Society

Society, 10 (2), 489-502, 2022
P-ISSN: 2338-6932 | E-ISSN: 2597-4874
https://society.fisip.ubb.ac.id

The Legality of Devious Cyber Practices: Readiness of Indonesia's Cyber Laws

Sardjana Orba Manullang
Department of Law, Faculty of Law, Universitas Krisnadwipayana, 13077,
Bekasi, West Java Province, Indonesia
Corresponding Author: somanullang@unkris.ac.id

ARTICLE INFO

Publication Info:
Research Article

How to cite:
Manullang, S. O. (2022). The Legality of Devious Cyber Practices: Readiness of Indonesia's Cyber Laws. Society, 10(2), 489-502.

DOI: *10.33019/society.v10i2.482*

Received: September 22, 2022;
Accepted: December 16, 2022;
Published: December 30, 2022;

ABSTRACT

The ever-expanding Indonesian cyberspace has ushered in significant economic growth to the country's online business and e-commerce. This is due to the country's rising internet penetration rate of 73% of its total population, with about 204 million people connected to the internet. This high connectivity has brought about several positive socio-economic opportunities but with other thorny issues like cybercrime, misinformation, cyber-induced intolerance, disinformation, trolling and cyber warfare. Despite the Indonesian government's intervention with measures to regulate cyber activities, some devious cyber practices undefined in legal literature continue to be practiced, even passed as legitimate, sometimes leading to negative consequences. These practices are often conducted as organized operations that target populations to create mistrust and polarize the targeted population. Some are crafted as cyber warfare declared by entities within a country or from a foreign country targeting another's populace, which poses a threat to social order. This paper explores these devious cyber practices and their strategies and mitigation possibilities. A sociological research approach coupled with the use of law enforcement theory was applied to study and analyze Indonesia's cyber security law enforcement policies, the Internet and Electronic Transaction (ITE) Law, the Criminal Prosecution Act, the Constitutional law, civil society actors and private sector actors on cyber security. Indonesian law and international law, coupled with available technology, were reviewed for readiness to address threats posed by these devious cyber issues to social order. Measures taken by the Indonesian government are in readiness to combat these cyberspace issues in its jurisdiction but also present more questions on the proposals for reviews to the legislation and

introduction of content monitoring systems, which risk being inappropriately deployed in censorships or suppression of legitimate freedom of expression.

Keywords: *Censorship; Cyber Policy; Cyber Warfare; Indonesian Cyber Law; Indonesian Law*

1. Introduction

Indonesia's cyberspace from October 2016 to April 2017 was filled with cyber activities and material that substantially led to the country's largest-ever protest rally. A series of protests in Jakarta started in mid-October 2016 following a video posted and shared online (Lim, 2017). The resulting events included the biggest mass street protest in the history of Indonesia and the arrest and eventual imprisonment of Jakarta's sitting governor (Mietzner & Muhtadi, 2018). Activities that substantially led to these played out in cyberspace especially social media, messaging apps and websites. The intentions of these cyber activities, whether devious or not, could sway a supposedly independent justice system, change the political landscape, reinforce existing social divisions and disrupt public order (Nuryanti, 2020; Paterson, 2019).

Indonesia's cyberspace is among the busiest in the world, with the biggest e-commerce in southeast Asia; similarly, it has one of the most active social media. With this high connectivity, Indonesia has had remarkable economic opportunities marked by increased economic growth, with a substantial portion directly tied to online activity (Manullang, 2021a; Nugraha & Putri, 2016; Paterson, 2019). The same opportunities are presented in the socio-political landscape. Many formally politically disengaged Indonesians, mostly from the middle class, have increasingly engaged in social and political conversations as the internet presents better platforms for free expression. The freedom of expression has also enabled an increased flow of negative information created and disseminated purposely to amplify contentious, polarizing, and even intimidating issues. For a country with much diversity and a history of divisive politics along religious, tribal, ethnic, and racial lines, the internet is being actively used to amplify and perpetuate these divisions (Lim, 2017; Toha et al., 2021). Some activities to this end even claim legitimacy depending on how, where and when they are done and or if those engaged in the practices have the backing or connections to the powerful and those in authority (Gaidosch, 2018; Tyson, 2021).

Such devious cyber practices continue to elude the local and international law of many countries (Lubin & Townley, 2020). The Indonesian authorities put policy and legal measures to regulate cyberspace with more revisions to the proposed legislation. The Indonesian government, civil society, academia, and private actors have been combating negative cyber practices (Manuhutu et al., 2021; Manullang, 2020; Nugraha & Putri, 2016). Some of the measures in place and proposed are under scrutiny for their possibility of authorizing censorship, infringement on rights to free expression, privacy and against democratic values (Paterson, 2019).

In this study, we examine the readiness of Indonesian cyber law to address practices of concern in its cyberspace by exploring the Indonesian Cyber policy the Cyber Legislation. To better understand the devious nature of some cyber practices in Indonesia's cyberspace, we will analyze the country's socio-political issues that are historically shaped by divisive, exploitative

https://doi.org/10.33019/society.v10i2.482

politics and how they are being impacted as they get magnified by the increased internet connectivity. We will examine the threats posed by these issues to the country's budding democracy and the government's policy shifts in response to these issues.

2. Increased Connectivity, Economic Growth, and Liberalism

A significant portion of Indonesia's expanding economy is attributed to online-based activity and e-commerce, as evidenced by huge investments in the sector by e-commerce giants such as Alibaba, JD.com, and Google (Jurriëns & Tapsell, 2017; Ramli, 2020). A projection of Indonesia's economic growth curve points toward the country becoming among the top largest world economies in purchasing power by 2050 (Nehru, 2016; Paterson, 2019).

