Narrative Policy Framework (NFP) Electronic System Operator Policy: Surveillance and Cyber Security

Ambar Alimatur Rosyidah; Farah Fajriyah
Communication Science, Gadjah Mada University, Indonesia
ambaralimaturrosyidah@mail.ugm.ac.id
farahfajriyah@mail.ugm.ac.id

10.22146/globalsouth.81057

Indonesia, as one of the Global South countries, has responded to digital transformation by launching the policy of the Minister of Communication and Information Technology Number 5 of 2020 concerning the Implementation of Private Electronic Systems (ESO) for the realization of digital sovereignty. The policy reaped negative sentiments from the public. Several articles considered 'rubber articles' indicated to weaken human rights in obtaining and conveying information, as stated in Article 28F of the 1945 Constitution. This study aims to understand the narrative of digital sovereignty built by Kominfo in the ESO policy and strategies to strengthen that narrative. The research method uses a qualitative approach to the Narrative Policy Framework (NFP) by collecting reliable online data from the official Kominfo website, online media, and press conference videos. This study was studied using Agency Theory, where the Indonesian people, as the principal, delegate authority to the agent, Kominfo, related to ESO policies. The results of the NPF found economic narration from the Ministry of Communication and Information Technology. This narration contradicts the narrative of ESO's policy with the goal of its existence, which is the realization of digital sovereignty. This study also underscores the importance of co-regulation with ESO to strengthen the narrative of digital sovereignty.

Keywords: *Narrative Policy Framework; ESO policy; digital sovereignty; surveillance; cyber security*

Introduction

As one of the Global South countries, Indonesia responds to digital transformation by launching the Regulation of the Minister of Communication and Information (Permenkominfo) for Electronic System Operators (ESO) in the private sphere to achieve digital sovereignty. The Ministry of Communication and Information (Kominfo) of the Republic of Indonesia announced through a press conference that the deadline for private ESO registration is to end on July 20, 2022. Based on Government Regulation Number 71 of 2019 and Minister of Communication and Information Technology Regulation Number 10 of 2021 concerning the Amendment to the Regulation of the Minister of Communication and Information Technology Number 5 of 2020 (ESO, 2020). Unfortunately, this policy reaps negative sentiments from the public.

Drone Emprit Publication, through news and conversations on Twitter with #BlokirKominfo, reported that negative public sentiment reached 81% while positive sentiment was only 12% (Rahman, 2022).

Negative sentiment contains tweets related to criticism of the steps of the Ministry of Communication and Information when blocking the Steam site, Paypal, and online game applications. In addition, the public said that Kominfo's steps had killed livelihoods and content creators' freedom of expression, and the people also compared them with not blocking gambling sites. Public digital rights threaten the public, which is related to privacy violations and restrictions on activities using social media (Rahman, 2022).

The policies that have the potential to violate Human Rights are the application of governance and moderation of information and/or electronic documents in Act 9, paragraphs 3 and 4, requests for termination of access to Act 14, and recommendations for access to data, information, and/or private conversations Act 36 Permenkominfo No. 5/2020 (SAFEnet, 2022). This situation has deviated from democratic values and human rights in obtaining and conveying information as stated in Act 28F of the 1945 Constitution. In addition to receiving information, the public as information transmitters is also faced with ambiguity because no policy specification regulates content.

According to IT expert Teguh Aprianto, the ESO policy raises the assumption of a 'rubber act' (Riyanto, 2022). Rubber Act or rubber law is an article on statutory regulations whose interpretation is subjective and originating from law enforcers or other related parties (Wulandari *et al.,* 2021). The rubber article has been indicated in the ITE Law, which is also the basis for creating ESO policies; the article is in Article 27, paragraph 3 on defamation, and Article 29 on threats of violence.

In terms of violence, this has happened to PSE loans or online loans. LBH Jakarta stated that these crimes consisted of bills committed with various criminal acts, such as threats, fraud, dissemination of personal data, and even sexual harassment (LBH Jakarta, 2021).

The case involved misuse of personal data by online lending ESO and was deemed to violate human rights. Moreover, indirectly there has been a crime in the digital space. Then the function of ESO is questioned as a third party present to fix people's problems in the digital space.

The above phenomenon is the background for this research to emerge. The ESO polemic, initially presented as a response to the problem of Indonesia's digital sovereignty, has raised questions about "whose digital sovereignty belongs to?". As a democratic country that uses the law as a guide, this polemic signifies the urgency of evaluating policies that have the potential to violate the purpose of its formation, digital sovereignty. Therefore, this study aims to find out the narrative of "digital sovereignty" built by the government regarding ESO policies and formulate strategies to strengthen ESO policies in Indonesia.

Adonis (2019) carried out critical research on digital sovereignty literature to discover the digital sovereignty narrative. Adonis (2019) classifies literature taxonomically into four main themes: conceptual development of digital sovereignty, actors in digital sovereignty, digital sovereignty and

global internet governance, and categorical issues. Of these four categories, the narrative of 'digital sovereignty' is dominated by the state's central position in the political security field. Meanwhile, the political-security narrative is far from social and economic civil rights.

Lambach and Oppermann (2022) researched digital sovereignty narratives on German political discourse using narrative analysis methods on three structural elements: setting, character, and employment. The study's results found seven overlapping and partially contradictory digital sovereignty narratives, summarized in five: economic prosperity narrative, security narrative, "European way of life" narrative, modern state narrative, and individual empowerment narrative (Lambach & Oppermann, 2022). These five narratives have different elemental structures.

In the narrative of economic prosperity, Germany emphasizes the global struggle to win economic competitiveness. The main character is the government, specifically the Ministry of Economy and Energy and the Ministry of Transportation and Digital Infrastructure, with a digital transformation setting. At the same time, the narrative plot comprises five pillars: market-oriented law, reducing dependence on non-European actors, German and European digital industrial policies, digital education, and the importance of cooperation across Europe (Lambach & Oppermann, 2022). The main characters are the Ministry of Home Affairs and the Ministry of Defense, various security agencies where the 'criminals' characters are transnational criminal networks and powerful economic actors (Google, Facebook, Amazon). Chinese companies (Huawei and Alibaba) and foreign state actors (regimes). Chinese and Russian authoritarians, and US intelligence agencies) (Lambach & Oppermann, 2022). Then the narrative plots that this is the government's effort toward strategic autonomy in cyberspace in security technology (Lambach & Oppermann, 2022).

