra[2]
Magister Ilmu Hukum Universitas Jayabaya Jakarta
10.15408/sjsbs.v8i4.21795

Abstract
Information Security, Electronic Transactions (ITE), and Crime ITE is constantly competing in various issues relating to information and electronic transactions (ITE). Cyber law, also known as information and communication technology law, is a term that is used on a global scale when it comes to the use of information and communication technology. This accomplishment in the field of cybercrime deserves two thumbs up in Indonesia. Although it is still considered a developing country in the real world, local hackers, crackers, and carders have successfully inscribed a very brilliant achievement. The Information and Electronic Transactions Law, also known as Law Number 11 of 2008 or the ITE Law, is a law that governs information and electronic transactions.
Keywords: Criminal Law; Cyber Crime; ITE Law

Abstrak
Keamanan Informasi dan Transaksi Elektronik (ITE) dan Kejahatan ITE selalu beradu dalam berbagai persoalan terkait dengan Informasi dan Transaksi Elektronik (ITE). Hukum siber atau cyber law, secara internasional digunakan dalam pemanfaatan teknologi informasi dan komunikasi. Di Indonesia sendiri juga sebenarnya prestasi dalam bidang cyber crime ini patut diacungi dua jempol. Walau di dunia nyata kita dianggap sebagai salah satu negara terbelakang, namun prestasi yang sangat gemilang telah berhasil ditorehkan oleh para hacker, cracker dan carder lokal. Undang-undang Informasi dan Transaksi Elektronik atau Undang Undang nomor 11 tahun 2008 atau UU ITE adalah UU yang mengatur tentang informasi serta transaksi elektronik, atau teknologi informasi secara umum. UU ini memiliki yurisdiksi yang berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini, baik yang berada di wilayah Indonesia maupun di luar wilayah hukum Indonesia.
Kata Kunci: Hukum Pidana; Tindak Pidana Cyber; UU ITE

* Received: May 22, 2021, Revision: May 28, 2021, Published: June 5, 2021.
[1] **Sefitrios** adalah Mahasiswa Magister Ilmu Hukum Universitas Jayabaya Jakarta. Email: sefitrios78@gmail.com
[2] **Tofik Yanuar Chandra** adalah Dosen Ilmu Hukum di Universitas Jayabaya Jakarta. Email: tyc.jayabaya@gmail.com

A. INTRODUCTION

The increase in information technology users, specifically internet users, has been significant, and the current trend has even become a requirement. This means that individuals and groups who are unable to adapt to this virtual era will see their survival and development abilities deteriorate. We can see that the current situation will be even strange for someone who does not have a means of communication.

On the one hand, technological developments provide a positive trend toward civilization; however, if they are not properly managed, such as the management of cellular operators, internet service providers, and law enforcement itself, technological developments will be widely used in unlawful acts. In the current virtual era, any crime can be committed, both against information systems (computer crime) and old crimes that will be easier to commit with information technology (computer related crime), and will have a negative impact on people's social lives and even state security. The characteristics of virtual crimes are carried out by anonymous modes that are difficult to detect.

The use of information technology, media, and communication has altered both societal behavior and human civilization on a global scale. The advancement of information and communication technology has also resulted in borderless world relations and the rapid adoption of significant social, economic, and cultural changes.

According to Dan Koeing, cyber crime focuses on the use of computer technology in the commission of crimes, both new and traditional.[3] The term cyber law used in this paper is based on the idea that cyber, if identified with cyberspace, will present enough difficulties in terms of proving and enforcing the law. This is due to the difficulty that law enforcement will face if they have to prove a problem that is assumed to be "virtual," that is, something that is not visible or pseudo.

When compared to other types of traditional crime, cybercrime is a relatively new form of crime (street crime). Cybercrime arose at the same time as the information technology revolution. According to Ronni R. Nitibaskara, another feature of the information technology revolution is social interaction that minimizes physical presence. The deviation of social relations in the form of (cyber) crime will adjust its shape to the new character with this type of interaction."

[3] Franz Magnis-Suseno, *Etika Politik: Prinsip-prinsip Moral Dasar Kenegaraan Modern,* Jakarta: PT Gramedia, 1987.