This e-commerce growth is powered by increased connectivity, with over 204 million people connected to the internet, especially via mobile connections (Chen, 2020; Manullang, 2020). Affordable data plans have led to Indonesians' exponential use of social media (Manullang, 2020; Ramli, 2020). Ranked as the highest in phone use, averaging up to 180 minutes of screen time daily (Amin, 2014), Indonesians are also among the top-rated active users of Twitter and Facebook (Paterson, 2019). In addition to e-commerce and social media, government, civil society and academia have significantly adopted online service delivery even in rural areas. The government's public feedback tool about its service delivery rating, called LAPOR, was launched to encourage transparent and accountable public service delivery (Dini et al., 2018; Manullang, 2021b).

Despite the increased connectivity, opportunities, social engagement and government efforts, problematic issues of cyber security and cybercrime, unbalanced connections between rural and urban areas still afflict Indonesia's cyberspace (Manuhutu et al., 2021; Manullang, 2021b; Setiawan & Suhartomo, 2019; Setti & Wanto, 2019). What is more low digital literacy and know-how among certain sections of the population exclude them from taking advantage of the opportunities presented by digital connectivity? Moreover, low digital connectivity literacy renders many more susceptible to devious cyber practices, cybercrime victimization and disinformation, which disrupt social order.

3. Devious Cyber Practices

Many devious cyber practices claim legitimacy (Manning & Agnew, 2020; Payne, 2018). In this section, we examine social media manipulation through Trolling, called locally in Indonesia called, 'Buzzing', but the focus will be on double-sided trolling. In other studies, it is referred to as rabble-rousing, which has eluded legal classification (Lubin & Townley, 2020). Social media manipulation in Indonesia has its foundations in the history of the country itself and was perpetrated by the state propaganda machinery of those eras as a means of controlling wider social discourses, weaponizing diversity to sow paranoia and setting the scene for authoritarianism (Berting, 2019; Shah & Taylor, 2021). The fall of authoritarianism in Indonesia ushered in democratization, which came with the freedom of expression that was accelerated by the coming of the internet and digital media. The social media scene exploded with activity with the prevailing democracy that tolerated the previously suppressed freedom of expression. However, the old habits of manipulating the narrative through popular media were now part of the social psyche. Anyone could carry them out, not only those dominated by the state machinery like in the past. This gave rise to social media troll factories' and 'cyber armies' that manipulate the narrative on social media on behalf of many parties, especially for political and socio-economic ends (Sastramidjaja & Wijayanto, 2022).

https://doi.org/10.33019/society.v10i2.482

The 2012 Jakarta gubernatorial elections kicked off the large-scale use of 'cyber teams,' notably 'buzzers'/trolls in political campaigns. The trend was set, and many subsequent political activities have recruited such cyber teams to push their agenda (Nuryanti, 2020; Sastramidjaja & Wijayanto, 2022). The heightened cyber activity of this nature has become part of daily life for Indonesians, often yielding real online and offline consequences (Lindsey & Pausacker, 2016; Lim, 2017). Much as this kind is cyber activity could be constructive such as an increase of political participation and free expression, much of it has resulted in amplified divisions and disrupting order, and even influencing the justice system like in the case of the imprisonment of Ahok the sitting governor of Jakarta (Lim, 2017; Berting, 2019).

The devious nature of trolling is often designed to intentionally sow negativity, which leads to negative consequences, yet prosecutions for trolling are rare or nonexistent. This could be partly due to the connection of the trollers to powerful entities in authority. A Muslim hacker activist group used social media to amplify religious intolerance (Tapsell, 2021). It stole targeted people's (perceived as insulting Islam) personal information and published it online (Paterson, 2019; Berting, 2019). There have been indications of links between powerful political parties and the Indonesian military (Paterson, 2019; Boyle, 2020).

4. Trolling/Buzzing

Online social network users lately have to grapple with trolling. Much as trolling has negative and positive classifications, this study focuses on the negative troller that practitioners particularly identify as a Hater (Hodge & Hallgrimsdottir, 2020; Horse et al., 2021). In this light, the term has been used to mean intentionally posting provocative, offensive or menacing messages through a communications network. This definition clearly illustrates the devious nature of trolling, yet it is an activity by many, including those in authority. Trolling continues to elude the law, even in some instances claiming legality and passing on as 'free speech' or 'art' as in the case of Elonis Vs. the United States (Reichel, 2019; Roark, 2015).

A common example of trolling in Indonesia is the 'cyber troops' locally referred to as 'buzzers' (Sastramidjaja and Wijayanto, 2022). The available literature on the subject holds that a buzzer amplifies certain points of view opinions on given issues or brands to reach a broader audience (Lim, 2017; Sastramidjaja & Wijayanto, 2022). The buzzing phenomenon in Indonesia became popular in 2009, with main influencers paid to promote products and brands, and it exploded during the 2012 gubernatorial elections in Jakarta (Neyasyah, 2020; Syahputra, 2019). Political candidates on all sides recruited and paid teams of buzzers to push their side of the political agenda. Of course, how the buzzers did was up to the creativity of the buzzer. The creativity in trolling often involves putting out material that will attract the most attention. Indonesian politics meant amplifying divisive opinions along religious, cultural, ethnic, racial and economic lines. After the blasphemy accusations against Ahok, the Jakarta governor, in 2016 and the subsequent demonstrations that led to his arrest and imprisonment, cyber activity was flooded with divisive material put out on the internet and amplified by trolls. Anti-Ahok material circulated was, for instance, critical of his Chinese ethnicity, which denotes being a foreigner and communist; his Christian faith was touted through radical Islamist tones as an infidel (Lim, 2017; Ong & Tapsell, 2021). The other side also pushed distorted facts about Ahok's opponent; Anies accused him of being linked to several corruption incidences and made absurd accusations that he had intentions of introducing sharia law and being cheered on by Iranian Shia groups. Such material drowned out alternative opinions and created a highly charged polarized atmosphere that spilled out of cyberspace into communities and homes, turning people against each other.