Next is the security narrative with the setting of digital sovereignty in cybersecurity. Cybersecurity refers to practices that ensure three important points called the CIA Triad. As mentioned by Warkentin & Orgeron in the book Digital Technology-Based Teaching by Sandirana Juliana Nendissa, The three points are confidentiality, integrity, and availability (Basmatulhana, 2O22). President Obama also 2009 proclaimed, "I call upon the people of the United States to recognize the importance of cybersecurity and to observe this month with appropriate activities, events, and training to enhance our national security and resilience" (The White House, 2009).

The national security issue is the question of digital sovereignty. As a regulation in Indonesia, ESO tries to provide a solution that still has many inequalities, both in terms of the basis of the law and its implementation. From the phenomena and facts discussed regarding data security issues in the internet world, this research is essential to present, especially in the Indonesian context, ESO policies.

Understanding Digital Sovereignty

The researcher focuses on the category, namely Digital Sovereignty, Government, and The State. This category is one of five categories of digital sovereignty, according to Couture & Toupin (2019), based on the actors involved and related issues. In digital sovereignty, the government and the state emphasize the importance of the state enacting regulations to control cyber activity.

The mobilization of the idea of 'sovereignty' that has existed since ancient Roman times (Hinsley, 1986) to the 'digital' realm has resulted in new terminology, digital sovereignty. The modern concept of sovereignty relates to the state (Couture & Toupin, 2019), which in the Cambridge Dictionary is defined as 'the power of a country to control its government' (Cambridge, 2022). Philpot mentions four essential aspects of sovereignty in the Stanford Encyclopedia of Philosophy (2020), namely:

1. the holder of the sovereign has authority,
2. the holder of the sovereignty derives authority from several mutually recognized sources of legitimacy,
3. the highest authority, and
4. this authority lies over an area.

Another definition is from Pierre Belanger, a CEO of a radio station in France. Pierre defined digital sovereignty in 2011 as 'control of our present and destiny as manifested and guided by the use of technology and computer network' (Gueham, 2017). The discussion of digital sovereignty depends on the perspective used because it will determine the meaning of this terminology.

The term 'digital sovereignty' started with the emergence of 'cloud technology. This technology allows someone to have a virtual space to store internet data. Raises several problems related to cross-border data, which the government responds to by regulating cyberspace. Regarding the relationship between national sovereignty and cyberspace, The Economist (2012) states that the state is divided into two camps: "One consists of the more authoritarian states, who want to turn back time and regain sovereignty over parts of the world. Others want to keep their national internet and its governance as it is".

Powers and Jablonski (in Couture & Toupin, 2019) exemplify China and the Western Government as two different camps, China with the discourse of information sovereignty and the Western Government with internet freedom. From the political economy perspective, globalism is considered beneficial for the Western economy, so it is necessary to control the information network. However, this raises the issue of excessive government surveillance. According to Hao Yeli (2017), it results in three debates from a virtual space perspective: contradictions with the spirit of the internet, human rights, and contradictions with multi-stakeholder involvement in internet regulation.

Indonesia responds to the digital world by trying to realize "digital sovereignty" through the PSE policy. Digital is conventionally defined, meaning technologies, infrastructures, data, and content based on and using electronic computing techniques (Peters, 2016, p. 94). Looking at the Cambridge Dictionary and the development of cyber-

space, researchers define *digital sovereignty* as 'the power of a country to control its government by regulating cyberspace to avoid problems related to cross-border data.'

The idea of "sovereignty" concerning digital is then mobilized by various actors, starting from the head of state and other parties involved. In this article, the Ministry of Communication and Informatics promotes goals as diverse as state protectionism, multi-stakeholder Internet governance, or protection against state surveillance.

Understanding Government as Agents

In analyzing this study, researchers used Agency Theory. Agency theory was introduced by Jensen and Mecking (1976), who are economists. This theory explains the relationship between an individual or group of individuals (principals) employing one or more people (agents) to delegate responsibilities/jobs. Jensen and Mecking give an example of principals, such as shareholders who give authority, while agents are company managers responsible for running the company. In line with the Agency Theory, the Indonesian people are the principals who delegate authority to agents, namely Kominfo, related to ESO policies.

According to Eisenhardt (1989), there are three assumptions of this theory, namely, assumptions about human nature, namely self-interest, bounded rationality, and risk aversion. This self-interested nature plays an essential role in policy and even affects the implementation of the policy itself (Rahayu, 2018). Agents controlling this system do not guarantee that they will obey the principal because there is an interest in maximizing profit (Rahayu, 2018).

There is an information gap between the agent and the principal, or what Scott (2000) calls information asymmetry. Agents have more information to act according to their self-interest, while principals with less information struggle to control agents. This causes differences in the direction and goals of the principal and agent, thus potentially creating conflict (Rahayu, 2018).

Methodology

The power of narrative in public policy illustrates the importance of language, examines discourse, and displays hidden ideologies (McBeth & Jones, 2010). Narrative research plays an important role, especially in analyzing public policy. Hukkinen, Roe, and Rochlin (1990) mention Narrative Policy Analysis (NPA) which aims to seek consensus and policy solutions. Jones and McBeth (2010) introduced the Narrative Policy Framework 2010 as a 'quantitative, structuralist, and positivist approach as a study and theory of policy narrative development.' Gray and Jones (2016) state that NPF is compatible with qualitative research. This qualitative NPF adapts previous studies regarding elements or components of policy narratives: setting or context, plot, characters, and story morals. The researcher uses this qualitative Narrative Policy Framework (NPF) method to analyze the ESO policy narrative.

In NPF research, there are three levels of analysis according to the focus of the analysis. At the macro level, the analysis focuses on institutional and cultural policy

narratives; at the meso level, with groups and coalitions, micro influences policy narratives on individuals (Gray & Jones, 2016). This micro-level focuses on how individuals create and are shaped by narratives, such as public opinion about a policy. At the meso level, policy actors build and communicate narratives to actors who influence the policy process. Then, at the macro level, the research elaborates on the research question of how policy changes or stability in the context of cultural and political institutions (Ristyastuti & Rofii, 2021). The researcher analyses this policy narrative at the meso level of analysis, namely the Ministry of Communication and Information (Kominfo) as the actor of the policy.

Researchers used secondary data from press releases on the Kominfo website, Kominfo press conferences on the Youtube platform, and online media relevant to the research topic. There are four main keywords that researchers use in determining research data' digital sovereignty', 'ESO policy,' 'surveillance,' and 'cybersecurity.' Several relevant literature sources from scientific journals, books, or reports support this research.

