Komunikasi : Jurnal Komunikasi, Vol. 14, No. 2, September 2023, E-ISSN: 2579-3292, Halaman 224 -232
KOMUNIKASI : Jurnal Komunikasi
Penerbit: LPPM Universitas Bina Sarana Informatika
***DOI**: https://doi.org/10.31294/jkom.v14i2.12018* ***Website**: https://jurnal.bsi.ac.id/index.php/jkom/*

Government Securitizing Effort of Online Harmful Content in Indonesia

Treviliana Eka Putri
Department of International Relations, Universitas Gadjah Mada, Yogyakarta, Indonesia

ARTICLE INFORMATION

Historycal

Received:
17 Juni 2023
Revised:
27 Oktober 2023
Accepted:
03 November 2023
Published:
05 September 2023

Abstrak - Internet dan media sosial telah mengubah bagaimana individu berkomunikasi dan berinteraksi dengan satu sama lain. Situasi ini telah mendorong perkembangan jumlah user generated content atau konten yang dibuat oleh individu pengguna platform, di mana platform hanya memfasilitasi iinteraski tersebut sebagai sebuah medium atau lingkungan siber. Meski di satu sisi perkembangan tersebut dilihat sebagai salah satu perkembangan dalam menciptakan ruang demokrasi yang lebih luas bagi masyarakat untuk mendukung kebebasan berekspresi dan berpendapat, terdapat beberapa kasus di mana medium yang sama justru digunakan oleh individu untuk menyebarkan konten-konten berbahaya seperti berita palsu, ujaran kebencian, konten penipuan, dan lainnya. Pemerintah dan platform memiliki tanggung jawab untuk mencegah persebaran konten berbahaya dan manifestasinya dalam kejahatan luring. Dalam menangani isu ini, pemerintah seringkali menerapkan sanksi hukum terhadap platform maupun individu. Menggunakan pendekatan sekuritisasi, tulisan ini melihat bahwa pemerintah Indonesia, dalam beberapa kasus telah menerapkan dan memberlakukan konten berbahaya dalam level keamanan nasional, menjustifikasi diberlakukannya tindakan-tindakan ekstra terhadapnya. Meskipun begitu, tulisan ini melihat bahwa penting untuk melakukan upaya desekuritisasi untuk mengembalikan permasalahan ini ke dalam diskusi dan negosiasi politik sehari-hari, di samping untuk memastikan perlindungan terhadap hak asasi masyarakat.

Keywords

harmful online content
securitization
freedom of speech

Abstract - *The emergence of the Internet and social media has altered the way individuals interact with each other. This has also led to the flourishment of user-generated content on many platforms, where platforms act as the medium or environment for users' posts and interactions. While these developments may contribute to bringing space for ensuring citizens' freedom of speech and expression, there are also cases where the very same environment is filled with 'harmful' content such as fake news, hate speech, online fraud, etc. The government along with other related stakeholders in the field has the responsibility to ensure such harmful contents do not manifest into offline harms. In handling these issues, the government has often utilized legal measures to apply sanctions for the platforms and or individual creators and restrict the spread of the contents. Using the securitization perspective, this study will look into the Indonesian government's current approach to tackling online harmful content. This study argues that the government has put the issue to a higher level, putting it into the national security agenda, which results in some extraordinary measures being applied in several instances. Nonetheless, this study suggests that it is important for the government and all related stakeholders to de-securitize the issue, putting it into everyday discussion and politics while ensuring the protection of citizens' rights.*

Corresponding Author:
Treviliana Eka Putri, Department of International Relations, Universitas Gadjah Mada, Yogyakarta, Indonesia, Email: treviputri@ugm.ac.id

INTRODUCTION

The Internet and social media have become one basic need of our modern society. According to Statista (2023) data, the global internet penetration now has reached 64.6%, more than half of the total population. In line with the high internet penetration, it also noted there is a significant increase in the number of social media users. It is estimated that there are 4.9 billion users of social media worldwide (Forbes, 2023). The high number of internet and social media users has also increased the number of risks that entail it such as online fraud, online addiction, cybercrimes, and the spread of hoaxes. In Indonesia, the spread of online disinformation and misinformation is deemed the most dangerous issue on the internet (Kurnia& Astuti, 2017).