https://doi.org/10.33019/society.v10i2.482

5. Double-sided Trolling (Rabble-rousing)

Having eluded the spotlight of extensive scholarly analysis is a very cruel and treacherous devious way of planting disharmony among the populace is the habit of "playing on both sides" on the internet (Fichman & McClelland, 2021). Practitioners who have studied this practice refer to it as 'rabble-rousing' (Lubin & Townley, 2020). For this study, we shall refer to it as 'double-sided trolling,' which involves organizing and coordinating operations to amplify a divisive issue by supporting both sides. To better grasp the practice, we will draw from examples from both the local and international scenes.

Locally, double-sided trolling manifested more in divisive, politically oriented issues. Back to the Ahok-Anies Jakarta gubernatorial campaign and the blasphemy incident, double-sided trolling was practiced by groups that operated different websites, which amplified divisive material in opposition to each other as operating similarly on social media. For example, arrahmah.com posted anti-Ahok material while its spoof arrahmahnews.com posted pro-Ahok material. The same was with VOA-islamnews.com, a knock-off of VOA-islam.com, and pkspuyengan.com, a spoof of the currently defunct pkspiyungan.com (Lim, 2017). Setting aside the ideological intentions of these double-sided trolling practices, their actions aim to plant disharmony in Indonesia's young democracy (Lubin & Townley, 2020). The trollers play both sides in such instances, making the Indonesian populace victims.

Internationally, the most notable instances of double-sided trolling played out in the United States cyberspace. Trolls played both sides by amplifying divisive issues, such as in the 2016 presidential elections between Trump and Hillary Clinton and the U.S. Vaccination mandate debate in 2020, which were blamed on Russian double-sided trolling to sow disharmony and undermine U.S. democracy (Broniatowski et al., 2018). In Germany, Russian double-sided trolls were said to have played both on the side of 'the far-right' and actively on the side of 'the left-wing anti-fascists, reaffirming the stance of analysts who assert that Russia intends to plant disharmony in western democratic countries. Similarly, analysts have pointed out that China has thousands of paid operatives, a.k.a. 'the 50-cent army,' whose task is to manipulate common belief through devious cyber practices such as social media interactions (Lubin & Townley, 2020).

6. Threats Paused by Double-Sided Trolling

The gist of the matter in double-sided trolling is its ability to simultaneously amplify contradicting issues. The double-sided nature of this kind of trolling, coupled with its mass production and dissemination, which sometimes involves bots while hiding their real intentions inflict real assaults on social harmony, disguising it as legitimate expression. The devious intentions of these practices do not offer any good to society.

The practice can destabilize wider communities, and therefore worth paying attention to its destructiveness. It stealthily intrudes on public discourse and contaminates genuine views and opinions, thereby adulterating the fundamental domains that enable the proper functioning of a democratic process (McGonagle et al., 2019). Double-sided trolling exploits polarizing elements in a community, driving people into embracing more divisive and extreme stances (Clark & Aufderheide, 2011). Studies have shown that social media algorithms are configured to accelerate social polarization (Paterson, 2019).

The double-sided trolling practice of amplifying divisiveness seriously threatens a young democracy with varied diversities like Indonesia, as it undermines the vulnerable issues of promoting an open society with freedom of information flow, free expression and discussion of conflicting issues and identities (Fichman & McClelland, 2021).

https://doi.org/10.33019/society.v10i2.482

From the international legal setup perspective, the essence of international law is in connecting countries in a coalescence around common values, collaboration and peace. Therefore, practices grounded in absurd intentions of driving groups, communities and individuals further apart contradict the idea of 'peace with one another' as expressed in the United Nations Charter (Lubin & Townley, 2020).

7. The Legality of Some Devious Cyber Practices

Most devious cyber practices may be placed in obvious cybercrime categorizations like disinformation, fake news, hacking and the like. However, trolling continues to evade all forms of legal categorization despite its destructive consequences. Being practices carried out in cyberspace, the challenges of finding the perpetrators or proving the illegitimacy of the practices are enormous.

The exploration of elements of Indonesian law and international law on this problematic issue of double-sided trolling is limited to a few principles, most of which are international law domains. These domains include prohibited coercive intervention, sovereignty, and self-determination. National and international law domains include human rights, freedom of expression and subversive activities. The illegality of these devious cyber practices can be conceptualized through these domains of law. Measures put in place and suggested for cyber policy and cyber law review in Indonesia are problematic in certain instances, ironically manifest as draconian measures that risk victimizing the very populace it is protecting (Ong & Tapsell, 2021).