Results and Discussion

The Private Electronic System Operator (ESO) policy is a response from the Ministry of Communication and Information, which is narrated to protect digital sovereignty and the rights of Indonesian citizens. It is an initial effort to create a more accountable digital ecosystem. Act 47 of the ESO Policy states that Private Scope ESOs have a registration deadline of no later than 6 (six) months since this Ministerial Regulation comes into effect on July 20, 2022, to be precise (Kominfo, 2020). ESOs who have yet to register will receive a warning and a letter and block access if they do not respond. In a press release dated July 29, 2022, Kominfo explained the evaluation results, where 10 of the 100 most popular SE in the mandatory registration category had yet to register (Kominfo, 2022). The result was 7 ESO blocked on July 30. After that, ESO policy was in the spotlight. The Kominfo Block hashtag has gone viral, with various negative opinions. Then, through a press release, Kominfo denied the issue.

For this reason, the setting of this research is on the role and involvement of Kominfo in handling digital sovereignty through the ESO policy. Meanwhile, the time setting follows the mention of the keywords 'digital sovereignty' and 'ESO' on the Kominfo website, from December 9, 2013, to August 6, 2022. There are 26 acts in the form of media highlights and press releases related to 'digital sovereignty, which are the primary data. For ESO, the researcher took a video of the Virtual Press Conference conducted by Kominfo.

Kominfo shows the narrative that they are heroes in their press release because they can maintain digital sovereignty by solving the problem of protecting people's rights in the digital world. These narratives can be seen in most press release headlines such as 'Fight for Digital Sovereignty,' 'Maintain Digital Sovereignty,' and 'Realise Sovereignty.' Electronic System Operators are criminals because they are considered owners of illegal systems in Indonesia. In its press

release, Kominfo stated that blocking and terminating access occurred at several ESOs because they had not registered, and some were online games with gambling elements (Kominfo, 2022). The public is a victim of the lack of sovereignty in the digital space, as seen in Table 1.

Table 1
Identification Results
Narrative Framework Policy

Narrative Framework Policy	
Level analysis	Meso: Ministry of Communication and Informatics
Settings	• Handling Digital Sovereignty • The role and involvement of Kominfo • December 9, 2013 - August 6, 2022 • Indonesia
Characters	Heroes: Kominfo (press release) Villain: Electronic System Operator (ESO dominant narrative) Victims: Indonesian Society (Counter Narration)
Plot	• Initial: Issuing a termination sanction for unregistered ESO • Middle: Blocking unregistered ESO • End: Responding to public sentiment regarding ESO
Moral of the story	Co-regulation with the electronic system operator (ESO)

The Settings: Narrative of Digital Sovereignty

Kominfo started the 'digital sovereignty' narrative on the official website kominfo.go.id on December 9, 2013. Before, 'digital sovereignty' referred to frequency sovereignty related to cellular operators. 2017 was the starting point for the 'digital sovereignty' issue to be included in the discussion. On January 20, 2017, the Kominfo website again included digital sovereignty, quoting the Indonesian Internet Service Providers Association (APJII) chairman. He stated that email and cloud-based in Indonesia were related to increasing digital sovereignty. The discourse of this term developed along with internet penetration, reaching 54.68% or 143.26 million people (Kominfo, 2017). On August 20, 2017, Press Release, Kominfo presented a discourse on redefining 'digital sovereignty. Through the Minister of Communication and Information Rudiantara, he stated:

"What do we need to do to redefine digital sovereignty? Because sovereignty in cyber media is different from others. I believe in added value; as long as there is added value from a business process. It does not have to be all in Indonesia because digital technology is already global, so we must formulate this sovereign mindset. In formulating sovereignty, we must not be chauvinistic in the digital world." (Kominfo, 2017)

Kominfo, through the Minister of Communications and Informatics Rudiantara, defines digital sovereignty as '...processes related to digital technology, applications, devices, ecosystems, and networks. These value-added processes must exist in Indonesia…' (Kominfo, 2017). Digital sovereignty is considered to impact the national economy by mentioning added value. The value is related to the magnitude of a commodity's increasing value at its production stage (Koedel, 2015). The solution offered by Kominfo at that time was to encourage the

development of local applications focused on education and health. In addition, the expansion of the Kominfo function is not only as a regulator but also as a facilitator and accelerator (Kominfo, 2017).

After the redefinition narrative, Kominfo uploaded media highlights which began to present a narrative of national borders in the digital world, considering that Indonesia is a profitable market. There is a discussion of the Draft Government Regulation (RPP) on e-commerce trade transactions to application developers and foreign OTT regarding taxes and royalties as material restrictions. Until 2018, digital sovereignty narrated on the official Kominfo website was still within the scope of economic and infrastructure issues.

Digital sovereignty is the ability to control digital assets, such as data, content, or digital infrastructure or the use of those data assets (Snowden, 2013). In 2019, Kominfo began narrating this data sovereignty-related digital sovereignty. Digital HR competence and data security are essential issues besides infrastructure issues. Data is a new wealth for the nation, giving rise to discussions and regulations on Personal Data Protection (PDP) with a narrative to benefit the state and the people (Kominfo, 2019).

Kominfo's narrative is in line with the statement from the Chief of Staff of the President, Dr. Moeldoko, who stated that digital sovereignty is a critical factor in protecting the country's economic growth and realizing national cybersecurity (Kantor Staf Presiden, 2022). Likewise, the statement of Muhammad Arif Angga, chairman of APJII, said that "defending cyber sovereignty is equivalent to defending the sovereignty of the Unitary State of the Republic of Indonesia (NKRI)" (APJII, 2022).

The pandemic has increased the discussion of digital sovereignty more comprehensively. Apart from the Government and APJII, Telkomsel, a state-owned telecommunications operator, also issued a statement linking digital sovereignty to the economy. First, Whisnutama, Main Commissioner PT Telkomsel, mentioned 'digital sovereignty to create opportunities and potential for service actors and local Indonesian products to be competent in the digital era' (Wijayanti, 2021). Next is Fajrin Rasyid, Digital Business Director of Telkom Indonesia, who underlined digital sovereignty as a critical factor in protecting the country's economic growth and security with online transactions (Chew, 2021).

The increased discussion of digital sovereignty is related to the increase in Indonesia's internet penetration and the government's plans for digital transformation. Internet penetration has increased from 64.8% in 2018 to 73.7% in 2019-2020 (APJII, 2022), and the commercial implementation of 5G technology in Indonesia in 2021 (Sugandi, 2022). In the 2020-2024 Kominfo Strategic Plan, Kominfo accelerates digital transformation around 5G infrastructure and implementation, digital literacy, and equitable access to communication and information technology regulations (Kominfo, 2021). Digital sovereignty is said to be the key to accelerating this digital transformation.