The rise of social media has altered the way people produce and consume information. Not only for entertainment and communication purposes, it found that there is a significant use of social media platforms such as Facebook to share and seek information by posting links to news sites and comments on other people's posts (Zuniga, Homera, Jung, Nakwon, & Valenzuela, Sebastian, 2012). However, earlier studies have also observed the significant power of social media to spread misinformation such as hoaxes, conspiracy theories, and fake news due to the ability of the users to share and spread any information, including false and inaccurate information with a lack of third-party filtering (Shao, et.al., 2016).

Information as part of the state's security is also not a new thing. We have witnessed the circulation of propaganda during wars, where conflicting parties tried to project their narratives to the wider public as their audience (Eriksson & Giacomello, 2006). The emergence of the Internet and social media have made it easier for any party who wants to utilize information as power and as a tool of propaganda. It is less costly to spread the information, people can anonymize their identity, and the information can spread faster globally. Therefore, online content regulation is also something that should be inextricably linked with information security. The information revolution has a notable impact on security issues, which are largely confined to the domain of cybersecurity and information warfare.

This study seeks to look at the dimensions of securitization in online speech or online content. Indonesia is deemed to have a deteriorating score on the Freedom on the Net (Freedom House, 2023), and these scores cover at least three significant aspects: obstacles to access, limits on content, and violations of user rights. This study will try to unpack other dimensions within the online content regulation, which is how the securitization of information and speech is being done within these countries. It will assess how information and speech—which will be categorized within the context of online content—are being securitized and how actors and agents of securitization engage. As Wæver (2004) put it, "It is by labeling something a security issue that it becomes one". Who are the important actors how is the securitization effort accepted by the audience—civil society and constituents, and how are the efforts to de-securitize this issue, which will put it to the normal day-to-day politics that will restrain any authoritative actors from moving beyond the normal (democratic) rules and regulations?

This research is important in looking at the new aspect of content regulation that is generally seen from the perspective of communication or public policy studies. This study will be looking at this issue from the perspective of securitization as part of international security studies. This research is significant in looking at how information, as well as the technology behind it, can be seen as a reference object that needs to be secured as well as a source of threat against civil society. The geopolitical context of where this study is undertaken, Indonesia, is important because it has recently been in the spotlight for Internet freedom in many studies. This study will be substantial also in unpacking the utilization of securitization theory where the authoritative agency that can do the securitizing move may also take part in becoming the source of the threat. It is specifically interesting to look at this new dimension of content regulation, where allows narratives from various actors to be assessed and see how the perception of threat is established by different actors. As stated, the emergence of social media platforms and big technology companies as transnational actors that are involved in this issue also invites another interesting contribution to how platforms have influenced global politics. The balance of power and influence that these newly emerging actors have may also bring into discussion how much civil

society and government can regulate security issues that affect them. The power imbalance might be more apparent since most of the social media platforms that are being utilized by its citizens are coming from outside of the region. How do civil society, governments, activists, and social media platforms navigate this? By acknowledging and engaging various actors involved in this issue, this study is expected to contribute to bringing various perspectives into the discussion.

RESEARCH METHODOLOGY

This study will utilize qualitative methods in looking at the practice of online harmful content regulation in Indonesia. The securitization move assessed by narrative and discourse that is created and perpetuated by various actors (including government, civil society, media, and Non-Governmental Organizations) will be obtained and assessed from governments' regulations and policies, publications, articles, and reports. This step is important to obtain data on how securitizing moves are being done by each actor; highlighting their contribution to the attempt of securitization of the harmful online content. Moreover, this study will also benefit from various research and studies that have been published regarding this topic.

In assessing information security in the digital era, the constructivist approach in International Relations contributes to establishing the understanding of digital-age security by examining the use of language, symbols, and images (which includes virtuality). While most literature on information security is policy-oriented, this study will also seek to contribute to the knowledge production and critical assessment of how the discourse of "security" has evolved in digital-age security.