8. The International Paradigm

8.1. The Principle of Non-intervention

Ordinarily, the principle of non-intervention intuitively connotes the implication that the devious cyber practices "intervene" in other people's matters. Through the lens of prohibitions attached to intervention in others' affairs, double-sided trolling is an act of interference. Practitioners point out that coercion must be proven to designate non-intervention as illegal (Lubin & Townley, 2020). Coercion as an element in law is a determinant in the legal principle of non-intervention. But again, trolling exploits existing discourse and technological systems to interfere in and or calculatedly pollute online discourse. As devious as this practice may be, it usually does not manifest as coercive or take over the functioning of anything.

8.2. Subversion

People have the right to self-determine. Local and international law recognizes people's right to decide on matters that affect their destiny and have the freedom to engage in political, economic, cultural and social activities without interference (Castellino, 2021). Subversive activities interfere with these freedoms; subversive propaganda is described as information intended to undermine the functioning of institutions by influencing a population toward an uprising or insurrection (Breitenbauch & Byrjalsen, 2019). The destabilizing nature of double-sided trolling could fit within subversive activities. Moreover, spreading subversive propaganda is a legal prohibition in local and international law. However, this may not be the case if the trolling only amplifies already existing issues, but again this amplification helps keep the activity alive and fulfilling its intended purpose.

https://doi.org/10.33019/society.v10i2.482

8.3. Human Rights

The broad nature of defining the right to free expression presents a challenge in designating trolling as legal or illegal. The broad definition international bodies on human rights law have put on freedom of expression includes the right to seek, receive and impart information and ideas of all kinds regardless of frontiers (Farsi et al., 2018). All kinds of frontiers are further expounded to refer to all kinds of ideas and opinions that can be transmitted to others through all kinds of media and methods of expression (Howie, 2018; Lubin & Townley, 2020). Many devious cyber practices capable of masquerading as genuine free expression manage to gain legal protection and even claim legitimacy as free expression. Double-sided trolling and other devious cyber practices receive less policy regulation because of the strong legal protection afforded to freedom of expression. In this light, cyber practitioners, academia and civil society in Indonesia share the view that the government measures to combat issues in its cyberspace have problematic legislative reviews, and automated content moderation could be a tool for censorship and suppression of free expression (Paterson, 2019; Ong & Tapsell, 2021).

9. Readiness of the Indonesian Cyber Policy and Laws

The huge benefits to the Indonesian populace of the internet are undeniable, and so are the disadvantages and threats. The national and international laws in their current form do not provide satisfactory legal solutions to the problem of devious cyber practices such as double-sided trolling. The phenomenon eludes capture even under the principles of non-intervention and self-determination. The same is true of subversive propaganda prohibitions, which may not offer substantive workable measures against a problem like trolling. The insufficiency of legal solutions calls for consideration of non-legal measures to address such cyber practices. The Indonesian government, civil society, academia and private sector are players in efforts to address negative cyber activity in Indonesian cyberspace.

9.1. Legal Landscape on Cyber issues in Indonesia's Cyberspace

The main legislation on cyber issues in Indonesia is the Electronic Information and Transactions (ITE) Law (2008) (Nugraha & Putri, 2016). This law was reviewed in 2006 to cater to cybercrime and also empowered officials with the power to block what is deemed as prohibited material. Articles 27 to 36 of the ITE Law stipulate the provisions for prohibited cyber-related acts (Siregar & Lubis, 2021).

9.1.1. Legal Elements of Cyber Issues

Evidence: Article 42 of the ITE Law also provides for conducting investigations in line with Article 183 of the Criminal Prosecution Procedure (Fernando et al., 2022). As such, the system of determining evidence adopted follows the theory of evidence where rulings follow the syllogistic form of reasoning, which experts have critiqued as not contributing to the knowledge of the truth (Sommer, 1997). Given that evidence should be based on provisions of the law, it is required to be recorded and submitted as evidence in a court of law following the provisions of Article 184 of the Criminal Prosecution Procedure, which requires the following:

Witness Testimony: This is expected to be delivered following the provisions of the Criminal Prosecution procedure and executed under oath and in fulfillment of the following requirements (Arimuladi, 2022).

- Free of fabrications, opinions and expert views.
- Align with the principle of '*unus* testis *nullus* testis' the existence of more than a single witness.

https://doi.org/10.33019/society.v10i2.482

- Witness testimony is not reliant on hearsay.
- Consistency of information among the witnesses.

The nature of cyber practices, which occur entirely in cyberspace, makes it difficult or impossible to attain usable witness testimony in a legal matter. The witness testimony here could only be hearsay, which can only be taken under the condition of '*testimonium di auditu*'. Much as it is not directly considered as evidence, it may be instrumental in attempts to strengthen the stance of the case (Amin & Huda, 2021; Pujoyono, 2020).

Experts' opinion: Involving an expert in the field under review, capable of clearly elaborating issues about the case/matter. Must be able to give compelling statements that reflect an impartial opinion on particular aspects of matters within his expertise that are in dispute (Harahap et al., 2019).

Documentation as evidence: Many kinds of documents are recognized as evidence if authenticated. Provisions for documentation as evidence are stipulated in Article 184, clause C and article 187 of the Criminal Prosecution Procedure (Asmara et al., 2019).

Defendants' statements: This is provided for in Articles 189 and 184 of the Criminal Prosecution Procedure, where the defendants make statements and narrations about their actions and what they experienced (Balo et al., 2020).