The year 2022 is a recovery period for Indonesia after the pandemic, as stated

in the Day of National Awakening tagline 'Heal Faster, Rise Stronger. The narrative of 'digital sovereignty' is increasingly echoed by the eight press releases on Kominfo's website related to these keywords and the mention of digital sovereignty in the Kominfo press conference at ESO. Kominfo began to take several steps by implementing the Private Scope Electronic System Operator (ESO) policy. It was ratified last November 2020, migration of analog to digital broadcasts, development of digital infrastructure from upstream to downstream, and HR training through the National Digital Literacy Movement.

Dominant Narrative and Counter-Narrative ESO Policy

The researcher identified two dominant narratives of the digital sovereignty narrative related to ESO policies: surveillance and cybersecurity.

Surveillance,

The narrative of digital surveillance in Indonesia was delivered by the Director of Aptika Kemkominfo, Samuel Abrijani Pangerapan, in a Press Conference on Youtube Kemkominfo TV. Pangerapan stated regarding state control, 'We will always open opportunities for anyone who wants to be a part of Indonesia's digital ecosystem; we open them, both domestically and abroad. We are open, but rules are rules. We stand where the sky is upheld' (Kemkominfo TV, 2022). The Private Scope ESO Law for those who do not register, as referred to in paragraph 1, is that the Minister provides administrative sanctions in the form of Termination of Access to Electronic Systems (access blocking) (Permenkominfo 5/2020).

Kominfo's narrative is not by the conditions in the field. From the news regarding the impact of the implementation of the ESO policy, LBH Jakarta, as of August 30, 2022, has received 182 public complaints. The complaint post is intended for disadvantaged people due to arbitrary blocking and repression of freedom in the digital realm due to the enactment of Regulation of the Minister of Communication and Information Technology No. 5 of 2020 (Permenkominfo 5/2020). There are four patterns of problems from the LBH Jakarta report. It is, first, reduced in the form of loss of access to services that are entitled to be obtained. Second, loss in the form of loss of income. Third, losses in the form of loss of work. Fourth, complainants who are doxed as a result of protesting and rejecting the blocking (LBH Jakarta, 2022). Still, in the same press conference, Pangerapan narrates about personal data, not as a form of monitoring feared by the public.

'We cannot see personal data, or we can monitor it; that is not monitoring that way. So the conversation could not let alone ask for the data not carelessly. It cannot be done merely if law enforcement officers, officials, or agencies have the authority. Yesterday I explained that it could all be done if a crime incident requiring additional data to reveal the crime or PT PPATK indicated that there was money laundering. However, those who request data must have authority first. Kominfo is not for that' (Kemkominfo TV, 2022).

The narrative is based on the relevant ESO policy being obliged to provide access to Electronic Systems and Electronic Data to Ministries or Institutions in the context of supervision. Following laws and regulations and must provide access to Electronic Systems and Electronic Data to Law Enforcement Officials in the context of law enforcement by statutory regulations (Permenkominfo 5/2020).

Cyber security expert and founder of Ethical Hacker Indonesia, Teguh Aprianto, called this a dangerous act because the rubber act uses the phrase "disturbing the public and disturbing public order," which has no explanation. This practice is common in Electronic Information and Transactions Law (ITE) cases. Later it can be used to 'turn off' criticism even if delivered peacefully. What is the basis? They (the government) are only responsible for disturbing public order (CNN Indonesia, 2022).

Regarding personal data, the Head of the Division of Freedom of Expression of SAFEnet, Nenden Sekar Arum, said the rules made by Kominfo are too lax. With that, there are gaps and opportunities for authority holders to access and monitor the specific data of ESO users. It is also exacerbated by the absence of an independent agency appointed to oversee Kominfo in implementing the regulation. According to Nenden, the Permenkominfo has had problems since its inception. He saw that Kominfo only involved the public a little, so the regulations produced seemed only for the government and the ESO. Meanwhile, the rights and losses of ESO consumers should be considered in the current regulations (Sugandi, 2022).

Cybersecurity

The ESO policy's cybersecurity narrative relates to the digital space's security. Pangerapan, at a press conference, explained that 'Every country has its rules, and these rules are to create a digital space that is conducive, safe, and comfortable. Indonesian people can feel digital economic growth and benefit Indonesia' (Kemkominfo TV, 2022). ESO policy prohibits electronic information. As referred to in paragraph 3, electronic documents are classified as: a. violate the provisions of laws and regulations, disturbing the public and disturbing public order, and notifying the way or providing access to Electronic Information Electronic Documents that are prohibited.

Contrary to statements regarding digital security, the current insecurity of the digital space threatens the public. It is proven by the leaks of government-managed data, such as the case of the leak of Indonesian population data from the KPU and BPJS (much, 2021). Likewise, in 2022 there were three data leaks. The data leak of 17 million customers of the State Electricity Company (PLN) in mid-August, browsing history data for Indihome on August 21, and 1.3 billion SIM Card registration data in September, claimed to have come from Kominfo (Saptohutomo, 2022).

Digital Sovereignty: Surveillance and Cybersecurity

In agency theory, agents are assumed to be self-interested. Kominfo, as an agent,

raises a discourse on digital sovereignty, which suggests that this ESO Policy is for the benefit of the Indonesian people. However, judging from the narrative built, Kominfo has economic and political motives as a policy agent. It can be seen in the initial mention of 'digital sovereignty' by the Minister of Communication and Informatics Rudiantara (2014-2019), which was based on the concept of 'added value. Then the discussion about the ESO tax was mentioned by the Director General of Aptika Kominfo Samuel Abrijani Pangerapan. In the Kominfo Press Conference on July 19, 2022, Pangarepan emphasized why he had to register the ESO 'This is governance because it is mandatory. They must pay the tax if there is a complaint or profit" (Kemkominfo TV, 2022).

People, as principals, want a digital space that provides freedom of expression and security for their data. The origins underlie the creation of the internet with the ideology of liberalism, which opposes all forms of control, both state and commercial entities (Castells, 2001). This misalignment of interests between the public (principal) and Kominfo (agent) shows vulnerabilities in surveillance and cybersecurity. Regarding surveillance, the Head of the Division of Freedom of Expression at Safenet, Nenden Sekar Arum, considers that the rules made by Kominfo are too lax. ESO creates gaps in opportunities between authority holders to access and monitor ESO user-specific data. It refers to the definition of specific personal data 'as health data and information, biometric data, genetic data, life/orientation sexual, political views, children's data, personal financial data, and other data by the provisions of laws and regulations.

Apart from supervision, the public, as principals, is also faced with cybersecurity threats with data leaks. Regarding the security of personal data, Kominfo's performance was questioned after three cases of data leaks throughout 2022. The narrative of 'creating a conducive, safe, and comfortable digital space.' What the Director General of Aptika Kominfo said contradicted reality. The hashtag #TuntutKominfo is trending on Twitter in response to the leak of 1.3 billion data that has touched 8,579 tweets since September 8, 2022.

