Available *online* at: http://ojs.atmajaya.ac.id/index.php/fiabikom/index

Jurnal InterAct

| ISSN (Print) 2252-4630 | ISSN (Online) 2614-1442 |

JURNAL InterAct

ETHICAL DISCOURSE OF DOXING IN INDONESIAN TWITTER USERS

Suci Marini Novianty [1], *Sri Wijayanti* [2], *Jihad Muamar*[3]

[1,2,3]Communication Science Dept, Universitas Pembangunan Jaya;

INFORMATION

Diterima: December 20, 2022
Direvisi: July 7, 2023
Tersedia: online: October 2, 2023

KEY WORDS

Doxing, Twitter, Discourse Analysis

CORRESPONDING AUTHOR

E-mail: suci.marini@upj.ac.id

ABSTRAK

Indonesia sebagai negara mayoritas kelima pengguna Twitter di dunia, menjadikan platform ini sebagai dunia maya populer untuk mencari informasi dan kumpulan opini dengan tujuan memenuhi keinginan rasa ingin tahu, pengetahuan, kebencian, suka, atau topik apapun yang dianggap menarik untuk dibicarakan. Tidak jarang diskusi semacam itu mengarah pada perdebatan penting atau sepele yang membuat seseorang mengungkapkan informasi kredensial lawan mereka. Tindakan mengungkapkan informasi kredensial tentang lawan mereka disebut 'doxing'. Namun demikian, fenomena doxing adalah paradoks, karena beberapa orang mungkin mengatakan doxing dapat terjadi dengan niat jahat, sementara yang lain menganggap doxing sebagai perbuatan baik mengungkapkan aktor kasus kriminal atau tidak bermoral. Oleh karena itu, tulisan ini bertujuan untuk membahas "apa wacana etis untuk aktivitas doxing di kalangan pengguna Twitter Indonesia?". Kasus doxing yang menjadi subjek kajian tulisan ini adalah kasus viral Natalie, Rizky Billar, Gilang 'Bungkus', akun *whistle blowe*r anonim, dan dugaan penipuan. Metode dalam tulisan ini adalah kajian wacana kritis, dengan menggunakan teknik pengumpulan data dokumentasi. Hasilnya, tulisan ini menemukan bahwa doxing adalah wacana terbuka yang memiliki kemungkinan untuk diperluas sesuai dengan pluralitas masyarakat, dinamika pemerintah, dan pembatasan kebebasan berbicara di bidang frekuensi publik. 'Doxing Netral' adalah terminologi baru yang diusulkan makalah ini yang percaya bahwa kecukupan doxing terletak pada tujuannya. Kesimpulannya, dalam hak apa pun ada batasan etis untuk mengetahui apakah ada lebih banyak manfaat dalam melakukannya. Ketika, orang memiliki hak untuk mengakui informasi mengenai kesejahteraan mereka maka doxing dapat diterima, juga berlaku sebaliknya. Selain itu, kami percaya bahwa itu berkompromi dengan tujuan doxing.

INTRODUCTION

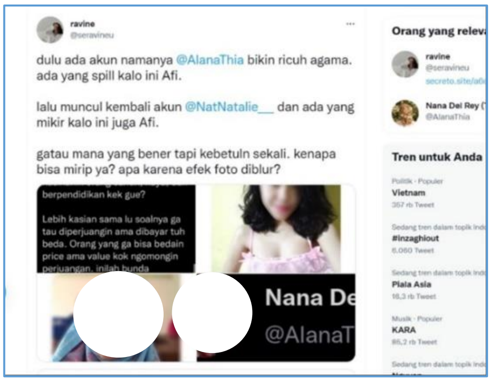
Per 2022, Twitter users in Indonesia is said to be approximately 18,45 million (Kemp, 2022). This figure also puts Indonesia as the fifth majority country of Twitter users in the world (Rizaty, 2022). The information that is posted on Twitter frequently contains opinion about products, services, celebrities, events, or anything that is of user's interest (Giachanou & Crestani, 2016). In Indonesia, Twitter is considered as the social media you use to seek information and opinion pool. Twitter as a popular social medium platform, is a host for users to express their opinions (Cheng et al, 2021). Indonesia is very active on social media; for example, in 2012 its capital, Jakarta, originated the most tweets of any city in the world (Alatas et al, 2019). Although Internet and Twitter usage are concentrated in Jakarta and Java's urban centers, their use is high in rural communities. Much internet access is through mobile technology (Carley et al, 2016).