9.2. Law Enforcement on Cyber Issues

Following the emergence of cyber issues, policy strategies aimed at preventing, eliminating and mitigating cyber-related issues were implemented in individual countries and on the international scene. Cyber law is one of the elements crucial to implementing cyber policy strategies, which cannot work on its own but in tandem with other strategic policy elements to address cybercrime (Amin & Huda, 2021). This was in line with deliberations of the United Nations Congress, which explored possibilities of using policies geared towards regulating cyber activities and practices to address cyber crime in conjunction with individual countries' criminal law (Rajput, 2018).

9.2.1. Punitive Approach

The penal approach to cybercrime and other cyber practices in Indonesia is being implemented. There have been several prosecutions related to the cyber activity. Most of the cases were related to straightforward criminal activity, such as fraud and theft through hacking; others were prosecuted as defamation cases. However, criminal law is often not taken as an ideal policy instrument for addressing devious cyber practices but rather as a tool of strategic importance in such an effort. Practitioners have put forth the idea of discussing cyber issues with the harmonization of existing cyber laws with a focus on criminalizing certain activities in cyberspace, paying attention to procedural approaches and considerations in constitutional law (Schallbruch & Skierka, 2018; Amin & Huda, 2021).

9.2.2. Non-punitive Approach

The idea of preventing devious cyber practices without a punitive approach in Indonesia has to involve more of taking preventive measures. Such measures could address a combination of factors that may lead to indulgence in devious cyber practices by talking about socio-legal phenomena that may lead to such practices (Paterson, 2019; Tapsell, 2021). Societal digital literacy efforts come in handy at this point. In harmonizing cyber laws and constitutional law, efforts can be undertaken to minimize negative cyber practices by identifying aggravating

https://doi.org/10.33019/society.v10i2.482

factors to such practices (Lim, 2017). However, the effectiveness of non-punitive efforts in dealing with the prevalence of negative cyber practices remains uncertain, but what is certain is that issues committed in cyberspace require global vigilance as they transcend territorial borders and could have consequences in any country (Lubin & Townley, 2020).

10. Technology and Government in Curbing Devious Cyber Practices

At least in its current versions, Indonesian and international law do not adequately address the issue of devious online practices. In the international realm, principles of non-intervention in other country's affairs or a nation's right to self-determination and safeguarding territorial sovereignty do not deter negative online practices. Prohibitions on transboundary harm, for instance, are more symbolic than practical in their ability to lessen the risks associated with cross-territorial online devious practices. Without proper legal remedies, countries could consider resorting to extra-legal methods to safeguard their society and aggressively combat the destabilizing effects of online actions like buzzing/ double-sided trolling. The many technological methods that may be employed to counter devious online practices are examined in this section.

Understanding the specific technological changes to our information is vital before considering what solutions may be beneficial. Without the aid of the information technology landscape, a phenomenon like trolling/buzzing could not have emerged. The dominance of the internet and social media in today's significantly transformed information and communication landscape directly contributes to devious online practices (Lubin & Townley, 2020). Decades ago, possessing a printing press was the sole realistic method of mass communication, and public discussion was done very differently. Common online negative practices are a phenomenon that could not happen in those conditions.

The public actions and debates of Internet users throughout the world are currently accessible, making it simple for actors to examine the cultural and socio-economic distinctions that are ripe for negative actions like double-sided trolling. Anybody may now instantaneously access a national audience since communication obstacles linked to offline paper-based communication and mass media have been greatly reduced. Determined and well-funded players can flood public discussion forums with data to sway discussions in their favor. Additionally, we have direct access to people owing to targeting techniques created for advertising. As a result, some actors are well-equipped to influence different demographic segments of a targeted community, often with devastating results to the community.

Devious cyber operatives are protected by anonymity. Many popular platforms have given up on using one's real name as a means of official identification. Users are not required to disclose any information about their physical identity while using various online platforms for communication, including posting reactions on news websites with feedback commentary capabilities. Clouded online identities make it harder for law enforcement to make a formal identification and allow devious online practices to deceive normal internet users into thinking there has been an unplanned rise in public opinion.

Sensitive, contentious, misleading and predatory material has been shown to spread. However, news feeds and curating algorithms are used (Tenove et al., 2018), which are necessary for organizing enormous amounts of internet content online that users can access more quickly. According to experts, content recommendations may steer users to more controversial or radical content than they were seeking. Others have shown that, despite most social media users being moderate, tiny, but extremely active, communities post and share links

https://doi.org/10.33019/society.v10i2.482

to manipulative and exploitative websites and are responsible for the most viewed online content.

Most popular platforms are designed to boost participation and generate revenue, leaving them vulnerable to trolls rather than providing structured, productive forums. This enables bad actors to frame sensitive issues in controversial ways that might become viral, giving them power over matters often debated in public.

Realistic solutions to these vulnerabilities are exceedingly difficult to put into practice. Divergent opinions exist on the subject matter of digital literacy. According to research, those with less digital literacy are more prone to manipulation since they are less able to evaluate the validity or origins of digital communications. Practitioners assert that blaming individuals rather than governments, tech companies, and Internet service providers would be inappropriate. Others argue that the only way to lessen the incidence and effects of online negativity like harassment campaigns is through technology providers; given their proximity to the problem and the rapid pace of technological advancement, they can develop ways to detect devious users and warn vulnerable users.

In the absence of, or in addition to, any effective long-term solutions, states may be obliged to respond by establishing proactive organizations dedicated to combating misleading information campaigns. These institutions might, if badly implemented, only serve to escalate public anger toward a system that is already inadequate at combating disinformation. The Indonesian government's internet monitoring initiatives, which were set up to decrease sneaky online behavior, have drawn criticism for their propensity to infringe on freedoms of expression while failing to stop hate speech from particular groups in society. These policies are seen as effective tools that support nations in their vigorous battle against misinformation and push their implementers toward dictatorship.

