

# The Use of Electronic Information and Transaction Law as a Police Social Engineering Tool to Maintain Homeland Security Stability from Hoaxes

Wira Prayatna<sup>1\*</sup>, Alvi Syahrin<sup>2</sup>, Edmon Makarim<sup>3</sup>

<sup>1, 2</sup> Faculty of Law, Universitas Sumatera Utara

<sup>3</sup> Faculty of Law, Universitas Indonesia

Email: [pol.wiraprayatna@gmail.com](mailto:pol.wiraprayatna@gmail.com)

## ABSTRACT

With the development of the use of the Information and Electronic Transactions Law today, there are various kinds of news that are not true circulating very quickly and rapidly which corners the government. In fact, these reports are hoaxes made by outside parties (foreign countries) to threaten the stability of domestic security in Indonesia and can trigger divisions between tribes, religions, and races. The act that threatens the stability of the Home Affairs Ministry, history records, Nazi Germany used the politics of "Propaganda" to rule the world. The politics of "Propaganda" is untrue news that is continuously reported to produce the truth desired by the German authorities at that time. This is what is assumed to be done by outside parties (foreign countries) as irresponsible parties, so that it can damage the order of life of the nation and one homeland, Indonesia. As the constitutional order created by the "founding fathers" as the Founding Fathers of the Nation, nationalism, and the Unitary State of the Republic of Indonesia. The ITE Law can be a social engineering tool to defend, dispel, and punish perpetrators who make fake news (hoax) on social media. Social engineering aims to protect the divisions between Tribes, Religions, and Races (SARA) to create the goal of state life, namely: "Social justice for all Indonesian people". The idea and idea of this research are that the Electronic Transaction Information Law can be used as a resistance for the Government to "counter" hoax attacks from outside parties that threaten the stability of the Home Affairs Ministry, which does not want peace in Indonesia to be well maintained.

**Keywords:** Social Engineering, Homeland Security, Hoax.

## 1. INTRODUCTION

### 1.1. Background

Roscoe Pound once said "law as a tool of social engineering", meaning: "Law as a tool of social engineering".[1] Associated with this research plan, Law no. 11 of 2008 concerning Information and Electronic Transactions as amended by Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Information and Electronic Transactions (hereinafter referred to as the Law on Information and Electronic Transactions) is a tool to carry out social engineering.

The development of globalization that occurs in people's lives causes many changes that occur in society. This can be viewed from the side of science and communication technology. Advances in science and communication technology have made human relations no longer limited only because of space, time, and place

and no single country can hinder the process of globalization [ 2 ] The real manifestation of the development of technology and communication can be felt by many people, one of which is the internet. Internet or interconnection networking is one of the media that has developed due to globalization. With the internet, people can access information from various servers around the world. The internet can also be a medium of communication between internet users in parts of the world directly or indirectly.

According to the e-Marketer market research institute, the population of internet users in Indonesia reached 83.7 million people in 2014. The figure that applies to everyone who accesses the internet at least once a month ranks Indonesia as the 6th largest in the world in terms of the number of internet users. In 2017, eMarketer estimates that internet users in Indonesia will reach 112 million people, beating Japan in 5th place, which has slower growth in the number of internet users.[3] In the

context of social media users in the world, it is reported that it has reached 4.2 billion by January 2021. This figure has grown by 13% with the number of new users reaching 490 million over the last 12 months. That's an average of more than 1.3 million new users on social media every day during 2020, or about 155,000 new users every second.[4]

For Miles Townes, as a technology, the internet contains norms. This can be understood if, as Townes understands, technology is seen as a form of "knowledge how," which can simply be interpreted as a set of knowledge that shows how something is used, done, and completed for a particular purpose.[5]

Based on this definition, it means that politically the internet has consequences for shaping behavior and by itself has a direction on how humans, as technology users, are conditioned to make decisions, exercise control over their own behavior and the behavior of others, as well as relate to others using a framework or design. certain. How an organization coordinates will be very different when instant messaging services develop in the cellular telephone network, and even more different when humans are introduced to instant messaging services where text, images, sounds, and snippets of what people are capturing at any one time can easily be seen. channeled through the device (gadget) he has.[6]