Conceptual Framework

This study will utilize the securitization concept as the approach to see the issue. Securitization means making an issue or aspect an "important" and "existential" issue, so that it must get different treatment from ordinary political issues and also get priority over other issues (Buzan, B., Waever, O., & Wilde, k., 1998). This securitization effort can then be institutionalized when a threat type is seen as persistent thereby increasing the urgency for addressing the issue (Buzan, B., Waever, O., & Wilde, k., 1998). The process itself allows political actors to securitize a low-security issue or situation into a high political priority that demands immediate solutions and actions.

The Copenhagen School defines the process of securitization as a speech act, in that something is considered to be done by the act of utterance (Buzan, B., Waever, O., & Wilde, J., 1998). The success of securitization depends on the audience acceptance of the speech act, a shared value on the perception of the existential threats (Buzan, B., Waever, O., & Wilde, J., 1998). The speech acts as an act of securitization is then delivered by the securitizing actor which is mainly performed by the government, political leaders, bureaucracies, lobbyists, and pressure groups (Buzan, B., Waever, O., & Wilde, J., 1998). On the other hand, referent objects are defined as "things that are existentially threatened by the issue and have a legitimate claim to survival" (Buzan, B., Waever, O., & Wilde, J., 1998). However, the Copenhagen school sees security as a negative, reflecting the failure to deal with issues of normal politics. It proposes that desecuritization is the better option, where issues are moved out of the "threat-defense sequence" into the public sphere (Buzan, B., Waever, O., & Wilde, J., 1998).

Talking about securitization, institutionalization is also an aspect that needs attention when discussing how an issue is seen as a security threat. limited ability to discuss or talk about security issues themselves. Thus, the securitization efforts that followed will only be metaphorical (Buzan, 2009). Therefore, the institutional aspect and how it plays a role in the securitization effort is an important aspect to see how the authority possessed by the actor who carries out the securitization effort influences the success of the securitization effort. Although the state remains an institution that has an important role in international relations, the functions and roles of the state can be seen as delegated through multi-level decision-making frameworks. It brings together governments, international institutions, and non-governmental organizations such as NGOs in a new, more complex form of relationship (Duffield, 2001).

This study will look into several important aspects of securitization, that is the issue that is being securitized, the securitizing moves, and also the securitizing actors. While online harmful content has become the object of securitization, this study will try to map the securitizing actors and also the securitizing moves

and the 'speech act' that have been done by the government to portray the issues as a salient threat to the national security, hence, the justification for the application of the extraordinary measure.

RESULTS AND DISCUSSIONS

Historically, the focus of online content regulation has been largely centered on the legal framework and is heavily discussed on its application in contrast to human rights issues like civil liberties and freedom of speech. This focus has been dominating the discussion of online content regulation where it often puts the government and civil society in two opposing polar (Audrine & Setiawan, 2021). Nonetheless, the urgency to tackle various harmful online content is actually in the interests of both parties. We have seen the circulation of harmful content like disinformation against specific ethnic minorities has contributed to acts of violence and mass killings like in Myanmar (Liebowitz, 2019). While the animosity towards the minority group has existed, the spread of disinformation has further fueled anger and rage towards the group, resulting in prolonged abuse and other human rights violations (Liebowitz, 2019; Grambo, 2019).

To date, there is little scholarship from International Relations and Security Studies that focuses on this issue, which is often perceived as a non-traditional security issue. In assessing online content moderation as part of a security issue, traditional positivist understandings of security, mainly focus on the Eurocentric assumptions about agency, objectivity, and what can constitute a threat or a referent object reproduce politics involving the use of force (Barkawi and Laffey, 2006:351). Nonetheless, the issue of online content regulation is very pertinent for both fields. For example, in assessing the geographical space in which International Relations actors interact and engage, cyberspace has become one domain where state and other actors extend their power and influence. Both the physical and digital worlds are becoming more interlinked than before. Moreover, non-state actors, who are represented by social media platforms and big tech companies, have also exerted a bigger power and influence within this area.