Some nations rely on digital literacy efforts and public awareness campaigns to raise awareness of harmful internet impacts. Experts agree that developing and sustaining constructive conversation is the best response rather than vigorously disputing the facts. Additionally, many nations have established institutions to preventively address negative online activities.

11. Conclusion

Given the distinctive elusiveness and contradictory character of devious online practices, the feasible options to address it is with the use of technology and the law, considering the importance of international multi-faceted collaborative initiatives on the same. It is challenging to identify a workable international legal framework that would permit the corrosive characteristics of devious online practices, such as double-sided trolling, to be categorically considered illegal, as is the case with amplification activities more broadly. Even if it may be challenging to do so legally, there are reasons to feel that devious online practices such as double-sided trolling and buzzing should not continue existing without being tackled by both local and international legal frameworks. The contradictory nature of double-sided trolling in the context of the human right to free speech leads one to believe that it does not have many expressive benefits deserving of protection. Double-sided trolling is made feasible by many significant changes in our informational environment brought about by technological advancement. Given the absence of legal remedies, states seeking to thwart the practice and lessen its negative impacts may need to consider technological alternatives. This paper creates the opportunity for more effort on several fronts. It sheds light on the importance of legal reviews and international collaboration on conceptual issues that address the distinctively

https://doi.org/10.33019/society.v10i2.482

destructive characteristics of online devious practices and operations of the same kind in the digital age, such as double-sided trolling and buzzing. The importance of conducting concentrated research into the effectiveness of various technology tactics to fend off devious online practices and other divisive online information operations has to be highlighted. Theorists and technologists should collaborate to advance these two goals since they should be pursued simultaneously.

12. Acknowledgment

The author is grateful to express gratitude to all of those who have had the pleasure to work during this research conducted.

13. Declaration of Conflicting Interests

The author has declared no potential conflicts of interest concerning this article's research, authorship, and/or publication.

References

Amin, K. (2014). Indonesians Spend most Time on Smartphones in the World. The Jakarta Post, June 5. Retrieved from https://www.thejakartapost.com/news/2014/06/05/indonesians-spend-most-time-smartphones-world.html

Amin, M. E., & Huda, M. K. (2021). Harmonization of Cyber Crime laws with the Constitutional Law in Indonesia. *International Journal of Cyber Criminology, 15*(1), 79-94.

Arimuladi, S. U. (2022). Access to Justice Based on Expert Testimony in Tax Crimes: An Integrated Criminal Justice System Perspective in Indonesia. *Pandecta Research Law Journal, 17*(1), 29-36. Retrieved from https://journal.unnes.ac.id/nju/index.php/pandecta/article/view/32622

Asmara, T. T. P., Ikhwansyah, I., & Afriana, A. (2019). Ease of Doing Business: Gagasan Pembaruan Hukum Penyelesaian Sengketa Investasi di Indonesia. *University of Bengkulu Law Journal*, *4*(2), 118–136. https://doi.org/10.33369/ubelaj.4.2.125-143

Balo, H. H. R., Wantu, F. M., & Tijow, L. M. (2020). System for Evidence of Corruption Criminal Act in Indonesia. *Asian Journal of Education and Social Studies, 8*(2), 46-55. Retrieved from https://doi.org/10.9734/ajess/2020/v8i230222

Berting, N. (2019). *On the shrinking spaces of social media, in Indonesia and elsewhere* (Graduation Thesis). Willem de Kooning Academy (WDKA), The Netherlands. Retrieved from https://pzwiki.wdka.nl/mw-mediadesign/images/c/cf/Tash_1902.2_Thesis.pdf

Boyle, P. (2020). *Indonesia's cyber war on West Papua solidarity*. Green Left Weekly, (1251), 13. https://search.informit.org/doi/abs/10.3316/informit.934561010777204

Breitenbauch, H., & Byrjalsen, N. (2019). Subversion, statecraft and liberal democracy. *Survival, 61*(4), 31-41. https://doi.org/10.1080/00396338.2019.1637118

Broniatowski, D. A., Jamison, A. M., Qi, S., AlKulaib, L., Chen, T., Benton, A., ... & Dredze, M. (2018). Weaponized health communication: Twitter bots and Russian trolls amplify the vaccine debate. *American journal of public health, 108*(10), 1378-1384. https://ajph.aphapublications.org/doi/abs/10.2105/AJPH.2018.304567

Castellino, J. (2021). *International law and self-determination: the interplay of the politics of territorial possession with formulations of post-colonial 'national' identity*. BRILL.

https://doi.org/10.33019/society.v10i2.482

Chen, L. (2020). *Improving digital connectivity for e-commerce: A policy framework and empirical note for ASEAN*. Economic Research Institute for ASEAN and East Asia. https://www.think-asia.org/handle/11540/11681

Clark, J., & Aufderheide, P. (2011). *A New Vision for Public Media. In Media and Social Justice* (pp. 55-67). Palgrave Macmillan, New York. https://doi.org/10.1057/9780230119796_5

Dini, A. A., Sæbo, Ø., & Wahid, F. (2018). Affordances and effects of introducing social media within eParticipation—Findings from government-initiated Indonesian project. *The Electronic Journal of Information Systems in Developing Countries, 84*(4), e12035. https://doi.org/10.1002/isd2.12035