Cybercrime includes the following types of offenses: First, there is cyber-terrorism. The National Police Agency of Japan (NPA) defines cyber terrorism as electronic attacks on critical infrastructures via computer networks that have the potential to disrupt the nation's social and economic activities. Second, there is cyber-pornography, which is the dissemination of obscene materials such as pornography, indecent exposure, and child pornography. Third, there is cyber-harassment, which is sexual harassment via e-mail, websites, or chat programs. Fourth, cyber-stalking refers to stalking crimes committed using computers and the internet. Fifth, hacking: the use of programming abilities with illegal intent. Sixth, carding (also known as "credit-card fraud") refers to a variety of credit-card-related activities. Carding occurs when someone who does not own a credit card uses it illegally.

The National Police, as one of the pillars of the nation with constitutional authority as law enforcement officers, is obligated to update the organization's capabilities and competencies so that they can actualize the state's presence in preventing, anticipating, and combating virtual crimes (cyber crimes), both computer related crime and computer crime. So that the police force can adapt to the challenges of virtual civilization in the current information age. This implies that the current cyber organizational structure must be evaluated and strengthened in order to adapt to the new civilization. The purpose of the evaluation is to modernize the organization so that it can respond to public challenges by analyzing formalization, centralization, specialization, standardization, complexity, and power hierarchies. So, in order to respond to these conditions, an in-depth study (research) on the development of cybercrime units/units in regional units (Polda and Polres) is required.

The problem of cybercrime has never been addressed in the Criminal Code (KUHP). As a result, in order to fill the legal void, the Law on Electronic Information and Transactions No. 11 of 2008 was enacted in 2008. It is also regulated regarding evidence and evidence against cyber crime in Law No. 11 of 2008 concerning Electronic Information and Transactions. Of course, considering the locus delicti of cyber crime in cyberspace or cyberspace is very different from conventional criminal acts contained in the Criminal Code, where the place where criminal acts occur in the "real world" in an attempt to prove is also very different.[4] How to prove and evidence used in cyber crime cases. How is the relationship between the evidence in the Criminal Procedure Code (KUHAP) and the evidence contained in Law Number 11 of 2008 concerning Information and Electronic Transactions.

[4] Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Based on some literature and empirical facts, cyber crime has several characteristics, namely: a. Acts that are carried out illegally, without rights or unethical occur in cyber space/region (cyber space), so it is not certain which country's jurisdiction applies to them. b. The act is carried out using any equipment that is connected to the internet. c. Acts that result in material and immaterial losses (time, value, services, money, goods, self-esteem, dignity, confidentiality of information) tend to be greater than conventional crimes. d. The perpetrators are people who master the use of the internet and its applications. e. These acts are often carried out transnationally/across national borders.

Law Number 11 of 2008 concerning Information and Electronic Transactions also discusses the violations contained in article 30 that: "Every person intentionally and without rights or against the law accesses computers and/or Electronic Systems: 1) Belongs to other people in any way. 2) With the aim of obtaining Electronic Information and/or Electronic Documents. 3) In any way violate, break through, exceed, or break the security system."

Indonesia's positive law governing online crime (cybercrime) is contained in Law Number 19 of 2016 concerning amendments to Law number 11 of 2008 concerning Information and Electronic Transactions. The crime of fraud committed online is specifically regulated in law number 19 of 2016 concerning amendments to law 11 of 2008 concerning electronic information and transactions, although this ITE Law does not specifically state the existence of a criminal act of fraud, but specifically implicitly there are elements that are almost the same as the criminal act of fraud which is regulated in general in Article 378 of the Criminal Code (KUHP).[5]

B. METHODS

This study is a legal study that connects the existence of existing laws and regulations that have been used as a reference with field practice. The primary research was conducted through a literature review to obtain secondary data on primary, secondary, and tertiary legal materials. Using qualitative analysis methods, data was analyzed on all legal regulations related to the subject matter discussed and argued theoretically based on the concept of criminal law.

In writing this research methodology, the reader is expected to at least get an illustration that can inspire the reader's frame of mind logically by knowing the basic knowledge of theories, methods and approaches that develop in

[5] Maskun. *Kejahatan Siber (Cyber Crime) Suatu Pengantar,* (Jakarta: Kencana Prenada Media Group, 2013).

doctrinal legal science (teachings of science). In addition, they also know the basics of making research proposals, the basics of data collection techniques, data analysis techniques and final report preparation, and as additional knowledge about legal writing guidelines, both mass media and legal news.