Twitter is micro-blogging social networking of textual message (Budiharto & Meiliana, 2018). Users of Twitter's microblogging service can publish up to 280 (up from 140 and longer now) character messages, which may also include links and images. Users can follow accounts, like messages, respond to them, and share (retweet) them in addition to actively contributing themselves. Using hashtags (#) and public messages or mentions (@) on other Twitter accounts, posts can be connected to more extensive debates on the social media network (Zhang et.al, 2020). Twitter successfully produced 500 million bytes of data per day (Miranda et al, 2019). The microblogging service that Twitter (now X) offers is still being used widely by users. In the business environment alone, Twitter is one of the most popular social media, with 321 million active users per month (Tao & Wilson, 2015). Twitter social media as a data source which will be analyzed in the form of sentiment analysis, which is a process of understanding, extracting, and processing textual data automatically to obtain sentiment information contained in an opinion sentence (Fitri & Hasibuan, 2019). A study shows Twitter is a logical source of data for Hate speech analysis as Twitter users are more likely to express emotions of an event by posting multiple tweets (Fauzi & Yunarti, 2018).

While blogging activity shifts to vlog and any kind of other multimedia content, microblogging stands as a part of social media experience. Therefore, amidst new development of social media platforms, Twitter is still popular to be used by various audience or we might call it followers. Its title as opinion pool where people could easily tweet their thoughts, make their users turn to the platform when they want to share their curiosity, knowledge, hatred, likings, or any topics they find interesting to talk about. Consequently, it is inevitable to find that various thinking is gathered in Twitter. Thus, triggering heated debate over overflowing topics.

Nevertheless, it is very alarming how in certain cases, the debate turns ugly. The debate over important or trivial matters could make people reveal the credentials information about their challenger. While the other party is actually being anonymous and revealing their true self on Twitter platform. The act of revealing the credentials information about their opponents is called doxing (Douglas, 2016). Doxing in Indonesian Twitter users are easily found. Various cases lead to doxing. Mostly, the doxing takes place in thread or series of Tweets regarding the same topic. Everyone has the potential of being doxed, whether they are a celebrity.

Popular cases, that we wish to elaborate are Natalie, Rizky Billar, and Gilang Bungkus (sexual harassments and abuse cases included). We also add general cases of doxing including the doxing of anonymous whistleblower accounts and alleged fraud. In Natalie's case, it was phenomenal because she was doxed as an anonymous account of Afi Nihaya Faradisa. This was blown up on September 17, 2022, when Afi asked an account to take down their post regarding a meme which shows her photo alongside a blurry photo of Natalie. Natalie was an anonymous account who posts provocative photos and words. When Afi clarified that she was on hiatus from Twitter for more than three months, therefore the meme hurt her image publicly.



ravine
@seravineu

dulu ada akun namanya @AlanaThia bikin ricuh agama. ada yang spill kalo ini Afi.

lalu muncul kembali akun @NatNatalie__ dan ada yang mikir kalo ini juga Afi.

gatau mana yang bener tapi kebetuln sekali. kenapa bisa mirip ya? apa karena efek foto diblur?

berpendidikan kek gue?

Lebih kasian sama lu soalnya ga tau diperjuangin ama dibayar tuh beda. Orang yang ga bisa bedain price ama value kok ngomongin perjuangan. inilah bunda

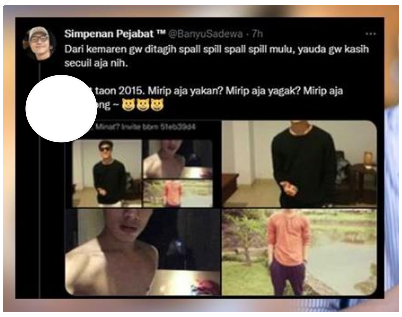
Source : Twitter Screenshot (Personal Document)

Figure 1. Doxing thread of Natalie's account owner

Afi Nihaya Faradisa, is actually a prominence name. Afi was invited by the President of Republic of Indonesia in 2017 for her article titled ‘Warisan’. The article gone viral from Facebook platform, thus granted her fame. Nonetheless, she was found guilty of plagiarizing another account (Irawati, 2022). Since then, she was laid low from the public, while still being active in various platforms of her personal accounts. The meme case blown up after Afi’s clarification because she doxed the meme’s account owner personal info and infuriating fellow Twitter users (Irawati, 2022). One was @seravineu, who gives clues of Afi being Natalie and another account @AlanaThia. The Natalie account is actually contradicting Afi’s image in public as a Muslim woman with her hijab, and @AlanaThia was viral for her statement which was degrading Islamic beliefs (Irawati, 2022).

Natalie’s account was filled with revealing photos and controversial tweets. Although the face is blurred purposively, @seravinue was able to give proof of Natalie being the same person as Afi. One account who claimed to be Afi’s college friend also tweeted of she already noticed the similarity for a while, giving her proofs and opening their WhatsApp chats. This case is left hanging, since Afi, Natalie, or @AlanaThia are gone and not stating any clarification anymore since the accounts were meticulous of dropping the documents of proofs.