Currently, the dissemination of information or news through online media is not only carried out by news sites that are already known to the public, but by anyone who uses the internet can play a role in the dissemination of information. Unfortunately, there is a lot of information or news that is spread individually or in groups that cannot be justified or are indicated as a hoax. Hoax is information or news that contains things that are not certain or which really are not facts that happened. Now information or news that is considered true is no longer easy to find. The Mastel survey (2017) revealed that of 1,146 respondents, 44.3% of them received hoax news every day and 17.2% received it more than once a day. Even mainstream media that are relied on as trustworthy media are sometimes contaminated with the spread of hoaxes. Mainstream media is also a channel for disseminating hoax information/news, each at 1.20% (radio), 5% (print media) and 8.70% (television).[7]

Not only by mainstream media, but hoaxes are also now circulating in the community through online media. The results of research conducted by Mastel (2017) state that the channels that are widely used in the spread of hoaxes are websites, at 34.90%, chat applications (Whatsapp, Line, Telegram) at 62.80%, and through social media (Facebook, Twitter, Instagram, and Path) which are the most used media, reaching 92.40%. Meanwhile, data presented by the Ministry of Communication and Information said there were as many as 800,000 sites in Indonesia indicated as spreading hoaxes and hate speech.[8]

The spread of negative content such as hoaxes, blasphemy, propaganda, and agitation has been used to

disrupt security, political stability, and the existence of the state both from within and outside the country. The spread of negative content with political motives is included in the realm of information war/cyberwar. So this action is outside the context of ordinary crime (cybercrime). The use of information technology with negative content like this has basically become a medium for organizing war with asymmetric dimensions (asymmetric war) by carrying out proxy war attacks (wars that use third parties).[9]

President Joko Widodo himself stated that hoaxes are part of the era of openness that must be faced. The President asked all parties to stop the spread of hoaxes and slander that can divide the nation, especially those circulating through social media.[ 10 ] Meanwhile, Coordinating Minister for Political, Legal, and Security Affairs, Wiranto said that the public will be harmed by a large number of unclear news distributions, among which, with doubts about all information received, the public becomes confused. This public confusion can be used by irresponsible parties to instill hatred so that there is a chance for division and hostility to occur.[11]

The progress and variety of communication media owned by the community cause the community and the state to face the effects of hoaxes as a result of communication jammed that occurs in the community. Communication jammed is caused by the development of communication technology that can no longer be controlled. Communication traffic is very complicated, causing hoax news as an act of simple social construction, but being the enemy of society and the state, it is easy to emerge.[12]

Situngkir (2017) researched hoaxes with the title "Spread of Hoax in Social Media".[ 13 ] This study discusses how to spread hoaxes as gossip and rumors on Twitter, by observing empirical cases in Indonesia. This study also discusses the factors of spreading gossip on social media and looks at the epidemiology of hoax propagation before and after hoaxes are clarified in conventional mass media. The results of the study concluded that Twitter, as a microblogging service, is one of the effective media for spreading news from person to person at a speed comparable to conventional mass media. Hoaxes have a large population coverage in five to six tweets, and potentially exponentially larger unless conventional media stops the spread of the hoax.

Allcott and Gentzkow (2017) also conducted a study entitled "Social Media and Fake News in the 2016 Election".[14] This study concludes that social media platforms such as Facebook have a very different structure from previous media technologies (mainstream media). Content on social media can be shared between users without third-party screening, fact-checking, or editorial judgment. The average US adult reads and remembers a sequence of one or more fake news articles during an election term, with higher exposure to pro-Trump articles than to pro-Clinton articles. How much impact these election results have will depend on the

effectiveness of exposure to hoaxes in changing the way people vote.

"Government Policy to Prevent the Spread of Fake News or Hoaxes", is the title of a study also conducted by Siswoko (2017).[ 15 ] The research method used is observation and content analysis of news coverage in Kompas and The Jakarta Post. The results of the study concluded that the government took other steps beyond blocking sites to anticipate the spread of hoax news. The steps in question are to establish a National Cyber Agency and cooperate with the Press Council and Facebook.

The studies described above mostly reveal about social media that has the potential to spread hoaxes. Also about hoax content that continues to be repeated through social media will have an impact on changing people's opinions and choices, especially in the case of the presidential election. Meanwhile, this study discusses comprehensively the use of the Electronic Information and Transaction Law as a social engineering tool to maintain the stability of domestic security by the National Police from fake news (hoax). Such research has never been done before, so it is important to do it.

## 1.2. Problem

Based on the above background, the problems in this research plan can be formulated as follows: How is the use of the Information and Electronic Transaction Law as a social engineering tool by the National Police to maintain the stability of domestic security in Indonesia from hoax news?