Looking at the recent Freedom House Report (2023), many Southeast Asian nations, including Indonesia, have experienced a daunting trend of restrictions against one of the aspects of civil liberties, which is freedom of speech on the Internet. Freedom of speech is in itself understood as a right that is fundamental, but not absolute, where regulations and limitations are set up to protect others' rights. This is interesting to look at in more depth, especially regarding the role of the internet as an environment where people can express opinions. In recent times, we have witnessed several cases of termination of internet access and censorship of "harmful" content in Southeast Asian countries. The cases of "hate speech" or "defamation" are often used against activists and ordinary citizens who utilize their social media platforms to voice their critics or concerns. Moreover, the definitions of "hate speech" and "defamation" are often solely subjected to the government's very own definition. Hence, this creates a sense of distrust against the government. However, we should also note that in the case of hate speech regulation, on the other hand, is also fundamental to protect individuals against racial or other identity-based hatred. Therefore, this research will try not to look at this case using the dichotomic lenses between government versus the citizen, but it will try to unpack the area where the existence of the civic space, in this case, the digital sphere, is important for all parties involved. Hence, the referent object, that is security for the people, is still salient in this issue. Discourses on security often function on these assumptions, framing communities as threats (cultural or economic) and highlighting exclusions and narratives (McDonald, 2013). This research will try to assess the case of the securitization of "harmful" online content by the government while also looking at the involvement and role of non-state actors in it. It is expected to contribute to discussions at the level of academics and policymakers regarding the regulation of "harmful" online content in Indonesia.

Online Harmful Content in Indonesia

Deriving from the Republic of Indonesia's MCI Regulation No. 19 the Year 2014 on online negative content, negative content is defined as pornography and other illegal activities based on statutory provisions relating to secrets about defense, threatening ideology, sexual immorality and exploitation, hate speech, discrimination and racial intolerance, and gambling. Therefore, the type of harm as well as the severity of the contents have its range, too. For example, a comparison between online gambling content and terrorism content, where the two share different severity in regards to national security.

Concerning terrorism, there have been several cases of the use of the internet and social media for disseminating terrorist propaganda or even recruitment for the would-be terrorists. This, in turn, has created a new phenomenon called online radicalization. Online radicalization here would be referred to as the "process whereby individuals, through their online interactions and exposure to various internet content, come to view violence as a legitimate method of solving social and political conflict" (Bermingham, 2009). An example of the success of online radicalization is the case of Dian Yulia Novi, the first female suicide bomber in Indonesia who was radicalized online through social media while she was working as a migrant worker in Taiwan (Campbell, 2014). Maura Conway describes five terrorist uses of the Internet, which are: information provision, financing, networking, recruitment, and information gathering (Conway, 2005). It is seen that the internet has added a new dimension to the group's operations by providing new tools and venues for its activities and the role of the internet is not limited to disseminating the propaganda only.

Meanwhile, online gambling activity's severity in regards to national security may not be as imminent as the terrorist activities on the internet, which may reproduce actual harm and violence in the offline sphere. Hence, there is a need for mapping the right approach to different levels of harmful content severity towards the public. Even so, the approach needs to have a degree of proportionality for the negative implication (i.e. access restriction) to outweigh the benefit (the minimum spread of the harmful content).

To date, Indonesia does not yet have any specific regulations governing harmful content in the digital realm aside from the Ministerial Regulation 19 the Year 2014 on negative sites issued by the Ministry of Communication and Information. On the other hand, based on data from the MCI, there is an indication of a delay in action from the platform in responding to MCI's report regarding dangerous content. In 2016 and 2017, there were at least 40% of content reports that had not been responded to by platform and Internet Service Providers (ISPs) (Haryanto, 2018). This statistic indicates the necessity for multi-sectoral cooperation in handling online harmful content considering there are differences in the characteristics of the circulation of content between conventional media and social media.

In contrast to traditional media where the information or content is created, controlled by, and is the responsibility of the media organization that houses it, information on social media is created and managed by its users (user-generated content). Social media users do not only use social media as a communication tool, but also to search, produce, and disseminate information (Reuter Institute, 2017). This certainly has an impact on the amount of content, the speed of distribution, and the actors who should be responsible for the content.