Kominfo responded with a narrative that this was the authority of BSSN, not Kominfo. However, in Government Regulation Number 71 of 2019, Kominfo has the authority as a regulator, accelerator, and facilitator in data management. At the Kominfo Press Conference, Samuel Abrijani told hackers, 'Yes, if you can, do not attack. Because every time there is a data leak, the public is harmed; it is an illegal access act' (Saptohutomo, 2022). For this response, Kominfo also received criticism from the Deputy Chairperson of the Indonesian House of Representatives Coordinator for People's Welfare (Korkesra), Abdul Muhaimin Iskandar, that Kominfo cannot provide personal data protection (Hidayatullah, 2022). Likewise, members of Commission I DPR Nico Siahaan and Nurul Arifin questioned the credibility of Kominfo (Dirgantara, 2022; Astian, 2022).

Concerning data leaks, apart from the credibility of Kominfo in handling cases, the public loss of this data leak is a paramount concern. Kominfo published 'Public Perception of Personal Data Protection 2021', and the public appears to suffer an economic loss. The thing they experienced the most was a reduction in savings in bank accounts (44.1%) and reduced balances in e-wallets (32.2%) to transfers or purchases because they were contacted by certain people or companies (28.1%) (Mutia, 2022). In the scope of cross-border data, on November 2022, a cybersecurity news site Cyber News reported that WhatsApp user data was leaked and sold in an online forum, of which 130,000 were active WhatsApp user numbers from Indonesia (Clinten, 2022). Even though it received objections from Meta, the parent of Whatsapp, this event certainly raises potential impacts detrimental to the state if looking at the Kominfo narrative of data as national wealth.

Policy Middle Way

Dominant narratives and counter-narratives shape digital sovereignty in Indonesia, where there is a gap between the two. This gap is in the form of different perceptions regarding digital sovereignty, information that is less specific from the government, and there needs to be a definition of what kind of crime constitutes a violation of digital sovereignty. From these results, the counter-narrative considers that the termination of access is not part of digital sovereignty because it causes harm to the public (principal), which in the narrative is a protected party.

Table 2
Results, Cons, Dominant and Narrative Differences

Counter Narrative	Dominant Narrative	Cause Difference
There are complaints from people who have experienced arbitrary blocking and repression of freedom due to the implementation of the ESO policy.	Kemkominfo opens opportunities for anyone who wants to be part of Indonesia's digital ecosystem by following existing regulations.	There are different perceptions that the termination of access by Kominfo is considered a process towards a sovereign state. However, it has a significant impact on various sectors.
Indonesia's digital security conditions are filled with hackers, user data leaks, and insecurity in expressing opinions in the digital space.	The narrative of Kemkominfo is that they created rules to form a conducive, safe, and comfortable digital space.	The Kemkominfo narrative is not followed by further detailing, which results in the use of data by some people who take personal advantage.
The ESO policy does not consider the rights and losses of ESO consumers with the opportunity for authorities to access and monitor user-specific data and the absence of an independent agency appointed to supervise.	Kominfo stated that requesting personal data is not a form of supervision. The party accessing it must also have authority for reasons of law enforcement.	Kominfo assumes that public data access and monitoring are related to digital space crimes without specifics on what is considered a crime, so it has the potential to be a policy with gaps to be used by the authorized person.

Minister of Communication and Information Rudiantara said this digital sovereignty relates to the economic concept of 'added value' (Kominfo, 2022). However, if the public suffers a loss due to this termination, the government's narrative makes the meaning of digital sovereignty far from social and economic civil rights.

In agency theory, the imbalance of policy interests between the principal (public) and the agent (Kominfo) causes differences in the direction and objectives of the ESO Policy. Kominfo as an agent controlling the ESO policy, does not guarantee that it will obey the public as the principal because of the interest in maximizing profit. Due to the conflict, the researcher recommends a middle-ground policy based on the facts analyzed from the ESO policy narrative.

Surveillance of information/data plays an essential role in global political economy relations, where its power should be the state's focus (Comor, 1996). In its implementation, there are two modes mentioned by Comor (1996). First, the problem of facilitation, empowerment, and creation, then the mode of control, exclusion, and prevention functions. The narrative shown by Kominfo is dominant in the control function. The termination of access by the Ministry of Communication and Informatics and the clause providing access to personal data if there are legal issues are two regulations showing state control over private sector ESO.

However, policies related to digital sovereignty need to look at from the perspective of the 3 (three) actors involved, namely the state, citizens (citizens), and the international community (Yeli, 2017). This unilateral blocking and access to personal data are not seen from the citizens' perspective. Regarding the blocking, the Indonesian people, as SE users, suffered material losses. Even though it only takes days, termination of applications without socialization with citizens is an unstructured form of the registration system. It shows the facilitation problem in ESO's policies regarding supervision. If this system has not been established, there will be the possibility of the same incident happening again. The public is again at a loss, digital sovereignty is again an issue, and the benefits are questioned for whom.

Next, regarding granting access to specific personal data, which in Act 1 paragraph 1 is defined as "... health data and information, biometric data, genetic data, sexual life/orientation, political views, child data, personal financial data, data other by the provisions of the legislation" (Permenkominfo 5/2020). This understanding shows the complete control of the state in the digital space, in this case, Kominfo. This act also contradicts Act 28G paragraph (1) of the 1945 Constitution, which states that "everyone has the right to personal protection (privacy), family, honor, dignity, and property (including personal data)" (UUD 1945). Several parties against this control question whether they have adhered to the principles of human rights, which in this case are citizens as netizens. Moreover, there is no facilitation; for example, there is no legal entity, the authorities access the data, and no neutral legal entity to examine or file an objection. The narrative of protecting citizens'

rights contradicts the insecurity about implementing the ESO policy.

Cyber security is an essential point for ESO policy in realizing digital sovereignty. Like the Kominfo statement that data is state property, data loss is defined as loss of wealth. In addition, this also relates to cross-border data. Maintaining its security is like maintaining Indonesia's relations with other countries. In this regard, the Global North countries already have a strong cybersecurity foundation.

Meanwhile, Indonesia implements ESO registration without providing an institution that guarantees data security; in addition to the security system, the narrative of the Code of Ethics on Security also needs to be discussed. Russia, China, and Central Asian countries proposed two Codes of Conduct on Information Security at the UN General Assembly in the interest of the country's greater digital ownership (Wood et al., 2020). Indonesia and Southeast Asian countries should have a digital interpretation and jointly build their security infrastructure.