C. RESULTS AND DISCUSSION

1. Methods and Proof of Cyber Crimes in Indonesia

Writing, sound, pictures, maps, designs, photographs, electronic data interchange (EDI), electronic mail (electronic mail), telegram, telex, telecopy or the like, letters, processed signs, numbers, access codes, symbols, or perforations that have meaning or can be understood by people who can understand them are examples of electronic information.[6]

The development of the internet can be described as a two-edged sword: on the one hand, it contributes to improved welfare and progress, while on the other hand, it becomes an effective means of committing illegal acts. Online entrepreneurs from other countries can take advantage of this situation to create a target market in Indonesia. Today, cybercrime in the field of electronic information and/or electronic transactions is a major concern, with a global impact.[7]

The ITE Law regulates two large pieces of content, namely the regulation of electronic transactions and cybercrime. The ITE Law is based on the implementation of several international principles, including the UNCITRAL Model Law on Electronic Commerce, the UNCITRAL Model Law on Electronic Signature, the Convention on Cybercrime, the EU Directives on Electronic Commerce, and the EU Directives on Electronic Signature. These provisions are international and regional instruments that are widely used by countries in Europe, America, and Asia.[8]

Pitlo defines proving as "giving certainty to judge about certain events." The six main points that become the measuring tool in proof theory are as follows:[9]

First, consider the evidence's foundation. The basics used to obtain a truth on facts are referred to as the Basis of Evidence. In other words, the content/material of the evidence itself serves as the basis of proof. If the

[6] Pasal 1 ayat 1 Undang-Undang Nomor 11 Tahun 2008

[7] Siwanto Sunarso, *Hukum Informasi dan Transaksi Elektronik,* Jakarta: PT.Asdi Mahasatya, 2009, h.136.

[8] Josua Sitompul, *Cyberspace, Cybercrime Cyberlaw Tinjauan Aspek Hukum Pidana,* Jakarta: Tatanusa, 2012, h.136.

[9] Edmon Makarim, *Kompilasi Hukum Telematika,* Jakarta: PT. Raja Grafindo, 2004.

container is the evidence, then the contents of the container are the basis of the proof.

Second; Evidence Tool. Evidence tools are tools used to describe or explain a criminal situation or event based on facts that occurred in the past for the purposes of criminal proceedings.

Third, evidence tools are decomposed. The methods used to describe an event or situation based on evidence used to commit a crime are referred to as evidence decomposition. The breakdown of evidence is very important in the examination of cases in court, because the judge bases his belief on the evidence.

The fourth point to consider is the importance of evidence. The term "Strength of Evidence" refers to the degree of proof provided by each piece of evidence. In criminal cases, the power of proof usually lies in the facts, where the proof is based on the truth of the facts that the judge has verified.

1. The burden of proof required by law to prove the indictment before a court hearing *(bewijslast).*
2. Minimum evidence required in proof to bind the judge's freedom *(bewijsminimum).*

According to Article 184 paragraph (1) of the Criminal Procedure Code (KUHAP), valid evidence includes: a) witness statements. b) Expert Opinion. Letters c) d) Directions. e) The Defendant's Statement According to paragraph (1) of Article 5 of the Law on Electronic Information and Transactions, electronic information and or printed results of electronic information are legal evidence and have legal consequences. Then, according to Indonesian Procedural Law, paragraph (2) Electronic information and or printed results of electronic information, as referred to in paragraph (1), is an extension of valid evidence.

Article 6 contains provisions in addition to those stipulated in Article 5 paragraph (4), which requires that information be in written or original form. Electronic information and/or electronic documents are considered valid if the information contained within them can be accessed, displayed, guaranteed for its integrity, and accounted for in order to explain a situation.

In criminal justice, proof is an attempt to find the material truth (material waarheid) about a crime and it is clear who the perpetrator is. For this reason, law enforcement officers at the investigation, prosecution, and trial levels are trying to go back in time to reconstruct the series of events and find the perpetrators. All of this was done based on legal facts embedded in the memories of witnesses, written in documents, concluded based on expert

testimony, acknowledged by the perpetrators. These legal facts can also be an integral part of the evidence.[10]

In general, cybercrime is divided into two categories: crimes that use information technology (IT) as a facility, and crimes that target IT systems and facilities. According to Law No. 16 of 2016 on Information and Electronic Transactions (UU ITE). Electronic or digital evidence is now admissible in court under Indonesian law. The ITE Law expands on the provisions of Article 184 of the Criminal Procedure Code regarding legal evidence in the criminal case of the Criminal Procedure Code.