Farsi, M., Daneshkhah, A., Far, A. H., Chatrabgoun, O., & Montasari, R. (2018). Crime data mining, threat analysis and prediction. In *Cyber Criminology* (pp. 183-202). Springer, Cham. https://doi.org/10.1007/978-3-319-97181-0_9

Fernando, J. Z., Pujiyono, P., Rozah, U., & Rochaeti, N. (2022). The freedom of expression in Indonesia. *Cogent Social Sciences, 8*(1), 2103944. https://doi.org/10.1080/23311886.2022.2103944

Fichman, P., & McClelland, M. W. (2021). The impact of gender and political affiliation on trolling. *First Monday, 26*(1). https://doi.org/10.5210/fm.v26i1.11061

Gaidosch, T. (2018). The Industrialization of Cybercrime: Lone-wolf hackers yield to mature businesses. *Finance & Development, 55*(2), 22-26.

Harahap, R. R. M., Munawir, Z., & Hidayani, S. (2019). Tinjauan Yuridis Penyelesaian Sengketa Atas Pemakai Kartu Kredit Tipe Gold Dengan Bank Penerbit Kartu Kredit (Studi Putusan No. 161/Pdt-G/2017/PN. Mdn). *JUNCTO: Jurnal Ilmiah Hukum, 1*(2), 136-142. https://doi.org/10.31289/juncto.v1i2.210

Hodge, E., & Hallgrimsdottir, H. (2020). Networks of hate: the alt-right,"troll culture", and the cultural geography of social movement spaces online. *Journal of Borderlands Studies, 35*(4), 563-580. https://doi.org/10.1080/08865655.2019.1571935

Horse, A. J. Y., Jeung, R., Lim, R., Tang, B., Im, M., Higashiyama, L., ... & Chen, M. (2021). *Stop AAPI hate national report*. Stop AAPI Hate: San Francisco, CA, USA. https://stopaapihate.org/wp-content/uploads/2021/11/21-SAH-NationalReport2-v2.pdf

Howie, E. (2018). Protecting the human right to freedom of expression in international law. *International Journal of Speech-language Pathology, 20*(1), 12-15. https://doi.org/10.1080/17549507.2018.1392612

Jurriëns, E., & Tapsell, R. (Eds.). (2017). *Digital Indonesia: connectivity and divergence*. ISEAS-Yusof Ishak Institute. https://doi.org/10.1355/9789814786003

Lim, M. (2017). Freedom to hate: social media, algorithmic enclaves, and the rise of tribal nationalism in Indonesia. *Critical Asian Studies, 49*(3), 411-427. https://doi.org/10.1080/14672715.2017.1341188

Lindsey, T., & Pausacker, H. (Eds.). (2016). *Religion, law, and intolerance in Indonesia*. Routledge, Taylor & Francis Group. https://doi.org/10.4324/9781315657356

Lubin, A., & Townley, H. (2020). The International Law of Rabble Rousing. *45 Yale Journal of International Law Online 1* (March 2020). https://www.repository.law.indiana.edu/facpub/2907/

Manning, M., & Agnew, S. (2020). Policing in the era of AI and smart societies: austerity; legitimacy and blurring the line of consent. In *Policing in the Era of AI and Smart Societies* (pp. 59-82). Springer, Cham. https://doi.org/10.1007/978-3-030-50613-1_2

https://doi.org/10.33019/society.v10i2.482

Manuhutu, M. A., Muttaqin, M., Irmayani, D., Tamara, T., Gustiana, Z., Hazriani, H., ... & Karim, A. (2021). *Pengantar Forensik Teknologi Informasi*. Medan: Yayasan Kita Menulis.

Manullang, S. O. (2020). The Declaration Content in Law of Electronic Transaction Information on Online Prostitution: In the Review of the Legal Sociology View. *International Journal of Social Sciences, 3*(1), 62– 70. https://doi.org/10.31295/ijss.v3n1.151

Manullang, S. O. (2021a). Perubahan Sosial Masyarakat Pedesaan Di Era Teknologi. *Cross-border*, *4*(1), 83-88.

Manullang, S. O. (2021b). Kesadaran Masyarakat Dalam Memahami Undang Undang Nomor 11 Tahun 2008 Tentang Informasi Transaksi Elektronik Dalam Media Sosial. *International Journal of Community Service and Development (INCOMMENT), 1*(1), 10–20. Retrieved from http://incomment.org/index.php/INCOMMENT/article/view/2

McGonagle, T., Bednarski, M., Francese Coutinho, M., & Zimin, A. (2019). *Elections and media in digital times*. UNESCO Publishing. https://hdl.handle.net/11245.1/fa304e04-40bb-4519-b0db-f272de79b83f

Mietzner, M., & Muhtadi, B. (2018). Explaining the 2016 Islamist mobilisation in Indonesia: Religious intolerance, militant groups and the politics of accommodation. *Asian Studies Review, 42*(3), 479-497. https://doi.org/10.1080/10357823.2018.1473335

Nehru, V. (2016). *Indonesia: The Reluctant Giant*. The National Interest, February 11. https://carnegieendowment.org/2016/02/11/indonesia-reluctant-giant-pub-62745

Neyasyah, M. S. (2020, March). Legal Resilience in the Phenomenon of Social Media Political Buzzer in Indonesia. In *3rd International Conference on Law and Governance (ICLAVE 2019)* (pp. 338-344). Atlantis Press. https://dx.doi.org/10.2991/aebmr.k.200321.044

Nugraha, L. K., & Putri, D. A. (2016). *Mapping the Cyber Policy Landscape: Indonesia*. London: Global Partners Digital.