The second case is Rizky Billar’s. He is actually being tangled with a domestic violence case against his wife. The couple is notorious in the entertainment industry for being romantic to each other. The wife, Lesti Kejora, is a dangdut singer who rose to fame after winning a talent contest in national television. After the news of his domestic violence appeared, his old photos in @GigoloJKT199 surfaced. The post contains several photos of him, one of him being topless and said, “*Rizky, Minat? Invite bbm…* (Rizky, interested? Invite BBM pin…)” back in 2015 (Ridho, 2022). This became a viral topic to talk about, as people are surprised because his image was pious in public. It is considered as doxing too, because we believe that the pictures are not meant to be seen in public anymore and do damage to his recent identity. Some Twitter users found it inevitable because he hurts his clueless wife. This case is still ongoing to this day.



Simpenan Pejabat ™ @BanyuSadewa · 7h

Dari kemaren gw ditagih spall spill spall spill mulu, yauda gw kasih secuil aja nih.

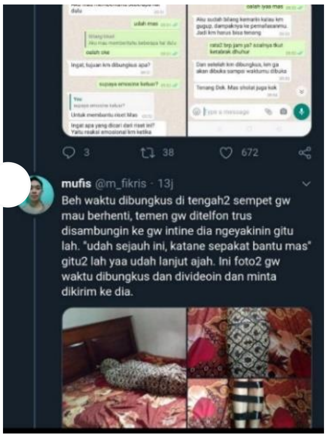
[redacted] taon 2015. Mirip aja yakan? Mirip aja yagak? Mirip aja ng ~ 😸😸😸

Minat? Invite bbm 51eb39d4

Source : Twitter Screenshot (Personal Document)

Figure 2. Doxing thread of Rizky Billar’s past

The third one was a case famous as Gilang ‘Bungkus’. This case was started when an account, @mfikris, made a thread titled “Predator ‘Fetish Kain Jarik’ Berkedok Riset (‘Jarik Cloth Fetish’ Predator Under the Guise of Research)” (Widiyani, 2020). The account told a story of his friend being a target of one person named, Gilang, a student from a notable university in Indonesia. His friend is a male who is Gilang’s junior acquaintance and been asked to cover himself inside *jarik* cloth in a way imitating how Muslim corpse is treated. Jarik cloth is Indonesian traditional cloth which commonly covered with batik patterns and has various use (Moselo, 2022). This case was viral, and people doxed Gilang personal information. To some extent, there is no longer private information about him. This case ended with Gilang being put in jail and being expelled from his school. Gilang’s case is actually similar to any ‘spilling the tea’ about sexual sexual assault perpetrators. We observe that since 2019, there is significant rise of Twitter’s thread in telling sexual assault’s victim experience and reason why they want public to know about their case. The sexual harassments and abuse or assault survivors in those threads were both, female and male. Most of the threads then ended with doxing the culprit’s personal information.



udah mas

oalah oke

Ingat, tujuan km dibungkus apa?

supaya emosine keluar?

Untuk membantu riset Mas

Ingat apa yang dicari dari riset ini? Yaitu reaksi emosional km ketika

oalah iyaa mas

Aku sudah bilang kemarin kalau km gugup, dampaknya ke pernafasanmu. Jadi km harus bisa tenang

rata2 brp jam ya? soalnya tkut ketabrak dhuhur

Dan setelah km dibungkus, km ga akan dibuka sampai waktumu dibuka

Tenang Dek. Mas sholat juga kok

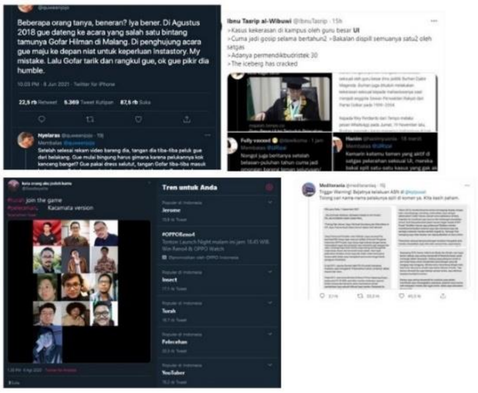
3 38 672

mufis @m_fikris · 13j

Beh waktu dibungkus di tengah2 sempet gw mau berhenti, temen gw ditelfon trus disambungin ke gw intine dia ngeyakinin gitu lah. "udah sejauh ini, katane sepakat bantu mas" gitu2 lah yaa udah lanjut ajah. Ini foto2 gw waktu dibungkus dan divideoin dan minta dikirim ke dia.

Source : Twitter Screenshot (Personal Document)

Figure 3. Doxing thread of Gilang Bungkus



Beberapa orang tanya, beneran? Iya bener. Di Agustus 2018 gue dateng ke acara yang salah satu bintang tamunya Gofar Hilman di Malang. Di penghujung acara gue maju ke depan niat untuk keperluan Instastory. My mistake. Lalu Gofar tarik dan rangkul gue, ok gue pikir dia humble.