In Indonesia, currently, three main approaches are often utilized to handle online harmful content; 1) tech-based approach, 2) human approach, and 3) legal-based approach.

1. Technology-based approach

The application of a tech-based approach to handling online harmful content has been utilized by platforms and the government. Using Artificial Intelligence (AI), online content that is indicated to be harmful to society can be quickly taken down by using automated mechanisms such as filtering. The use of technology enables a quick and accurate takedown, thus reducing the number of individuals that access the content as well as empowering the capability of platforms to identify online harmful content. MCI also develops AI technology to filter pornographic content that circulates social media (MCI, 2018). Such a machine is called an Automatic Identification System (AIS) which in practice filters content in the coordination with National Anti-Terrorism Agency (BNPT), National Food and Drugs Agency (BPOM), and Financial Services Authority (OJK) (MCI, 2019). Detection of content that contains visual-based pornography is generally easier to categorize, identify, and takedown, which quickens the removal process. Based on the government's efforts, MCI also actively requests platforms to use AI-based technology and Machine Learning (ML) to filter online harmful content.

It can be seen that for visual and text-based harmful content which are explicit, such as pornography, gambling, and illegal drugs, technology can be utilized to detect it. Nonetheless, problems might arise when the perpetrators use specific symbols and or disguise the content with some unrelated pictures and or text. Therefore, the government and also platform need to keep updated on the behaviour of these perpetrator groups. The machine will be as good as the information that it can get for it to learn about pattern and image detection.

2. Human approach

The human-based approach emphasizes understanding the context of content and languages used by social media users. In Indonesia, the government, authorities, and platforms utilize a human approach to review online harmful content. On explicit content such as child exploitation or the use of race-based hate speech with specific languages, search engines can easily detect and takedown its circulation within social media. However, some contents require human judgment to understand its context, measure its level of hazard, and decide what kind of action needs to be done.

MCI established a fact-checking team that consists of 100 members to review suspected contents from AIS. In addition, the public can also report online harmful content through emails and social media through @aduankonten (Dewi, 2019). Throughout 2019, there have been more than 430,000 reports from the public regarding online harmful content that are processed by the MCI (MCI, 2020). These reports are then reviewed by the Content Report Team based on the Undang-Undang Informasi dan Transaksi Elektronik (UU ITE /Electronic Information and Transaction Law). Contents that are deemed to violate national law will be sent to the social media platform with a blockage request.

The law enforcement agency, in this case, the Directorate of Criminal Offence of the Criminal Investigation Agency of the Indonesian National Police, also has a mechanism to review online harmful content which also includes cybercrime. Named "Patroli Siber", the police conducts mitigation and prevention operation towards social media accounts that spread hoaxes, hate speech, provocation, and SARA (GATRA, 2019). In addition, the website patrolisiber.id is also available for the public to report different kinds of cybercrime, including the spread of dangerous content, such as child pornography, radical ideologies, etc. (Anugrahadi, 2019).

In 2021, the Criminal Investigation Agency (Bareskrim) POLRI also launched the "Polisi Virtual" or "Virtual Police" program. The virtual police are part of the Indonesian National Police at the Directorate of Cyber Crimes at the Indonesian National Police Criminal Investigation Department. However, the virtual police have a more specific objective, namely monitoring social media with the main objective of educating the public regarding the ITE Law. The prosecution of these violations will be the domain of the cyber police. The work carried out by the virtual police is divided into two stages. First, the virtual police monitor posts and if they find a post that is considered to contain elements of slander, discrimination against sexuality, religious, and racial identities, hoaxes, hate speech, especially those that violate the ITE Law and so on, they will be consulted with a team consisting of linguists, criminal experts, and ITE experts. Second, after determining that the post is a violation (in the definition of a violation of the ITE Law), the virtual police will contact the perpetrator who will give a warning to the perpetrator to delete the post within a certain period. If the individuals do not delete their posts promptly, they will then be called and interrogated by the police (KOMPASTV, 2021).

Aside from government initiatives, social media platform also employs human agents as content moderators. The ever-changing nature of social media demands this level of constant vigilance and innovation. Specific expertise is necessary to handle categories such as terrorism, hate speech, and child safety as content moderators need to understand the context of the contents that they review (Jee, 2020).