The purpose of this research plan is to get an overview of hoaxes on social media and to examine and analyze descriptively the use of the Information and Electronic Transaction Law as a social engineering tool by the National Police to maintain the stability of the Home Affairs Ministry in Indonesia from these hoax news.

## 2. METHODS

This writing uses qualitative research methods with a literature approach and is based on theories in understanding the role of cybersecurity in overcoming fake news (hoaxes) in realizing domestic security stability. With this research method, it is expected to generate ideas as the outcome of data processing and analysis by emphasizing the quality aspects of data sources. The qualitative method is a research process that produces descriptive, spoken, or written data or observable behavior from the people themselves.[16]

## 3. RESEARCH RESULTS AND DISCUSSION

### 3.1. Homeland Security Stability

As mandated in the fourth paragraph of the Preamble to the 1945 Constitution of the Republic of Indonesia that the Unitary State of the Republic of Indonesia was established with national objectives including: "protecting the entire Indonesian nation and the entire homeland of Indonesia, advancing public welfare, educating the nation's life and participating in carrying out world order based on independence, eternal peace, and social justice." [17]

New paradigms of democratization, human rights, the environment, and the free market have been used as norms and standards in international relations. This requires careful and measurable adjustments so that the Indonesian nation still exists, is sovereign, and respectable. Meanwhile, advances in science and technology have also triggered changes in the pattern of modern life that are more rational and individualistic. As a result, the spectrum of security threats is getting wider, not only from inside or outside but also global in nature. In line with that, the types and forms of threats have also shifted to become multi-dimensional, no longer leading to mere military threats, but to culture, economy, politics, as well as defense and security. The types and forms of domestic threats currently include poverty, public health problems, epidemics and pandemics, natural disasters, social unrest, inter-group conflicts, crimes, rebellions to armed separatist movements.[18]

Efforts to realize national security stability can no longer stand-alone, meaning that defining the concept of national security cannot only be limited to traditional meanings that are only oriented to state defense and security tools. However, national security must be seen as an integral part of various aspects of the life of the nation and state, namely ideology, politics, economy, social, culture, defense, and state security. In this case, national security has developed to include national defense, state security, security of public order, and human security.[19]

To achieve stability in the security sector so that it can support national economic growth, the government, in this case, the Coordinating Ministry for Political, Legal and Security Affairs, Ministry of Defense, Ministry of Home Affairs, Ministry of Foreign Affairs, Commander of the Indonesian National Armed Forces, National Police Chief and the State Intelligence Agency need to take policies, including: First, "Optimizing the use of defense and security forces that are directed at dealing with threats and disturbances to national security, as well as assisting the implementation of national development in a programmed, integrated and synergistic manner among relevant stakeholders. Second, revitalizing forms of international cooperation in the field of defense and security, which is one of the bridges to build confidence-building measures with other nations for the realization of regional security stability. Third, increasing the development of defense and security forces which not only have a deterrent effect but can also guarantee the protection of national interests".[20]

Indonesia as a developing country must develop the strength and ability to face various challenges of global

development which at any time can cause national security to be unfavorable. From the era of the proclamation of Indonesian independence until now, the Indonesian government along with all other components of the nation based on existing laws have made efforts to maintain national security stability from various threats faced. During the Reformation Era, various products of the Law on Security as the elaboration of Article 26, Article 27, and Article 30 of the 1945 Constitution of the Republic of Indonesia were used as the basis for the implementation of national security. Based on the existing laws and regulations, no clause expressly states the existence of binding cooperation and coordination between actors implementing national security. On the other hand, other Institutions/Departments based on the elaboration of Article 31 paragraph (5), Article 32, Article 33 paragraph (2), paragraph (3), paragraph (4) and Article 34 paragraph (2), paragraph (3) still prioritize the management of aspects of welfare, have not enabled him to participate in realizing national security stability by their respective fields of facing the existing threats.

The above conditions have created various weaknesses in coordination and synergy between actors as well as sectoral pride and community awareness. Faced with demands, developments in threats, and developments in the strategic environment, the implementation of national security by existing components requires adjustments and improvements to software and hardware for the preparation of a comprehensive national security system. To create a conducive and comprehensive national security, it is not only the responsibility of the Indonesian National Army and the Indonesian National Police as the main force but also to involve all relevant government agencies and community participation as mandated in the 1945 Constitution of the Republic of Indonesia.