22,5 rb Retweet 5.369 Tweet Kutipan 87,5 rb Suka

Ibnu Tasrip al-Wibuwi @IbnuTasrip · 15h

>Kasus kekerasan di kampus oleh guru besar UI
>Cuma jadi gosip selama bertahun2 >Bakalan dispill semuanya satu2 oleh satgas
>Adanya permendikbudristek 30
>The iceberg has cracked

Source : Twitter Screenshot (Personal Document)

Figure 4. Series of doxing threads sexual perpetrator

In Indonesia, we also witness where there is also a tendency of people to dox controversial anonymous accounts who is active in tweeting political or government related topics. We observe such actions rooted back from 2019 where politics polarization felt the strongest amid presidential elections. The account owners are stripped of their anonymity and have their personal information shown to public. While, for some being anonymous is to save themselves as they are actually a whistle blower from the institution. Another trend is to dox someone when they have done fraud. Various fraud cases can be read on Twitter, as the victim put all of their allegations inside a chronological thread.

Those cases which we mentioned above are contradictory. In a way, some people might see the doxing being done to those names is unnecessary. While for others, it is obligatory to expose those identity, thus making people aware of their doing in Twitter universe since it could possibly harm others in real life. From those stances, we would like to discuss this paper with "What is the ethical discourse of doxing in Indonesian Twitter users?" as the research question.

Thus, this study aims to give another perspective upon seeing the doxing discourse ethically. Based on the case of Indonesian Twitter users act, we could see doxing in a new light.

LITERATURE DAN METHODOLOGY

Every Internet user is subject to potential doxing (Bei Li, 2018). Doxing, also spelled "doxxing", is the practice of publishing someone's private information online in a way that is simple for others to access (Douglas, 2016). Doxing is a form of cyberbullying in which personal information on others is sought and released, thereby violating their privacy, and facilitating further harassment (Chen et al, 2019). Doxing refers to the practice of disclosing sensitive personal information about a person without their consent (Karimi et al, 2022). The main purpose of doxing attacks is to threaten, embarrass, harass, and humiliate the organization or individual (Khanna et al, 2016). Trottier in Li & Whitworth (2022) categorizes doxing along several axes, including: doxer, target, and/or law enforcement. Douglas (2016) emphasizes that doxing should be understood as releasing 'publicly' a type of identity knowledge about an individual (the subject of doxing) that establishes a verifiable connection between it and another type (or types) of identity knowledge about that person. Doxing details may include but not limited to legal name, residential address, school, office, personal photograph, personal relationship, or their achievements. Nevertheless, Marx in Douglas (Douglas, 2016) stated that there are seven types of identity. For those who have not the seven types revealed, means they have their anonymity protected. The seven types of identity are:

Table 1. Types and example of identity knowledge

No	Type	Description
1	Legal name	The name that a person is recognized by in official and legal contexts
2	Locatability	Information that indicates a person's residence or personal contact information, such as

		an address or phone number
3	Pseudonyms linked to name or location	a name or number that identifies a single person (for example, a bank account number in a system linked to their legal name or any other potentially distinctive attribute (such as an address)
4	Pseudonyms linked to name or location a. For policy reason b. Audience is unaware of pseudonym	a. A name or code used to identify a person in a system that is unrelated to her legal name, such as in a medical record that has been anonymized. b. An alias or other name used by someone to conceal their identity or to deceive others in place of their real name
5	Pattern knowledge	Someone who is easily identifiable by her recurring public behaviors or customs, such boarding the same bus at the same time every morning
6	Social categorization	Information that can be used to classify someone into one or more social groups (or stereotypes), such as physical characteristics, an accent, a fashion style, etc.
7	Symbols of eligibility/non-eligibility	Possessing objects or information, such as a uniform, password, or rail ticket, that allow someone to be recognized as being entitled to specific rights and treatment

Doxing is online abuse where a malicious party harms another by releasing identifying or sensitive information. Motivations for doxing include personal, competitive, and political reasons, and web users of all ages, genders and internet experience have been targeted. Doxing is one of a few cyberattacks that can cause direct, serious, and lasting harm to its victims (Snyder & Kanich, 2017). Doxing is fundamentally described by Douglas as "the purposeful publication of personally identifiable information about an individual on the internet by a third party, frequently with the intent to humiliate, threaten, intimidate, or penalize the named individual." (Douglas, 2016). Therefore, the most important part about doxing is removal one’s anonymity to some extent. Doxing is about one’s intention to dox. Therefore, the doxing activity is open to interpretation of being good or bad thing. The term suggesting ‘doxing’ is ‘dropping document’ or ‘dropping dox’. The verification in doxing is what differs its process from another revelation, such as exposure and publicity (Douglas, 2016).

Silva adds that there are two kinds of doxing, common doxing, and organizational doxing (Silva, 2021). Due to widespread usage of online social networks (OSN) and a lack of privacy awareness, regular doxing behaviors are more prevalent among adolescents. These exposed PIIs are more likely to be disseminated in social media platforms, chat rooms, and online discussion forums by facilitating group cyberbullying and threats. Organizational doxing is more likely to be motivated by a group's goal, and its actions are carried out methodically. Customer, employee, or organizational important data that is sold or made public online would be the doxing outcome data.