Based on the mechanisms that have been established by the government, law enforcement agencies, and platforms, the tasks of content moderators can be categorized into two: proactively filtering content that circulates online and responding to reports done by users regarding content that violates the law or platform-established community standard.

3. Legal-based approach

The legal approach is closely related to prosecutions and sanctions enacted towards the contents found through the aforementioned tech-based and human approach, as well as the category of the identified online harmful content. Specifically, there are three laws and regulations that govern online content in Indonesia, which are: Undang-Undang Informasi dan Transaksi Elektronik (UU ITE /Electronic Information and Transaction Law), Undang-Undang Pornografi (Pornography Law), and Undang-Undang Hak Cipta (Copyright Law). However, other laws regulate the limitation of information which closely related to content circulation. Based

on the report released by Lembaga Studi dan Advokasi Masyarakat (Institute for Policy Research and Advocacy) (ELSAM) in 2017, there are at least 10 laws and government regulations that regulate harmful content:

a. Undang-Undang No. 1 Tahun 1946 tentang Kitab Undang-Undang Hukum Pidana (KUHP/Law No. 1 Year 1946 on Criminal Law Code).
b. Undang-Undang No. 36 Tahun 1999 tentang Telekomunikasi (UU Telekomunikasi/Law No. 36 Year 1999 on Telecommunications)
c. Undang-Undang No. 40 Tahun 1999 tentang Pers (UU Pers/Law No. 40 Year 1999 on Press)
d. Undang-Undang No. 32 Tahun 2002 Tentang Penyiaran (UU Penyiaran/Law No. 32 Year 2002 on Broadcasting)
e. Undang-Undang 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana diubah dengan No. 19 Tahun 2016 tentang Perubahan UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE/Law No. 11 Year 2008 on Electronic Information and Transaction, as changed by Law No. 19 Year 2016 about changes to Law No. 11 Year 2008 on Electronic Information and Transaction)
f. Undang-Undang No. 14 Tahun 2008 tentang Keterbukaan Informasi Publik (UU KIP/Law No.14 Year 2008 on Public Access of Information)
g. Undang-Undang No. 44 tahun 2008 tentang Pornografi (UU Pornografi/Law No. 44 Year 2008 on Pornography)
h. Undang-Undang No 17 tahun 2011 Intelijen Negara (UU Intelijen Negara/Law No. 17 Year 2011 on National Intelligence)
i. Undang-Undang No. 28 Tahun 2014 Tentang Hak Cipta (UU Hak Cipta/Law No. 28 Year 2014 on Copyright)
j. Peraturan Menteri Komunikasi dan Informatika No. 19 Tahun 2014 tentang Penanganan Situs-Situs Internet Bermuatan Negatif (Permen Kominfo Penanganan Situs Internet Bermuatan Negatif/Minister of Communication and Information Rule No. 19 Year 2014 on Handling Internet Sites with Negative Content)

The types of online harmful content that have been regulated by the law are subject to Indonesian Law, making consequences not limited to blocking of content or account, but also legal consequences. Legal punishment that is given to perpetrators of online harmful content is based on reports that are given by the MCI, social media users, platforms, or investigations done by the police.

Securitization through Regulation: The Case of ITE Law 2016

Drawing upon the cases and approaches that have been taken by the government, this study seeks to understand the current government approach using the lens of securitization. The securitization approach believes that security is not fixated, as any issues can be utilized by political entrepreneurs to justify extraordinary measures if being put as a security issue. The act of labeling issues with 'dangerous', 'alarming', and so forth by securitizing actors can move the issue 'beyond politics'. This means that, dealing with the issue, as in any other emergency measure, governments have the permission to deal with it in a non-democratic way, where the values of citizens' rights might not be that of importance vis a vis the national security.