Nuryanti, S. (2020). Populism in Indonesia: Learning from the 212 Movement in Response to the Blasphemy Case against Ahok in Jakarta. In *Populism in Asian Democracies* (pp. 165-175). Brill. https://doi.org/10.1163/9789004444461_011

Ong, J. C., & Tapsell, R. (2021). Demystifying disinformation shadow economies: fake news work models in Indonesia and the Philippines. *Asian Journal of Communication*, 1-17. https://doi.org/10.1080/01292986.2021.1971270

Paterson, T. (2019). Indonesian cyberspace expansion: a double-edged sword. *Journal of Cyber Policy, 4*(2), 216-234. https://doi.org/10.1080/23738871.2019.1627476

Payne, B. (2018). White-Collar Cybercrime: White-Collar Crime, Cybercrime, or Both?. *Criminology, Criminal Justice, Law & Society, 19*(3), 16-32. https://www.proquest.com/scholarly-journals/white-collar-cybercrime-crime-both/docview/2164138515/se-2

Pujoyono, N. W. (2020). Penal Policy dalam Upaya Preventif Kejahatan Carding di Indonesia. *Jurnal Panji Keadilan: Jurnal Ilmiah Nasional Mahasiswa Hukum, 3*(1), 86-98. https://doi.org/10.36085/jpk.v3i1.1183

Rajput, B. (2018). Identifying the challenges of criminal justice system while responding to cyber economic crime. *International Journal of Creative Research Thoughts, 6*(1), 146-155.

Ramli, K. (2020). *Indonesia on the Move: Improving Connectivity to Support E-commerce*. E-commerce Connectivity in ASEAN, 31.

Reichel, P. L. (Ed.). (2019). *Global Crime: An Encyclopedia of Cyber Theft, Weapons Sales, and Other Illegal Activities* [2 volumes]. ABC-CLIO.

https://doi.org/10.33019/society.v10i2.482

Roark, M. M. (2015) Elonis v. United States: The Doctrine of True Threats: Protecting Our Ever-Shrinking First Amendment Rights in the New Era of Communication. *Pittsburgh Journal of Technology Law & Policy, 15*. https://doi.org/10.5195/tlp.2015.162

Sastramidjaja Y. & Wijayanto (2022). Cyber Troops, Online Manipulation of Public Opinion and Co-Optation of Indonesia's Cybersphere. *ISEAS – Yusof Ishak Institute. Issue 7*. https://doi.org/10.1355/9789815011500

Schallbruch, M., & Skierka, I. (2018). Current Priorities and Gaps in German National Cybersecurity, Future Trends. In *Cybersecurity in Germany* (pp. 49-64). Springer, Cham. https://doi.org/10.1007/978-3-319-90014-8_5

Setiawan, T., & Suhartomo, A. (2019, August). The relation between internet use and societal development in Indonesia. In *2019 International Conference on Sustainable Engineering and Creative Computing (ICSECC)* (pp. 133-137). IEEE. https://doi.org/10.1109/ICSECC.2019.8907127

Setti, S., & Wanto, A. (2019). Analysis of Backpropagation Algorithm in Predicting the Most Number of Internet Users in the World. *Jurnal Online Informatika, 3*(2), 110-115.

Shah, T. S., & Taylor, C. H. (2021). The "Ashoka Approach" and Indonesian Leadership in the Movement for Pluralist Re-Awakening in South and Southeast Asia. *The Review of Faith & International Affairs, 19*(2), 56-71. https://doi.org/10.1080/15570274.2021.1917149

Siregar, G., & Lubis, M. R. (2021). Juridical Analysis of Religious Blasphemy Crimes Through Smartphone Application Based On The Information and Electronic Transaction. *Journal of Contemporary Issues in Business and Government, 27*(2), 1006-1012. http://dx.doi.org/10.47750/cibg.2021.27.02.120

Sommer, P. (1997). Downloads, Logs and Captures: Evidence from Cyberspace. *Journal of Financial Crime, 5*(2), 138-151. https://doi.org/10.1108/eb025826

Syahputra, I. (2019). Expressions of hatred and the formation of spiral of anxiety on social media in Indonesia. *SEARCH Journal of Media and Communication Research, 11*(1), 95-112. http://search.taylors.edu.my/

Tapsell, R. (2021). Social media and elections in Southeast Asia: The emergence of subversive, underground campaigning. *Asian Studies Review, 45*(1), 117-134. https://doi.org/10.1080/10357823.2020.1841093

Tenove, C., Buffie, J., McKay, S., & Moscrop, D. (2018). *Digital threats to democratic elections: how foreign actors use digital techniques to undermine democracy*.

Toha, R. J., Gueorguiev, D. D., & Sinpeng, A. (2021). The normalization of intolerance: The 2019 presidential election in Indonesia. *Electoral Studies, 74*, 102391. https://doi.org/10.1016/j.electstud.2021.102391

Tyson, A. (2021). Blasphemy and judicial legitimacy in Indonesia. *Politics and Religion, 14*(1), 182-205. https://doi.org/10.1017/S1755048319000427

About the Author

Sardjana Orba Manullang obtained his Doctoral degree in Legal Studies from Universitas Parahyangan, Indonesia, in 2011. The author is a lecturer at the Department of Law, Faculty of Law, Universitas Krisnadwipayana, Indonesia.
E-Mail: somanullang@unkris.ac.id

https://doi.org/10.33019/society.v10i2.482