The negative evidence system according to the law (negative wettelijk stelsel) has the following purposes:[11]

1. To blame a defendant (accused) requires a minimum of evidence, which is stipulated by law.
2. However, even if the evidence accumulates, exceeding the minimum stipulated in the law, if the judge does not believe in the guilt of the accused, he cannot blame and punish the accused.

The Criminal Procedure Code regulates in a limited manner the evidence, namely: witness statements, expert statements, letters, instructions and statements of the defendant. All evidence is declared valid if it meets the formal and material requirements. The provisions and requirements regarding the evidence regulated in the Criminal Procedure Code as described above are intended so that the evidence submitted in court is valid evidence so that it can be used in court.

Proof is a matter that plays a role in the trial process, with this proof the fate of the defendant is determined. The process of proving in cyber crime cases is basically no different from proving in conventional criminal cases, but in cyber crime cases there are several things that are electronic which are the main thing in proof, regulated in article 5 paragraph (1) and (2) Law Number 19 of 2016 that Electronic Information and Documents (UU ITE) are considered as valid evidence in the evidentiary process and matters relating to legal actions carried out by the Electronic System in cyber crime cases).[12]

2. Policies for Countering Cybercriminal Behavior in Indonesia

The enactment of Republic of Indonesia Law Number 11 of 2008 concerning information and electronic transactions is a form and responsibility

[10] Josua Sitompul., h. 264-265.

[11] R. Subekti, *Hukum Pembuktian,* Jakarta: Pradnya Paramita, 2010, h. 7.

[12] Anis Dewi Lestari; Meliana Damayanti; *Cakupan Alat Bukti sebagai Upaya Pemberantasan Kejahatan Siber (Cyber Crime)*, JURNAL ILMU SYARI'AH DAN HUKUM., Vol. 3, Nomor 1, h.201.

that the state must carry out in order to provide maximum protection to all activities in the country that use all information and communication technology, so that they are well protected from potential crimes and misuse of technology.

Information technology is used by a variety of institutions, including industry, health care, financial institutions, educational institutions, and government agencies. Information and communication technology has been used in people's social lives, as well as in the government, business, banking, education, health, and personal life sectors.[13]

Cybercrime, even if it takes place in another world in the form of communication media and computers, has a very real impact. Cyber crime prevention policies based on criminal law include a penal policy as part of the criminal policy (crime prevention policy). From the standpoint of criminal policy, crime prevention efforts (including combating cybercrime) cannot be carried out solely through criminal law (penal means), but must also be approached holistically.[14]

According to Bassiouni, the decision to criminalize and be criminalized must be based on certain policy factors that take into account a variety of factors, including: first, the balance of the means used in relation to the desired results. Second, a cost-benefit analysis of the results obtained in relation to the goals sought. Third, conduct research or interpret the goals sought in relation to other priorities in human resource allocation. Fourth, the social impact of criminalization and decriminalization in relation to or as a result of their secondary effects.[15]

So far, the following criminalization policies or criminal law formulations in Indonesia have been identified in relation to cyber crime problems: First, in the Criminal Code, the formulation of criminal acts is mostly still traditional and has not been directly linked to the development of cyber crime. Furthermore, there are numerous weaknesses and limitations in dealing with technological developments and high-tech crime. For example, in terms of dealing with credit card counterfeiting and electronic fund transfers, the Criminal Code has difficulties because there are no special rules regarding these matters. The existing provisions only concern: (a) oath/false statement (Article 242); (b) counterfeiting currency and banknotes (Articles 244-252); (c)

[13] Reza Hikmatulloh; Evy Nurmiat; *Analisis Strategi Pencegahan Cybercrime Berdasarkan UU ITE Di Indonesia (Studi Kasus: Penipuan Pelanggan Gojek)*, Vol. 20 No. 2 (2020).

[14] Barda Nawawi Arief, *Pembaharuan Hukum Pidana dalam Perspektif Kajian Perbandingan,* Bandung: Citra Aditya Bakti, 2005, h.125.

[15] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana,* Bandung: Citra Aditya Bakti, 2002, h.32.

counterfeiting stamps and marks (Articles 253-262); and (d) falsification of letters (Articles 263-276).