Collaboration is the ideal middle ground. The issue of digital sovereignty is cross-sectoral, so the collaboration of ministries, other government agencies, and related industries is needed. Germany does this by holding a Digital Summit, a joint government-industry discussion forum to advance Germany's digital transformation (Lambach & Oppermann, 2021). Regarding ESO, self-regulation does not work because there is a market blind spot regarding digital privacy and the lack of government control. In contrast, government regulations have political barriers, and the ability to overcome digital problems is also questioned (Hirsch, 2011). Collaboration with industry (in this case, ESO) with the information capital and experience to create a digital sovereignty narrative related to ESO's digital policy has been strengthened.

Regarding policy, Kominfo can use an alternative approach, namely co-regulation, in which the government and industry share responsibility for drafting and regulating (Hirsch, 2011). The European Union uses this approach to implement personal data protection, where the 2018 General Data Protection Regulation (GDPR-General Data Protection Regulation) applies. Another country, Australia, has also responded by passing the News Media Bargaining Code Law, which aims to address the imbalance between Australian news publishers and the two Silicon Valley giants (Riyanto, 2021).

Conclusion

The virtual world is an inseparable part of all aspects of Indonesian people's life. The presence of the internet forms a digital pattern and ecosystem, forming a living space that moves massively and dynamically on social media. These activities are diverse and worldwide. No longer national but also international. Digital problems arise until digital sovereignty varies from a safe and conducive digital ecosystem. Kominfo responds to this by implementing an ESO policy and a private scope. However, this policy has many interpretations and is considered a rubber act that can be codified and utilized.

Based on the results and discussions related to the ESO policy narrative with the NPF approach, the researchers found that the dominant narrative built by Kominfo is that the ESO policy was carried out to protect people in the digital space for the creation of digital sovereignty. Second, the counter-narrative that hinders the dominant narrative is that excessive surveillance threatens human rights and the reality of personal data protection in Indonesia, which is not yet ideal.

Third, strategic recommendations strengthen the narrative of digital sovereignty related to ESO policies by prioritizing protecting the public's data as the principal rather than the interests of agents with control functions. The first recommendation to Kominfo is to revise the ESO policy, especially in acts related to specific personal data and the prohibition of content that disturbs the public. Then, Kominfo as a facilitator, helps companies from Indonesia, especially in terms of financing, to improve the quality of digital infrastructure facilities in the form of 'cloud' so that data storage as a state asset is located in Indonesia. Kominfo, as the executor, issued an independent institution authorized to protect personal data. Next, collaborate with other ministries and government agencies like Germany did because the issue of digital sovereignty is cross-sectoral. Finally, co-regulation with ESO in making regulations will become a reference for self-regulation platforms operating in Indonesia.

Furthermore, further research is needed in future studies related to digital sovereignty. By knowing the predictions of cyberspace problems, we can take preventive steps, such as preparing regulations that are a priority as the embodiment of digital sovereignty. This regulation will affect the self-regulation platform that will operate in Indonesia.

References

Books

Eisenhardt, K. M. (1989). *Agency Theory: An Assessment and Review*. Academy of Management Review.

Gueham, F. (2017). *Digital sovereignty steps towards a new system of Internet governance.* Paris: Fondapol.

Fischer, C. S. (1994). *America Calling: A social history of the Telephone to 1940.* Oakland: University of California Press.

Powers, S.M., & Jablonski, M. (2015). *The Real Cyber War: The Political Economy of Internet Freedom.* Urbana, IL: University of Illinois Press.

Peters, B. (2016). Digital. In: Peters B (ed.) *Digital Keywords: A Vocabulary of Information Society and Culture*. Princeton, NJ: Princeton University Press, pp. 93–108.

Conference Paper

Wulandari. S., Sulfary. A., Putri, R.R.T., Firdaus. A., Pradnyawan. S.W.A. (2021). Dampak Pasal-Pasal Multitafsir Dalam UU ITE Terhadap Penanggulangan Cyber Crime di Indonesia, *Proceeding of Conference on Law and Social Studies* http://prosiding.unipma.ac.id/index.php/COLaS Held in Madiun on

August 6 th 2021 e-ISSN: 2798-0103

Report

APJII. (2022*). Profil Internet Indonesia 2022*. https://apjii.or.id/survei2022x

Wood, Sam, et al. (2020). *Digital sovereignty: the overlap and conflict between states, enterprises, and citizens, Plum.* https://oxil.uk/publications/2021-01-20-plum-digital-sovereignty/

Rahman. A. (2022). *#BlokirKominfo Dalam Pemberitaan dan Perbincangan 19-30 juli 2022*. https://pers.dronemprit.id/blokirkominfodalam-pemberitaan-dan-perbincangan19-30-juli-2022/

Journal Article (retrieved online, with DOI)

Adyos, M., Vural, Y., Tekerek, A. (2019). Assessing Risk and threats with a layered approach to the Internet of Things security. *Measurement and Control, 52*(5-6), 338-353. https://doi.org/10.1177/0020294019837991

Adonis, A. A. (2019). Critical Engagement on Digital Sovereignty in International Relations: Actor Transformation and Global Hierarchy. *Global: Jurnal Politik Internasional, 21*(2), 262-282. doi.org/10.7454/global.v21i2.412

Couture, S., & Toupin, S. (2019). What does "sovereignty" mean when referring to the digital?. *New Media & Society, 21*(10), 2305-2322. https://doi.org/10.1177/1461444819865984

Gray, G., & Jones, M. D. (2016). A qualitative narrative policy framework? Examining the policy narratives of US campaign finance regulatory reform. *Public Policy and Administration, 31*(3), 193–220. https://doi.org/10.1177/0952076715623356

Hoofnagle, C.J, Sloot, B.V, Borgesius, F.Z. (2019). The European Union general data protection regulation: what it is and what it means, *INFORMATION & COMMUNICATIONS TECHNOLOGY LAW, 28*(1), 65–98. https://doi.org/10.1080/13600834.2019.157350

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs, and ownership structure. *Journal of Financial Economics, 3*(4), 305-360. https://doi.org/10.1016/0304-405X(76)90026-X

Jones, M. D., & McBeth, M. K. (2010). A narrative policy framework: Clear enough to be wrong? *Policy Studies Journal, 38*(2), 329–353. https://doi.org/10.1111/j.15410072.2010.00364.x

Koedel, C., & Rockoff, J. E. (2015). Value-added modelling: A review. *Economics of Education Review, 47,* 180-195. https://doi.org/10.1016/j.econedurev.2015.01.006

Martinez, M. (2019). An Examination of Higher Education Policy Problems Using Narrative Policy Analysis. *American Behavioral Scientist, 63*(3), 369–386. https://doi.rg/10.1177/0002764218820569.