### **3.2. Internet as a Technology and its Regulation**

As Miles Townes has quoted above, the content of norms identified by Townes shows that the basic direction of the development of the internet is the idea of academic freedom. In short, it was this academic norm that allowed the internet to form from its inception. At first, this initiative to develop computer network technology developed from the need for the United States and its allied countries to coordinate during the Cold War. This need then makes the United States and its allies facilitate meetings between academics and computer experts to build knowledge and technology that allows them to share data quickly to support policymaking and decision-making more quickly and effectively.

This meeting of academics then created a space characterized by the doctrine of freedom – which of course is one of the principles that make up the academic space – which was then embedded in the internet technology they developed. In the United States itself, this space was initially made possible by the creation of a research platform initiated by the Department of Defense. However, beyond the tightness that is usually

attached to security institutions, the technology founders involved in this research believe that the responsibility for security and maintenance of internet technology should not be in the hands of a network node or even a centralized institution, but should be in the hands of each computer users.[21]

Based on the table above, the discipline most related to the internet is Cyberlaw. Because in every mapping of scientific areas there are legal disciplines, especially in this context Cyberlaw. Therefore, Cyberlaw at this time is very appropriate and worth exploring.

This belief forms the principle that underlies the dissemination of this technology for use by the wider public. The beliefs of the founders of the internet later shaped the character of the internet as a technology which, although initiated by the public sector, was more developed as a private tool and tool. This is reflected in the character of TCP/IP (Transmission Control Protocol/Internet Protocol) which is the core of internet technology. TCP is a protocol that regulates interactions between computers (or host-to-host), while IP is a protocol that regulates interactions between networks (networks).

The character of the internet makes internet regulation a complicated thing and until now there has not been found a standard or global consensus. This complexity relates to the many parties involved, from the government, the private sector, and civil society, with all the rules – including values, principles, and applications – that govern the internet. In addition, it should be noted that the regulation of the internet in general means not only the regulation of its use, but also the regulation so that the evolution of the internet is still possible. These two things are reflected in the definition of internet governance offered by The United Nations Working Group on Internet Governance.[22]

Meanwhile, academically, internet regulation is something that intersects with many disciplines. At least there are rubrics in internet regulation that emerge from academic studies, namely: internet governance, telecommunications policy, information security economics, and cyber law.[23] This interdisciplinary condition means that internet management will always attract the attention of various experts from different disciplines including communication, computer science, economics, information engineering, law, politics, and economics. Thus, the nature of internet regulation is multidimensional and complex. This is reflected in the table above about the mapping of the internet regulatory area made by van Eeten and Mueller.

### **3.3. Internet Regulation Ideas in Indonesia**

The Law on Information and Electronic Transactions was formed through a long process that occurred along with the development of information technology, especially the use of the internet in Indonesia. A comprehensive understanding of the various developments and reasons driving the establishment of this Law is important to see what is the basis and main

objective (original intent) for the establishment of the Electronic Information and Transactions Law. From that footing, it can then be analyzed whether the Information and Electronic Transaction Law has fulfilled the needs and main objectives of the enactment of the Law.

The main issue is whether the Information and Electronic Transaction Law can be placed as cyberlaw that regulates all forms of activity in cyberspace. The focus and the details of the problem that mostly discuss the regulation of electronic transactions should encourage Indonesia to have more than one law to regulate all activities in cyberspace. However, until now, the Information and Electronic Transaction Law is still placed by policymakers as the only cyber law in Indonesia. Thus, many issues have not been clearly and precisely designed to be included in the law (cyberspace).

According to Jovan Kurbalija, in general, there are two approaches to internet regulation in various countries. The first approach is called the 'old-real approach', which says that the internet does not provide any particular novelty to how government works. The Internet is considered only as a new tool that is no different in function from the earlier tools (eg telegram, telephone, and radio). The main consequence of this approach is that existing laws apply to the internet, and require only minor adjustments.[ 24 ] The second approach is the 'new cyber approach', which says that the internet is fundamentally a new form of the communication system that is different from other communication systems. This approach sees cyberspace as different from the real world and therefore requires a different form of regulation. In other words, this second approach requires new laws for the internet.[25]

These two different points of view can be used as a reference to understand what approach Indonesia used in establishing the Electronic Information and Transaction Law. To assess this, it is necessary to look at cases related to the Electronic Information and Transaction Law in its implementation since 2008.