Second, laws outside the Criminal Code include: a) Law Number 36 Year 1999 concerning Telecommunications, threatening criminal acts against: (1) manipulating access to telecommunications networks (Article 50 jo.22); (2) cause physical and electromagnetic disturbances to telecommunications operations (Article 55 jo.38); (3) intercepting information through telecommunications networks (Article 56 jo.40). b) Article 26A of Law Number 20 of 2001 concerning Amendments to Law Number 31 of 1999 concerning Eradication of Criminal Acts of Corruption; Article 38 of Law Number 15 of 2002 concerning the Crime of Money Laundering; and Article 44 paragraph (2) of Law Number 30 of 2002 concerning the Corruption Eradication Commission; recognize electronic records as valid evidence. c) Law Number 32 of 2002 concerning Broadcasting. d) Law Number 11 of 2008 concerning Information and Electronic Transactions (UU-ITE).

Chapter VII Prohibited actions contain criminal provisions for any person who intentionally and without rights or against the law distributes and/or transmits and/or makes electronic information and/or electronic documents accessible with the following contents: (1) Violating decency; have a gambling charge; contains insults and/or defamation; has a charge of extortion and/or threats (Article 27). (2) Spreading false and misleading news that results in consumer losses in electronic transactions; Disseminate information aimed at creating feelings of hatred or hostility towards certain individuals and/or groups of people based on ethnicity, religion, race, and inter-group (SARA) (Article 28). (3) Sending information that contains threats of violence or intimidation aimed at personally (Article 29). (4) Accessing other people's computers and/or electronic systems; access computers and/or electronic systems with the aim of obtaining electronic information and/or electronic documents; accessing computers and/or electronic systems by violating, breaking through, exceeding, or breaking into the security system (Article 30). (5) Interception or wiretapping of electronic information and/or electronic documents; conduct electronic interception of the transmission of electronic information and/or electronic documents that are not public (Article 31). (6) Changing, adding, reducing, transmitting, destroying, removing, transferring, hiding, electronic information and/or electronic documents belonging to others or to the public; move or transfer electronic information and/or electronic documents to the electronic system of another person who is not entitled; resulting in the disclosure of electronic information and/or electronic documents that are confidential in nature to be accessible to the public with improper data integrity (Article 32). (7) Disruption of the electronic system

and/or resulting in the electronic system not working properly (Article 33). (8) Producing, selling, procuring for use, importing, distributing, providing, or possessing (a) hardware or software designed or specially developed to facilitate acts as referred to in Articles 27-33; (b) computer passwords, access codes, or other similar things intended to make the electronic system accessible for the purpose of facilitating the actions in Articles 27-33 (Article 34). (9) Manipulating, creating, changing, deleting, destroying electronic information and/or electronic documents with the aim that the electronic information and/or electronic documents are considered as if they were authentic data (Article 35). (10) Performing the acts as referred to in Article 27-34 that result in harm to other people (Article 36). (11) 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).

According to Article 42 of the ITE Law, investigations into criminal acts as defined in this law are conducted in accordance with the provisions of the criminal procedure law as well as the provisions of this law. This means that all provisions of the Criminal Procedure Code and other laws relating to criminal procedural law apply in the context of investigations aimed at uncovering criminal acts committed in cyberspace.

Search and/or confiscation of electronic systems related to alleged criminal acts must be carried out with the permission of the Head of the local District Court. In conducting searches and/or confiscations, investigators are obliged to maintain the maintenance of the interests of public services. In making arrests and detentions, investigators through the public prosecutor are required to request a determination from the Head of the local District Court within twenty-four hours.

Indonesia itself is not included in the top row in the list of countries that are victims of cybercrime, but is the country of origin where cybercrime is carried out.[16] According to Barda Nawawi Arief, cyber crime prevention efforts can be viewed from a variety of perspectives, including aspects of criminalization policy (formulation of criminal acts), aspects of criminal responsibility or punishment (including aspects of evidence and evidence), and aspects of jurisdiction.[17]

Cybercrime occurs as a result of a lack of personal and social control. This is due to the fact that the perpetrator is not physically present. According to the normative approach, cyber crimes are traditional crimes with new modes,

[16] Dewi Bunga. *Politik Hukum Pidana Terhadap Penanggulangan Cybercrime,* Vol 16 No.1 - Maret 2019, h. 1-15.