Lambach, D., & Oppermann, K. (2022). Narratives of digital sovereignty in German political discourse. *Governance*. https://doi.org/10.1111/gove.12690

Ristyastuti, M. P., & Rofii, M. S. R. (2021). Analisis Naratif Kebijakan Penyelenggaraan Pilkada Saat Pandemi Covid-19 di Indonesia. *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial, 8*(2), 47-53. http://dx.doi.org/10.31604/jips.v8i2.2021.47-53

Journal Article (retrieved online, without DOI or page numbers)

Asmoro, W., & Lindiasari Samputra, P. (2021). ANALISIS NARATIF KEBIJAKAN: KEBIJAKAN GANJA MEDIS DI INDONESIA. *Matra Pembaruan, 5*(1), 13-24. Retrieved from: https://www.researchgate.net/publication/352252430_Analisis_Naratif_Kebijakan_Kebijakan_Ganja_Medis_di_Indonesia

Hirsch, D. D. (2011). The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?. *Seattle University Law Review, 34*(2). Retrieved from: https://ssrn.com/abstract=1758078

Yeli, H. (2017). A three-perspective theory of cyber sovereignty. *Prism, 7*(2), 108–115. Retrieved from: https://cco.ndu.edu/PRISM-7-2/Article/1401954/a-three-perspective-theory-of-cyber-sovereignty/

Audiovisual media (videos, music recordings, podcasts, etc.)

Gladu, A. (Producer), & Brodeur. M. (Director). (2001). *Dance of the Warrior* [Motion picture]. Canada: National Film Board.

Kemlu TV. (2017, May 5). *Laporan Pemajuan Ham Indonesia di PBB* [Video file]. Retrieved from: https://www.youtube.com/watch?v=8VLR-yuLX3uw

Electronic Source

Astian, A. (2022, September 8). Dugaan Kebocoran Data, Nico Siahaan Pertanyakan Kinerja Kominfo. Retrieved from https://republiknews.co.id/dugaan-kebocoran-data-nico-siahaan-pertanyakan-kinerja-kominfo/

Basmatulhana, H. (2022). Cyber Security atau keamanan siber: Pengertian, Jenis dan Ancamannya. Retrieved from https://www.detik.com/edu/detikpedia/d-6262847/cyber-security-atau-keamanan-siber-pengertian-jenis-dan-ancamannya

Chew, J. (2021, November 2). Bagaimana Indonesia Bisa Mewujudkan

Kedaulatan Digital. Retrieved from https://id.techinasia.com/indonesia-mewujudkan-kedaulatan-digital

Clinten, B. (2022, November 28). Meta Bantah Data Pengguna WhatsApp Bocor dan Dijual Online. Retrieved from https://tekno.kompas.com/read/2022/11/28/18060007/meta-bantah-data-pengguna-whatsapp-bocor-dan-dijual-online-?page=all.

CNN Indonesia News. (2022, Juli 20). 4 Bahaya PSE Kominfo Versi Pakar Siber. Retrieved from https://www.cnnindonesia.com/teknologi/20220719170626-192-823466/4-bahaya-pse-kominfo-versi-pakar-siber

Deretan Kasus Bocor Data Penduduk RI dari Server Pemerintah. (2021, September 1). Retrieved from https://www.cnnindonesia.com/teknologi20210901150749-185-688400/deretan-kasus-bocor data-penduduk-ri-dari-server-pemerintah

Dirgantara, A. (2022, September 7). Kritik Data Bocor, Nurul Arifin: Masa Kominfo Sebulan 3 Kali Kebobolan, Memalukan!. Retrieved from https://nasional.kompas.com/read/2022/09/07/13092301/kritik-data-bocor-nurul-arifin-masa-kominfo-sebulan-3-kali-kebobolan.

Hidayatullah, A. Thoriq. (2022, September 8). Kebocoran Data, Muhaimin Iskandar Sebut Kominfo Belum Canggih. Retrieved from https://beritajatim.com/politik-pemerintahan/kebocoran-data-muhaimin-iskandar-sebut-kominfo-belum-canggih/

Kantor Staf Presiden. (2022, Oktober 26). Moeldoko : Indonesia Serius Mewujudkan Kedaulatan Digital. Retrieved from https://www.ksp.go.id/moeldoko-indonesia-serius-mewujudkan-kedaulatan-digital.html.

Kominfo. (2022). SIARAN PERS NO. 312/HM/KOMINFO/08/2022, Pemutusan Akses terhadap 15 PSE Game Online yang Memuat Unsur Perjudian. Retrieved from https://www.kominfo.go.id/content/detail/43441/siaran-pers-no-312hmkominfo082022-tentang-pemutusan-akses-terhadap-15-pse-game-online-yang-memuat-unsur-perjudian/0/siaran_pers

Kominfo. (2022, Agustus 17). Momen HUT ke-77 Kemerdekaan RI, Menkominfo Tekankan Kedaulatan Digital SIARAN PERS NO. 329/HM/KOMINFO/08/2022. Retrieved from https://www.kominfo.go.id/content/detail/43745/siaran-pers-no-329hmkominfo082022-tentang-momen-hut-ke-77-kemerdekaan-ri-menkominfo-tekankan-kedaulatan-digital/0/siaran_pers

Kominfo. (2020, Agustus 17). Digitalisasi Perkuat Resiliensi, Menteri Johnny: Indonesia Pulih Lebih Cepat SIARAN PERS NO. 330/HM/KOMINFO/08/2022. Retrieved from https://www.kominfo.go.id/content/detail/43748/siaran-pers-no-330hmkominfo082022-tentang-digitalisasi-perkuat-resiliensi-menteri-johnny-indonesia-pulih-lebih-cepat/0/siaran_pers

Kominfo. (2022). Perjuangkan Kedaulatan Digital, Menkominfo: Indonesia Usung Empat Prinsip Utama Arus Data Lintas Batas Negara SIARAN PERS NO. 98/HM/KOMINFO/03/2022, (22 Maret 2022). Retrieved from https://www.kominfo.go.id/content/detail/40711/siaran-pers-no-98hmkominfo032022-tentang-perjuangkan-kedaulatan-digital-menkominfo-indonesia-usung-empat-prinsip-utama-arus-data-lintas-batas-negara/0/siaran_pers

Kominfo. (2022, Juni 8). Jaga Kedaulatan Digital, Menkominfo Tekankan Empat Sektor Strategis, SIARAN PERS NO. 239/HM/KOMINFO/06/2022. Retrieved from https://www.kominfo.go.id/content/detail/42388/siaran-pers-no-239hmkominfo062022-tentang-jaga-kedaulatan-digital-menkominfo-tekankan-empat-sektor-strategis/0/siaran_pers

Kominfo. (2022, Juni 7). Wujudkan Kedaulatan, Menkominfo Dorong Pemanfaatan Ruang Digital untuk Semua, SIARAN PERS NO. 238/HM/KOMINFO/06/2022. Retrieved from https://www.kominfo.go.id/content/detail/42383/siaran-pers-no-238hmkominfo062022-tentan g-wujudkan-kedaulatan-menkominfo-dorong-pemanfaatan-ruang-digital-untuk-semua/0/siaran_pers

Kominfo. (2022). SIARAN PERS NO. 308/HM/KOMINFO/07/2022. Retrieved from kominfo.go.id/content/detail/43385/siaran-pers-no-308hmkominfo072022-tentang-pendaftaran-penyelenggara-sistem-elektronik-pse-lingkup-privat/0/siaran_pers.