Until 2008, Indonesia did not have a reference in the law related to information technology. However, discussions to formulate the law actually took place more or less than 2001.[26] Thus, the ratification of the ITE Law in 2008 could be said to be very late. Especially because internet penetration has started to enter Indonesia since the late 1980s. In 2000 users of ISP (Internet Service Provider) services have reached 1.5 million people.[27] Based on a survey by Association of Indonesian Internet Service Providers, Indonesia's internet penetration in 2005 reached 7.8% with 16 million users.[28]

The delay in launching the cyber law was largely due to various debates and the slow legislative process. Discussion on the academic text of the Draft Law on Information and Electronic Transactions has been going on since 2002. Seriousness in the process of pursuing this law has only occurred since the issuance of a letter from President Susilo Bambang Yudhoyono to the DPR on September 22, 2005, for the formation of the law. The development of the digital world goes hand in hand with

the development of businesses that use internet services as infrastructure. But at a time when other countries have moved to ease of doing business through the digital world, Indonesia is a step behind. Existing laws and legislation are inadequate in regulating business via the internet or e-commerce.[29]

Thus, the beginning of Draft Law on Information and Electronic Transactions was passed into the Law on Information and Electronic Transactions, as a guardian of the public in conducting electronic transactions by internet users in cyberspace. However, over time it turns out that the development of internet users in the world affects the stability of a country's domestic security.

### ***3.4. The Role of the Police in Using the Electronic Information and Transaction Law as a Social Engineering Tool to Maintain the Stability of Indonesia's Homeland Security from Fake News (Hoax)***

The National Police of the Republic of Indonesia has the authority to overcome and overcome the spread of fake news through online media based on Law No. 2 of 2002 concerning the National Police of the Republic of Indonesia, the main tasks and authorities of the National Police are: To maintain public security and order; Enforce the law, and provide protection, protection, and service to the community.

In the process of investigating the criminal act of spreading fake news through social media, the Indonesian National Police carry out law enforcement starting from investigation and investigation until the handover of suspects and evidence to the prosecutor's office. the investigation, so that investigators must take down (closure of accounts) by sending a letter to the Ministry of Communication and Information.

One of how the Police handle fake news cases is by taking down (closing accounts) social media, while if you look at the Police Law and the Information and Electronic Transactions Law, it is not stated that the police have the authority to take down social media accounts. The Police in Article 42 of the Information and Electronic Transactions Law states that the police are authorized as investigators and in Article 1 paragraph (1) of the Criminal Procedure Code which states the authority of the Police, that Investigators are state police officers of the Republic of Indonesia or certain civil servants who given special authority by law to conduct investigations.

Investigators and investigators as referred to in Article 6 paragraph (1) letter a have the authority to carry out their respective duties in general throughout the territory of Indonesia, especially in their respective jurisdictions where they are appointed by the provisions of the law. In Chapter X regarding investigations in Article 43 paragraph (1) of the Electronic Information and Transactions Law, that apart from Investigating State Police Officers of the Republic of Indonesia, certain Civil Service Officials in the Government environment whose scope of duties and responsibilities are in the field of Information Technology and Electronic Transactions are

given special authority. as an investigator as referred to in the Law on criminal procedural law to conduct criminal investigations in the field of Technology and Electronic Transactions.

Many things can be done by the police to tackle the spread of fake news, one of which is by conducting socialization with the community and increasing public understanding of fake news and also about the application of anti-fake news so that people understand very well how the public should be able to report directly to the police regarding accounts. fake news spreader. Indeed, the government has created the hoax tracking device, but if you look at the facts, this has not been realized properly. Many people do not understand and understand how to report provocative accounts and content to the authorities, so that fake news is still widely circulated on social media and becomes public consumption every day, and as it is known that hoaxes are still increasing every day. year, especially in election years, if it is not handled properly by the police.

Based on the above, it is necessary to make changes in each element. Not only from the legislation and law enforcement, but also from the community side. A perfect regulation will not work well without good legal awareness from the community. As users of social media, of course, people are indirect victims and also perpetrators of spreading fake news. The existing legal system has been running quite well, but it is still not enough to keep up with the increasingly rapid developments of the times. Various modes of crime will emerge every day and alertness from the police is needed and continuous infrastructure improvement, it is very difficult to limit content containing fake news (hoaxes) circulating on social media, therefore emphasizing the role of the police as well as the government to continue educating the public so that they can sort out content and use the internet wisely. Providing education about positive internet to the public will no longer be a place for the perpetrators of spreading fake news to spread fake news (hoax) or issues that can divide the Unitary Republic of Indonesia. In fact, fake news also thrives and develops rapidly due to a lack of understanding from the public.