Anderson and Wood (2022) agree that Douglas succeeded in elaborating the most sophisticated typology for doxing’s forms. For Douglas (Anderson & Wood, 2022) there are three forms of doxing (1) deanonymizing doxing; (2) targeting doxing; (3) delegitimizing doxing. The victim of deanonymizing doxing must deal with losing their anonymity, whether it be in their personal or professional life. While targeting doxing involves the target losing their anonymity, for instance by having their home address posted online. Furthermore, delegitimizing doxing involves exposing evidence that the target has committed fraud or other "immoral" behavior, for instance, and causes the target to lose credibility.

Another stance from Lee (Lee, 2020), doxing is performed through intertextuality since the "success" of doxing depends on the actor who compiles a range of source texts from websites, social media profiles, and other offline sources. Intertextuality is the process by which texts allude to one another. The affordances of social media help intertextuality in the digital realm even more. Boyd in Lee (2020) asserts that the characteristics of public communication on networked media include their persistence (the capacity to record and archive web content), replicability (the capacity to reproduce and modify web content), scalability (the limitless possibilities of making content visible), and searchability (the ease of locating a person and their information).

Members of networked publics can easily produce intertextual relations by changing and reappropriating texts from various semiotic sources and platforms, becoming what Androutsopoulos refers to as "intertextual operators" (Lee, 2020). As more people reveal the most private areas of their life on social media, personal information is readily public online. Even when such content is intended to be shared just with close friends and family, it can be readily removed from its original context, leading to a condition known as context collapse where any posted content addresses an endless, unknowable audience (Lee, 2020).

Doxxing can be viewed in this light as a "recontextualized social practice" (Leeuwen, 2009). Van Leeuwen (2009) believes that discourses always represent and modify social actions through recontextualization processes. In social media, the simplicity of "sharing" content across media platforms necessitates reinterpreting an already-written text in light of fresh discursive settings (Androutsopoulos, 2014). These social media features also make it possible for one's personal information to be shared inadvertently, which gives birth to doxing. The real name policy of social media and internet users' lack of critical awareness of their online privacy to safeguard the information published on their newsfeeds are two more reasons that may lead to the "accidental" disclosure and spread of personal data (Wauters, Lievens, & Valcke, 2014).

Silva (2021) proposes the idea of mitigation to avoid doxing cases. Though the process uses several software and computer processing techniques, in this paper we sought to limit the main idea of mitigation can also be done with limited source and dismissing the probability of advance application. The first step is to conduct a self-audit. For Silva (2017) this initial phase of doxing prevention/adoption procedure is to identify the already published/leaked information on the subject.

The second is to remove unnecessary information. After identifying any potential data leaks or unnecessary data releases, take the required precautions to stop them from spreading further online. These processes can range from being as easy as removing unnecessary entries, dormant accounts, and images to being as complex as removing already revealed and other sensitive data like a person's biometric information, geo-location, identification, or any private number. Employees or organizational operation products like articles, reports, or white papers are two examples of unnecessarily disclosed organizational information that should be avoided. Silva believes, if such an incident has ever occurred, organizations must try to stop any lingering user data breaches and corporate data leaks (Silva, 2021).

Third, activating privacy and security settings and anti-abuse options. Sabah and Thalheim stated that, the majority of the crucial private information, including a person's name, location, and activities, is either always visible or made available to others by default on many platforms (Silva, 2021). Users are actually provided with privacy and security setting options in the majority of platforms so they can choose between three degrees of data visibility Public, Peers, and User alone. This is an easier method to prevent any personal identifiable data leaks. A certain level of protection from doxing or online harassment will be provided by turning on features like Secure browsing, two factor authentications, and the use of Anti-Abuse filters. Yet, it is unfortunate that the majority of consumers only apply these security settings when something bad happens.

Fourth, only trust the known and reliable people we know. False identities and profiles are very common and pose a threat to the site. The best approach to avoid this problem is to ignore and reject these fictitious identities. A quick background check and human intuition will confirm a person's legitimacy. Fifth, scheduling security updates. Platform or application security flaws are fairly common, and criminals don't hesitate to take advantage of them. Therefore, the leaking of private information and personally identifiable information is closely related to security improvements. A crucial element in the doxing environment is routine application security updates and patches. Sixth step or the last, raising awareness of third-party applications, whitelisting, and bloatware. The bulk of information systems often capture user data while also archiving numerous tasks through third-party applications. Malicious software, programs, and services sometimes ask for unnecessary access privileges to user information before carrying out the perp's damaging goals. The system's security will be improved, and the danger of data exposure will be reduced by using a core set of approved and verified applications and services (whitelisted). Security issues regarding bloatware are also growing. Modern consumer electronics are loaded with these applications, but it's likely that the user has never utilized them, losing out on important personally identifiable information. Even though it is necessary to remove these applications, doing so will be against the terms of the vendor contracts.

Those concepts above are the fundamental of this research. We examine the discourse of doxing by comparing ethical perspectives in academic journals and using their ethical stances to compare action done in cases we chose to answer the research question.