Kominfo. (2022, Juli 20). Arus Data Lintas Negara, Menteri Kominfo Tekankan Kedaulatan Digital. SIARAN PERS NO. 294/HM/KOMINFO/07/2022. Retrieved from https://www.kominfo.go.id/content/detail/43209/siaran-pers-no-294hmkominfo072022-tentang-arus-data-lintas-negara-menteri-kominfo-tekankan-kedaulatan-digital/0/siaran_pers

Kominfo. (2022). Siaran Pers No. 308/HM/KOMINFO/07/2022, Pendaftaran Penyelenggara Sistem Elek-

tronik (PSE) Lingkungan Privat, Kementerian Komunikasi dan Informatika (kominfo.go.id)

Kominfo. (2022, Juli 11). Transformasi Digital dari Hulu Hingga Hilir: Gerak Cepat Menteri Kominfo Jawab Kebutuhan Digitalisasi Sektor Keuangan, siaran pers. Retrieved from https://www.kominfo.go.id/content/detail/43071/siaran-pers-tentang-transformasi-digital-dari-hulu-hingga-hilir-gerak-cepat-menteri-kominfo-jawab-kebutuhan-digitalisasi-sektor-keuanga n/0/siaran_pers

Kominfo. (2022, Juli 11) Bangun Infrastruktur Digital untuk Rakyat, Menkominfo Apresiasi Dukungan Semua Pihak. Retrieved from https://www.kominfo.go.id/content/detail/43052/bangun-infrastruktur-digital-untuk-rakyat-m enkominfo-apresiasi-dukungan-semua-pihak/0/berita_satker

Kominfo. (2019, September 15). Tingkatkan Kesadaran Perlindungan Data Pribadi. Retrieved from https://www.kominfo.go.id/content/detail/21751/tingkatkan-kesadaran-pelindungan-data-pribadi/0/berita_satker

LBH Jakarta. (2021). Hari Konsumen Internasional: Korban Pinjaman Online Desak Negara Buat Regulasi Yang Menjamin Perlindungan Hukum dan HAM, Siaran Pers,172/RILIS-LBH/III/2021. Retrieved from https://bantuan-hukum.or.id/hari-konsumen-internasional-korban-pinjaman-online-desak-negara-buat-regulasi-yang-menjamin-perlindungan-hukum-dan-ham/

Mutia, A. (2022, October 14). Ini Sederet Kerugian yang Dialami Publik Akibat Kebocoran Data Finansial. Retrieved from https://tekno.kompas.com/read/2022/11/28/18060007/meta-bantah-data-pengguna-whatsapp-bocor-dan-dijual-online-?page=all

Riyanto, G. P. (2022, July 20). 7 "Pasal Karet" Di Aturan PSE Kominfo Yang Ancam Blokir Google dkk. KOMPAS.com. Retrieved from https://tekno.kompas.com/read/2022/07/19/10150087/7-pasal-karet-di-aturan-pse-kominfo-ya ng-ancam-blokir-google-dkk?page=all

Riyanto, G.P. (2021, Februari 26). Australia Sahkan UU Media, Google dan Facebook Harus Bayar Konten Berita. Retrieved from Australia Sahkan UU Media, Google dan Facebook Harus Bayar Konten Berita (kompas.com)

Rizkinaswara, L. (2022, Maret 31). Pemulihan Global, DEWG G-20 Bahas Penggunaan Teknologi Digital, Pemulihan Global, DEWG G-20 Bahas Penggunaan Teknologi Digital – Ditjen Aptika (kominfo.

go.id)

SAFEnet. (2022, Juni 24). Siaran Pers Stop Registrasi PSE Lingkup Privat dan Tarik Kembali Permenkominfo yang Mengancam Kebebasan Berekspresi dan Hak Atas Privasi Pengguna. Retrieved from https://id.safenet.or.id/2022/06/siaran-pers-stop-registrasi-pse-lingkup-privat-dan-tarik-kembali-permenkominfo-yang-mengancam-kebebasan-berekspresi-dan-hak-atas-privasi-pengguna/

Sanjaya, et al. (2021). Laporan Situs Hak-Hak Digital Indonesia 2020, SAFEnet Sudah Tiga Jurnalis Dipenjara di Era Jokowi-Ma'ruf Pakai Jerat UU ITE (cnnindonesia.com)

Saptohutomo, A.P. (2022, September 8). Berbagai Alasan Kominfo soal Rentetan Kebocoran Data. Retrieved from https://nasional.kompas.com/read/2022/09/08/06300031/berbagai-alasan-kominfo-soal-rentet an-kebocoran-data

Sugandi, A. T. (2022, Agustus 9). Blokir Platform Digital Berujung Kontroversi. Retrieved from https://news.detik.com/x/detail/investigasi/20220809/Blokir-Platform-Digital-Berujung-Kon toversi/

Sugandi, A.T. (2022, 8 Februari). Jaringan 5G Jangkau Seluruh Indonesia 3 Tahun Lagi, Ini Alasannya. Retrieved from https://teknologi.bisnis.com/read/20220208/101/1498094/jaringan-5g-jangkau-seluruh-indonesia-3-tahun-lagi-ini-alasannya.

The Economist. (2012). A digital cold war? Retrieved from https://www.economist.com/babbage/2012/12/14/a-digital-cold-war

The White House. (2009). National Cybersecurity Awareness Month, 2009 [Press release]. Retrieved from https://www.whitehouse.gov/the_press_office/Presidential-Proclamation-National Cybersecurity-Awareness-Month

Wijayanti, S. I. (2021, 9 April). Whisnutama : Kedaulatan Digital untuk Indonesia. Retrieved from https://fisip.ui.ac.id/whisnutama-kedaulatan-digital-untuk-indonesia/