In carrying out prevention, the government has the authority to terminate access and instruct the electronic system operator to cut off access to information or documents held in violation of the law. The government has issued many laws to tackle the spread of fake news, but the number of fake news continues to increase and is unstoppable so that the government and law enforcement officers must have other initiatives in tackling the spread of fake news.

In the application of sanctions for fake news spreaders, it is also still ineffective because there are still many obstacles that law enforcement officials have, in investigating the perpetrators of fake news spreaders because of the lack of personnel in conducting online investigations and a large number of anonymous accounts (fake accounts) which after spreading fake news than the perpetrators of spreading fake news. the fake

news closed his account, then also because the state as the provider of social media did not consider the spread of fake news a crime and could not be asked for data on the social media user. Hasn't basically the government issued the Electronic Information and Transaction Law to ensnare the perpetrators of spreading fake news to eradicate the spread of fake news that can lead public opinion to negative things so that it can cause animosity between Tribes, Religions, and Races (SARA) which can lead to instability. Homeland Security.

## 4. CONCLUSIONS

The use of the ITE Law as a social engineering tool to maintain the stability of the Kamdagri by the National Police from fake news (hoax) is to close accounts. The Law on Information and Electronic Transactions can be used as resistance for the Government to "counter" hoax attacks from outside parties that threaten the stability of the Home Affairs Ministry, which does not want peace in the motherland of Indonesia to be well maintained.

The role of the police and the government is needed to continue educating the public so that they can sort out content and use the internet wisely. Providing education about positive internet to the public will no longer be a place for the perpetrators of spreading fake news to spread fake news (hoax) or issues that can divide the Unitary Republic of Indonesia. In fact, fake news also thrives and develops rapidly due to a lack of understanding from the public

## REFERENCES

- [1] Roscoe Pound in Matnuh, Harpani., "Law as a Tool of Social Engineering", *Advances in Social Science, Education and Humanities Research (ASSEHR)*, Vol. 147, 1<sup>st</sup> International Conference on Social Sciences Education: Multicultural Transformation in Education, Social Sciences and Wetland Environment (ICSSE 2017), Atlantis Press, 2018, p. 118-120.
- [2] Musa, M.I., "Dampak pengaruh globalisasi bagi kehidupan bangsa Indonesia", *Jurnal Pesona Dasar* Vol. 3, 3, (2015).
- [3] Website Resmi Kominfo.go.id., "Pengguna Internet Indonesia Nomor Enam Dunia", [https://kominfo.go.id/content/detail/4286/pengguna-internet-indonesia-nomor-enam-dunia/0/sorotan\\_media.](https://kominfo.go.id/content/detail/4286/pengguna-internet-indonesia-nomor-enam-dunia/0/sorotan_media.), diakses Kamis, 04 Maret 2021.
- [4] Jemadu, L., and Prastyo, D., in Berita Online Suara.com., "Selama 2020, Jumlah Pengguna Media Sosial di Dunia Tembus 4,2 Miliar", <https://www.suara.com/teknologi/2021/02/02/222926/selama-2020-jumlah-pengguna-media-sosial-di-dunia-tembus-42-miliar.>, diakses Kamis, 04 Maret 2021.