This research focuses on comparing discourses in ethical state of doxing. By concentrating on ethical point of view, the method used is critical discourse studies. Critical discourse studies are approach that lies in the constitutive problem – oriented, interdisciplinary approach of dynamic (socio)-cognitive or interactional moves and strategies and functions of the (social, situative, and cognitive) contexts of language use (Wodak & Meyer in Armayanti, 2019). Critical discourse studies and critical discourse analysis for Wodak (Wodak & Meyer in Armayanti, 2019) is different. While the practice of critical discourse studies lies on being critical as objectives of the research. The main focus is to seek new perspectives on the chosen topic.

In the analysis of Discourse either Critical or not, those are basically having the same point from language side or language used (Habibie, 2016). While discourse relies on scientific terms, critical discourse analysis uses a critical approach (Wodak & Meyer in Mullet, 2018). First, they have different purposes or ends in mind, which affects how they might be put to use. Scientific ideas have an "instrumental use" that aims to successfully manipulate the outside world. Critical theories work to reveal hidden coercion to "agents," liberating them from it and enabling them to choose what is in their best interests. Second, the "cognitive" architecture of critical and scientific beliefs is different. Scientific theories are "objectifying" in the sense that they may be distinguished from the things they refer to. The object domain that the theory defines does not include it. On the other hand, a critical theory is "reflective" in that it is constantly a component of the object-domain it represents. These theories partially concern themselves. Thirdly, the type of data that would establish whether or not critical and scientific hypotheses are valid varies. These hypotheses therefore call for various forms of proof.

This paper focuses on the ethical aspect of doxing. It is better to say that when we apply the context principle in ethical philosophy — that is, when we pay careful attention to the actual contexts of recognizably ethical thought and discourse — we will find that there are no words that in their primary function are used exclusively in ethical utterances (no technical terms), there are no words that are necessarily used in ethical utterances, and moreover there are not even any words that are used typically in ethical utterances. But this is something we find when we look at contexts of ethical discourse, not an implication of the context principle itself (Schoellner, 2016). Thus, using research papers to examine how they perceive doxing in ethical perspective and link it with cases in Indonesian Twitter users.

Data collection is carried out through documentation techniques, namely the technique of collecting and analyzing documents, both written, drawings and electronic, that are relevant to the source of research data. In this paper, documentation techniques are implemented through the activity of finding cases relevant to the object of study, namely doxing cases which involve paradoxical discussions, meaning that there are statements of pros and cons to doxing that have been carried out in these cases. Then the collected data is captured in screenshots for further analysis to find out ethical discourse for doxing activities among Indonesian Twitter users.

RESULTS AND DISCUSSION

In Indonesia’s Twitter sphere, the doxing phenomenon is a paradox. Because some might say that doxing may occur with malicious intent, while others perceive doxing as a good deed to reveal actors behind criminal or immoral cases. Douglas in Anderson and Wood (2021) believe that doxing intention should not be undertaken with malicious intent. Even when there is no malicious intent, doxing can also occur when journalists reveal in public the names of someone's pseudonyms in stories. But according to Douglas, mistakenly "doxing" someone online by inadvertently disclosing personal information is not the same as doxing. In other words, doxing and internet exposure are not the same thing, even though doxing may be one type of it. Douglas (2016) asserts that while doxing may be a kind of blackmail, it is not the same as defamation, blackmail, or gossip. Doxing, in contrast to gossip, trades on identity information rather than "suggestion, hearsay [or] innuendo" (Douglas, 2016). The distinction between doxing and gossip is "the difference between communicating information about someone and communicating information of someone," as Douglas (2016) persuasively notes.

In spite of that statement, for Fadhila, in her article "Two Wrongs Don't Make a Right: How Indonesia Netizens Use Doxing as a Weapon to Attack Others" (Fadhila, 2022), doxing is potentially harming the journalists and activists for the works and movement. Fadhila stated that according to SAFEnet, the increase in doxing in Indonesia was brought on by the numerous personal attacks on journalists and activists over the course of several years (Fadhila, 2022). For instance, a journalist from TopSkor named Zulfikar tweeted on a sensitive subject in 2017 that Hong Kong has the authority to deny Abdul Somad, an Indonesian ulema, entry into the territory. Despite the fact that his argument was rational, the followers of the ulema are bound to criticize it. They began to persecute him by doxing him and mailing threats. In no time, hashtags like #BoikotTopSkor became popular topics. As the result, TopSkor phoned Zulfikar to fire him. Or when famous activist Veronica Koman, who appears to be the target of doxing more frequently due to her aggressive advocacy for Papua's rights. In 2019, the Twitter user @/digeembok attempted to dox Koman by disclosing her residence and scaring her by claiming to have been watching her (Fadhila, 2022).