In assessing the government's approach to handling harmful online content, it has been clear that the securitization move has become the dominant approach that is being taken by the government. Firstly, content that is deemed harmful or negative, such as pornography, defamation, hate speech, etc. has been stipulated in the MCI Regulation Number 19. In this case, the term "negative" has put the issue into a higher level of notice. Secondly, in handling the issues, the government's move, especially by putting measures that is under the ITE Law No. 40, which mentions "The government protects the public interest from all kinds of disturbances as a result of the misuse of Electronic Information and Electronic Transactions that disrupt public order, under the provisions of laws and regulations." Legal protection for the public is even regulated as an obligation of the Government by preventing the spread of fake news by blocking or cutting access as contained in Article 40 paragraph (2a) of the ITE Law which reads: The government is obliged to prevent the dissemination and use of Electronic Information and/or Electronic Documents which has a prohibited load under the provisions of the legislation. Article 40 paragraph (2b) of the ITE Law reads: "In carrying out the prevention as referred to in

paragraph (2a), the Government has the authority to terminate access and/or order Electronic System Operators to terminate access to Electronic Information and/or Electronic Documents that have unlawful content."

However, there have been several cases where the act to move the issue into a security issue, is being widely criticized and questioned by citizens, human rights activists, and the media. For example, in June 2019, the Indonesian government temporarily limited access to social media for three days following violent post-election protests in Jakarta. The government claimed the move aimed to stop the spread of disinformation that could worsen the violence (Tehusijarana, K.M. & Valentina, J., 2019). Social media, indeed brings the challenge of information circulation to another level, where it will be difficult for the government to curb the information flows. Nonetheless, this move has been widely criticized by human rights activists and citizens as well for limiting individuals' freedom of speech and access to information. Another case of the limitation of freedom of expression would be the case of cyber patrol, which focuses a lot on cases of defamation and hate speech. A study that is released by SAFE.net based on data from the patrolisiber.id web stated that from 2017-2020 there were around 39% of the 15,056 cases investigated by the cyber police related to defamation and hate speech (Juniarto, 2021). Moreover, the rate of cases that are being investigated by the cyber police shows a disproportionate number of reports that are coming from ordinary citizens vis-a-vis powerful groups or individuals (governments, private institutions, etc). The percentage of reports coming from ordinary citizens is only 23% and the rest, who come from groups that have power, 68% (Juniarto, 2021). This fact may signify that this regulation of UU ITE may only benefit those in power and further suppress ordinary citizens' freedom of speech and expression.

CONCLUSION

Drawing from the cases of securitization approach dominance on how the government tackles online harmful content, this study offers another approach to moving the issue into the day to day politics, in which, citizens' inputs and concerns, as well as other stakeholders that are concerned, can be incorporated into a move towards the perseverance of digital safety as well as freedom of expression. The very regulation that once became a tool for protecting the citizens, the ITE Law 2016, has now manifested into becoming a source of threat for the citizens as well. The duality of this regulation has to be addressed, and therefore, the call for a revision of the regulation must be made to ensure a better policy. The government must also engage with communities, private enterprises, and academics, who are going to be the subject of the regulation to ensure the feasibility and applicability of the policy and regulation. The government and all related stakeholders need to work hand in hand not only in the course of punishment or sanctions against unlawful behavior (the spread of harmful online content), but also in a move towards prevention and education. There is a dire need for better access to education, especially digital literacy for all citizens. Preventive measures are important to address the issue even before the events occurred. The application of several measures such as regional blocking, access limitation, or content take will not be needed as much if all parties involved have aligned objectives and visions in creating a safe digital space for all.

REFERENCES

Adam Bermingham, et.al., "Combining Social Network Analysis and Sentiment Analysis to Explore the Potential for Online Radicalisation", Conference Proceeding in 2009 International Conference on Advances in Social Network Analysis and Mining, p.2.

Anugrahadi, A., (2019, August 15), Polri Luncurkan Patrolisiber.id, untuk Mudahkan Masyarakat Lapor Kejahatan Siber [daring], Liputan6.com, https://www.liputan6.com/news/read/4038070/polri-luncurkan-patrolisiberid-untuk-mudahkan-masyarakat-lapor-kejahatan-siber.

Buzan, B. (1991). People, States, and Fear, An Agenda for International Security Studies in The Post-Cold War Era, (2nd ed), Colorado, Lynne Rienner Publishers.