[17] Barda Nawawi Arief. *Pembaharuan Hukum Pidana dalam Perspektif Kajian Perbandingan,* Bandung: Pranamedia Group, 2005 , h. 125.

such as pornography, fraud, defamation, and so on, that use the internet as a means to commit crimes, and they can be punished by referring to the provisions stated in the Indonesian Law, Act of Criminal Law (KUHP). Meanwhile, for new types of cybercrime such as hacking, there is no provision for this crime in the Criminal Code. Thus there is a legal vacuum *(rechts vacuum).* Some of the cases include: First, Defacing; Second, Phishing; Third, Pornography; Fourth, Defamation Cases; Fifth, Hacking State Sites.

D. CONCLUSIONS

1. It should be noted that valid evidence (article 184 paragraph (1) of the Criminal Procedure Code) is: Witness Statements, Expert Statements, Letters, Instructions; and the Defendant's Statement. In order to be punished, the perpetrator of defamation must be considered to have committed an act by accusing someone of having committed a certain act with the intention that the accusation will be broadcast (known to many people). Unlike in the case of written defamation, where the media used to carry out defamation can be in the form of writing (letters) or pictures, the media used in carrying out defamation cannot be in the form of writing (letters) or pictures (Print Screen). Print screens of words or sentences from social media can be used as valid evidence in court as long as the evidence's authenticity is technically justifiable. In addition to the search for evidence, the investigator faces internal and external obstacles to finding evidence in the crime of defamation.
2. Cyber crime prevention policies are part of the criminal policy. The enforcement of criminal law is highly dependent on the development of legal politics, criminal politics, and social politics.

REFERENCES:

A, M. Yustia. Pembuktian dalam Hukum Pidana Indonesia terhadap Cyber Crime., PRANATA HUKUM Volume 5 Nomor 2 - Juli 2010

Arief, Barda Nawawi. Bunga Rampai Kebijakan Hukum Pidana, Citra Aditya Bakti, Bandung, 2002.

Arief, Barda Nawawi. Pembaharuan Hukum Pidana dalam Perspektif Kajian Perbandingan, Citra Aditya Bakti, Bandung, 2005.

Bunga, Dewi. Politik Hukum Pidana Terhadap Penanggulangan Cybercrime., Vol 16 No.1 - Maret 2019 : 1-15.

Hikmatulloh, Reza; Nurmiat, Evy. Analisis Strategi Pencegahan Cybercrime Berdasarkan UU ITE Di Indonesia (Studi Kasus: Penipuan Pelanggan Gojek)., Vol. 20 No. 2 (2020).

Lestari, Anis Dewi; Damayanti, Meliana. *"Cakupan Alat Bukti sebagai Upaya Pemberantasan Kejahatan Siber (Cyber Crime),"* JURNAL ILMU SYARI'AH DAN HUKUM., Vol. 3, Nomor 1, 201.

Makarim, Edmon. Kompilasi Hukum Telematika, PT. Raja Grafindo. Jakarta, 2004.

Maskun. (2013). Kejahatan Siber (Cyber Crime) Suatu Pengantar, (Jakarta: Kencana Prenada Media Group

Mukri, S.G.; Aji, A.M.; Yunus, N.R. (2016). "Implementation of Religious Education in the Constitution of the Republic of Indonesia," Salam: Sosial dan Budaya Syar-i, Volume 3 No. 3.

Mukri, S.G.; Aji, A.M.; Yunus, N.R. (2017). Relation of Religion, Economy, and Constitution In The Structure of State Life, STAATSRECHT: Indonesian Constitutional Law Journal, Volume 1, No. 1.

Sitompul, Josua. Cyberspace, Cybercrime Cyberlaw Tinjauan Aspek Hukum Pidana, Tatanusa, Jakarta, 2012.

Subekti, R. Hukum Pembuktian, Pradnya Paramita, Jakarta, 2010

Sunarso, Siwanto. Hukum Informasi dan Transaksi Elektronik, PT. Asdi Mahasatya, Jakarta 2009

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

W.S, Ervina Lerry; Iman; dan Stella K, R. The World of Cyber Crime: Carding, Bheta Versions, IKI-40000.

Yunus, N.R.; Anggraeni, RR Dewi.; Rezki, Annissa. (2019). "The Application of Legal Policy Theory and its relationship with Rechtsidee Theory to realize Welfare State," 'Adalah, Volume 3, No. 1.