Fadhila statement is actually contradicting to what Douglas thought. Where for Douglas, doxing could be used as a tool for activism. For Douglas, doxing could actually be used as audience vigilantism in response to hate speech conducted by the contender (Douglas, 2020). Digital vigilantism is a response to a transgression that "seek[s] to render a targeted individual (or category of individual) visible through information sharing practices such as assembling and publishing their personal details" (Trottier, 2017). Douglas argues that doxing that deanonymizes a supporter of hate speech is a suitable strategy for stopping it if it aims to start a reeducation process (Douglas, 2020). In Indonesian Twitter user's case for Fadhila (2022) doxing is a cybercrime that requires considerable attention. Fadhila argues because Indonesian internet users frequently use it to harm one another, and doxing should never be carried out because it will never be relevant to the issue no matter how serious a mistake someone makes (Fadhila, 2022).

To contend with the stance made by Fadhila (2022), we believe that doxing in Indonesian Twitter users cannot be simplified as giving final verdict of no doxing allowed. Since journalism and activism are indeed a field full of limited stakeholders. This paper proposes the opposites. For the cases brought upon the article, we ponder the narrative of journalism and activism is a risky task. Therefore, with their line of work, it is important to mitigate the impact caused by their project or movement. Thus, doxing cases in Indonesian Twitter users vary.

Lee (2020) proposed another perspective in seeing doxing through ethical approach. The research focus was about Hong Kong Protesters act of doxing in a social movement. Bear in mind that this paper only highlights the general idea, since the findings are heavily related to Hong Kong protest event back in 2020. Lee uses 'doxer' as the term to call the doxing actor. For Lee, there are four key strategies of legitimizing doxing in the data:

a. Rationalization: doxing as effective self-defense

   Doxing is rationalized in the name of self-defense. Doxing is legitimized as a response to power imbalance. Being the powerless one, doxing empowers the weak to fight for their movement;

b. Re-definition: "we're not doing anything illegal."

   Doxing done with data in internet is not doxing. Moreover, if the doxer already being friend in any platform which makes the data is easily accessible for them. The doxers stand with the belief of their doxing activity is not guilty and rejecting ‘privacy’ to what has been available online;

c. Construction of negative-other: authorities as uneducated and immoral

Doxing is conducted to their target’s immoral actions, such as violence and abuse. Thus, making the target is acceptable to be doxed; and

d. Victimizing ‘US’: doxers as powerless

Doxers put themselves as victim. Therefore, their way to cope is by doxing the target. Thus, they are not the only victim, and creating wave of doxing when more doxers come up (Lee, 2020).

Additionally, Lee emphasizes vagueness and ambiguities of privacy and doxing definition legally (Lee, 2020). Since ‘Privacy’ and ‘Doxing’ could be legitimized by fellow doxers as they have the support of their group, creating altruism, a common legitimation strategy.

We acknowledge that those two papers are not using Indonesian Twitter users in their mind while conducting the research. Nevertheless, we find the link between those stances to see the ethical discourse of Indonesian Twitter user. Based on those discourses above, we tried to link them with cases we have mentioned in introduction above, as shown in table below:

Tabel 2. Cases and Ethical Discourse

No.	Case Name	Case Description	Ethical discourse
1	Natalie	Natalie's situation was exceptional because she was shown to be the anonymous Afi Nihaya Faradisa account. This gained attention on September 17, 2022, when Afi requested that a user delete a post about a meme that used both Natalie's and her own fuzzy photos. Natalie was an anonymous user who published provoking images and text. The face of the account’s owner was intentionally blurred, but @seravinue was able to provide evidence that Natalie and Afi were the same individual. @seravinue claimed that what she had done cannot be called doxing, because every document of evidence that she put was already online. Afi's alleged college friend's account tweeted that she had already recognized the similarities for some time, provided evidence, and accessed their WhatsApp conversations. Since Afi, Natalie, or @AlanaThia are no longer present and aren't providing any further explanation—their accounts were diligent about deleting the supporting paperwork—this case is left open.	There is no tangible cause to dox Natalie’s account owner at the first place. Because, she had done nothing that could actually harm other people significantly. The doxer seems to enjoy the stance to dox their target because they put such an effort to reveal the documents. However, their stance about the data revealed is not privacy is also valid. Nonetheless, we believe that this case does greater harm than good.
2	Rizky Billar	He is allegedly involved in a case of domestic abuse against his wife. In the entertainment industry, the couple is renowned for their passionate relationship. His earlier images on @GigoloJKT199 surfaced as the story of his domestic violence spread. People are astonished that he had such a religious public persona, therefore this has become a hot topic of discussion. It is also seen as doxing because the images are no longer intended for public viewing and harm the subject's present-day persona. Because he abuses his wife, some Twitter users believed it to be inevitable.	The domestic violence case is already handled by the police with some CCTV leaked to the public proving the actual action. However, for us, this case is unrelatable to the domestic violence case. Thus, does more harm than good at this point.
3	Gilang Bungkus & Sexual harassments and abuse Perpetrator	• The third case was the infamous Gilang "Bungkus" case. A topic named "Predator 'Fetish Kain Jarik' Berkedok Riset ('Jarik Cloth Fetish' Predator Under the Guess of Research'") was created by the user @mfikris, which started official police investigation. According to the account, his friend was the target of Gilang, a student from a prestigious Indonesian institution. His pal was a male who is Gilang's junior	The idea to dox the perpetrators in Twitter is proven more effective to bring justice in real for some sexual harassments and abuse or abuse survivors. Be it changes in regulation, or legal punishment. Hence, we believe that opening up verified sexual harassments and abuse perpetrators does better than harm.