Buzan, B. H. (2009). The Evolution of International Security. Cambridge: Cambridge University Press.

Buzan, Bary, Waever, Ole, de Wilde, Jaap, (1998). Security: A New Framework of Analysis, Lynne Rienner, London.

Belle Wong, J. D. (2023, August 7). Top social media statistics and trends of 2023. Forbes. https://www.forbes.com/advisor/business/social-media-statistics/#:~:text=In%202023%2C%20an%20estimated%204.9,record%204.9%20billion%20people%20globally.

Charlie Campbell, "ISIS Unveiled: The Story Behind Indonesia's First Female Suicide Bomber", TIME, 3 March 2017, viewed 10 August 2017, < http://time.com/4689714/indonesia-isis-terrorism-jihad-extremism-dian-yulia-novi-fpi/>

Conway, Maura, 'Terrorist "Use" of the Internet and Fighting Back', Oxford Internet Institute, paper presented on the Conference Cybersafety: Safety and Security in a Networked World: Balancing Cyber-Rights and Responsibilities, 8-10 September 2005, pp. 1-34.

Eka, R. (2018). Hoax Distribution through Digital Platforms in Indonesia 2018 [online] DailySocialID. https://dailysocial.id/post/laporan-dailysocial-distribusi-hoax-di-media-sosial-2018.

Freedom House (2023). Freedom on the Net 2023: Indonesia [online]. Freedom House. https://freedomhouse.org/country/indonesia/freedom-net/2023

GATRA, (2019, June 19), Kepolisian Jelaskan Tahapan Patroli Siber [online]. GATRA. https://www.gatra.com/detail/news/422851/politik/kepolisian-jelaskan-tahapan-patroli-siber.

Gil de Zúñiga, H., Jung, N., & Valenzuela, S. (2012). Social media use for news and individuals' social capital, civic engagement, and political participation. Journal of computer-mediated communication, 17(3), 319-336.

Haryanto, A., 2018, Menkominfo Ungkap Alasan Twitter dkk Tak Diblokir Seperti Tumblr [online], Detik.com, https://inet.detik.com/law-and-policy/d-3905290/menkominfo-ungkap-alasan-twitter-dkk-tak-diblokir-seperti-tumblr

Hirschauer, S. (2014). The securitization of rape: Women, war and sexual violence. Springer.

Statista. 2023. Number of internet and social media users worldwide as of July 2023. [online], Statista, Available at: https://www.statista.com/statistics/617136/digital-population-worldwide/

Jee, C., 2020, Facebook needs 30,000 of its own content moderators, says a new report [online], Technology Review, https://www.technologyreview.com/2020/06/08/1002894/facebook-needs-30000-of-its-own-content-moderators-says-a-new-report/

Juniarto, Damar., 2021. Penindasan Teknologikal (Technological Repression) terhadap Aktivisme Digital di Indonesia. [online] <https://www.youtube.com/watch?v=z4XGEDCndp0&t=6755s>

KOMPASTV, 2021. Eksklusif, Masuk ke Dapur Polisi Virtual - AIMAN. [video] https://www.youtube.com/watch?v=I1NeJ2jasQs

Linke, A. & Zerfass, A. 2013. Social Media Governance: regulatory frameworks for successful online communication. Journal of Communication Management. Vol 17. No 3. pp. 270-286. DOI. 10.1108/JCOM-09-2011-0050.

Reuter Institute for the Study of Journalism. 2017. Digital News Report 2017 [ebook]. Reuters Institute. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/Digital%20News%20Report%202017%20web_0. pdf, 11.

Shao, Chengcheng, Ciampaglia, Giovanni, Flammini, Alessandro, & Menczer, Filippo 2016, Hoaxy: A Platform for Tracking Online Misinformation, Proceeding at the International World Wide Web Conference WWW'16 Companion, http://www2016.net/proceedings/companion/p745.pdf

Tehusijarana, K.M. & Valentina, J., 2019. Jakarta riot: Government temporarily limits access to social media, messaging apps, https://www.thejakartapost.com/life/2019/05/22/jakarta-riot-government-temporarily-limits-access-to-social-media-messaging-apps.html.