- 
- [5] Townes, M., “The Spread of TCP/IP: How the Internet Became the Internet”, *Millenium: Journal of International Studies*, Vol. 41 (1), (2012), p. 41.
- [6] Basuki, T., dkk., “Unintended Consequences: Dampak Sosial dan Politik UU Informasi dan Transaksi Elektronik (ITE) 2008”, *CSIS Working Paper Series WPSPOL*, Jakarta, (2018), hlm. 2.
- [7] The results of Mastel's survey on the national hoax outbreak in 2017 in Juditha, C., “Interaksi Komunikasi Hoax di Media Sosial Serta Antisipasinya”, *Jurnal Pekommas* Vol. 3 No. 1, (2018), hlm. 31-44.
- [8] Pratama, A.B., “Ada 800 Ribu Situs Penyebar Hoax di Indonesia”, <https://www.cnnindonesia.com/teknologi/20161229170130-185-182956/ada-800-ribu-situs-penyebarhoax-di-indonesia/>, diakses Kamis, 04 Maret 2021.
- [9] Siagian, L., dkk., “Peran Keamanan Siber Dalam Mengatasi Konten Negatif Guna Mewujudkan Ketahanan Informasi Nasional”, *Jurnal Prodi Perang Asimetris*, Vol. 4, 3, (2018), hlm. 3.
- [10] Website Resmi Kominfo, “Presiden Jokowi: “Stop Berita Bohong!”, [https://kominfo.go.id/content/detail/9219/presiden-jokowi-stop-berita-bohong/0/sorotan\\_media..](https://kominfo.go.id/content/detail/9219/presiden-jokowi-stop-berita-bohong/0/sorotan_media..), diakses Kamis, 04 Maret 2021.
- [11] Tarigan, A., “Menkopolkam: Berita Hoax Buat Masyarakat Merugi”, <http://www.antaranews.com/berita/604730/menko-polhukam-berita-hoax-buat-masyarakat-merugi..>, diakses Kamis, 04 Maret 2021.
- [12] Burhan Bungin, *Politik Hiperreality dan Communication Jammed dalam buku Turned Back Hoax: Tantangan Literasi Media Digital*, Buku Litera dan Aspikom Korwil Jawa Timur, Surabaya, 2017.
- [13] Situngkir, H., “Spread of Hoax in Social Media: A report on empirical case”, *Journal of Economic Perspectives*, Vol. 31, 2, (2017).
- [14] Allcott, H., and Gentzkow, M., “Social Media and Fake News in the 2016 Election”, *Journal of Economic Perspectives*, Vol. 31, 2, (2017), p. 211-236.
- [15] Siswoko, K.H., “Kebijakan Pemerintah Menangkal Penyebaran Berita Palsu atau Hoax”, *Jurnal Muara Ilmu Sosial, Humaniora, dan Seni*, Vol. 1, 1, (2017), hlm. 13-19.
- [16] Furchan, A., *Pengantar Metode Penelitian Kualitatif*, Usaha Nasional, Surabaya, 1992.
- [17] Kementerian Negara Perencanaan Pembangunan Nasional/Badan Perencanaan Pembangunan Nasional, Visi dan Arah Pembangunan Jangka Panjang (PJP) Tahun 2005 – 2025.
- [18] Sani, M., “Artikel RUU Keamanan Nasional”, Website Resmi Kemenkumham RI, [http://ditjenpp.kemenkumham.go.id/index.php?option=com\\_content&view=article&id=2269:ruu-keamanan-nasional&catid=64:rancangan-undang-undang..](http://ditjenpp.kemenkumham.go.id/index.php?option=com_content&view=article&id=2269:ruu-keamanan-nasional&catid=64:rancangan-undang-undang..), diakses Kamis, 04 Maret 2021.
- [19] *Ibid.*
- [20] Kusmanto, H., “Mewujudkan Stabilitas Keamanan Mendukung Pertumbuhan Ekonomi Nasional”, *Jurnal Kajian Lemhanas RI Edisi 25*, (2016), hlm. 13-23.
- [21] Townes, M., “The Spread of TCP/IP: How the Internet Became the Internet”, *Millenium: Journal of International Studies*, Vol. 41 (1), (2012), p. 51.
- [22] WGIG, “Report of the Working Group on Internet Governance”, (2005).
- [23] van Eeten, M.J.G., and Mueller, M., “Where is the Governance in Internet Governance?”, *New Media & Society* 15, 5, (2012), p. 722.
- [24] Kurbalija, J., *An Introduction to Internet Governance*, Diplo Foundation, Jenewa, 2010, p. 15.
- [25] Kurbalija, J., *An Introduction to Internet Governance*, Diplo Foundation, Jenewa, 2010, p. 15.
- [26] Pada tahun 2001 telah dibuat RUU PTI dan RUU IETE.
- [27] Saragih, B., “Tantangan Hukum Atas Aktivitas Internet”, Harian Kompas, 09 Juli 2000.
- [28] APJII, *Profil Pengguna Internet Indonesia 2014*, APJII, Jakarta, 2014, hlm. 22.
- [29] Basuki, T., dkk., “Unintended Consequences: Dampak Sosial dan Politik UU Informasi dan Transaksi Elektronik (ITE) 2008”, *CSIS Working Paper Series WPSPOL*, Jakarta, (2018), hlm. 11-12.