		acquaintance and was instructed to dress in a jarik cloth to resemble how a Muslim corpse is handled. • Sexual harassments and abuse survivors are using Twitter as a platform to tell their story of being a victim. Mostly, they tell the event chronologically, with some proof, and their intention of revealing the case and doxing the culprit. At some points, there were so many men being the perpetrators and their photos were collaged to one "wanted" list. There were also users who came forward to dox their organization being the sexual harassments and abuses and abuse enabler. They state the name of institution since they feel anxious with the alleged culprit still maintain the power inside the organization.	
4	The doxing of anonymous whistle blower accounts	Heated political and governmental tension, also the growth of buzzer (paid users to drive and intensify selected issues), for those Indonesian Twitter users that annoyed by the movement created by anonymous account, they tend to open the actor behind. By using the personal data, they made the anonymous users shut their account and stop the movement. Since the harm is also impacting their real life.	For this case, we believe that the doxing should not happen. Because whistle blowing is one of the catalysts in organization to find faults or issues that need to be resolved.
5	Alleged fraud	Since Twitter is really considered as public sphere, there are threads using the platform to find people who swindling them. They usually put the chronology, efforts, and the personal identification card. Some blurred the address and number, while others, prefer to make it open to public, because for them, they are the powerless and sole victim.	This kind of certain cases, most of the time does not have exact result that they want to achieve by doxing private documents. Since fraud is said to be a tricky case to handle. We believe that there is more harm than good when revealing personal information.

Based on those cases examined regarding doxing activities, this paper found that doxing is an open discourse. Doxing discourse has the possibilities to be expanded in accordance with society plurality, government dynamics, dan free speech limitation in public frequency territory. By connecting them to doxing case in Twitter sphere in regions or country and find a doxing trends to distinguish, whether or not it is legitimate to conduct such action.

CONCLUSION

Doxing is neutral. This statement is what the paper believes, based on critical discourse study regarding doxing cases and linking them to Indonesian Twitter users' trend. In Natalie and Rizky Billar's cases, we should agree that doxing is not necessary because what they have done did not bring harm to wider audiences. However, for Gilang 'Bungkus' and other sexual harassment cases, we can condemn the wrongdoings and with some solid evidence, doxing is reasonable to be done on that account. Based on those cases presented above, we propose that idea because there is no statement as such. By emphasizing the 'neutral' nature of doxing, its action has its own positive and negative impact to overview.

Doxing can be seen as positive action when it is necessary to reach a wider audience then alarming, informing and educating them through dropping dox. Hence, public information that has been stored in public domain is accessible for everyone to open, therefore the term of breaching someone's consent is not applied. Additionally, they put them on purpose. When talking about consent in public domain, we could refer to doxing mitigation steps. Moreover, bear in mind that intertextuality meaning, and interpretation is a free subject to discuss among the viewers. It is a different case, however, if doxing is conducted with the intention to trash people or organizations in public with no mass advantage. When the action is managed with sole hatred.

Doxing could also be a powerful weapon for marginalized groups to make their voice heard. To answer our research objective, this paper believes that the adequacy of doxing lays in its purpose. In any right, there are limitations; ethical limitation in doxing is to know whether there is more to gain in doing so. When people have their right to acknowledge information regarding their wellbeing, then doxing is acceptable. Furthermore, we believe that it compromises the objectives of doxing. For further research, we would offer the replication of this method with different country's Twitter users. Seeking the doxing trends then discussing their ethical approach.

REFERENCES

Alatas, V., Chandrasekhar, A. G., Mobius, M., Olken, B. A., & Paladines, C. (2019). *When celebrities speak: A nationwide twitter experiment promoting vaccination in Indonesia* (No. w25589). National Bureau of Economic Research.

Anderson, B., & Wood, M.A. (2022). *Harm imbrication and virtualised violence: Reconceptualising the harms of doxxing.* International Journal for Crime, Justice and Social Democracy 11(1): 196-209.

Anderson, B., & Wood, M. A. (2021). *Doxxing: A Scoping Review and Typology. In J. Baile, A. Flynn, & N. Henry, The Emerald International Handbook of Technology-Facilitated Violence and Abuse* (pp. 205 - 226). Bingley: Emerald Publishing Limited.

Androutsopoulos, J. (2014). *Moments of sharing: Entextualization and linguistic repertoires in social networking*. Journal of Pragmatics, 4- 18.

Armayanti, R. (2019). *Critical Discourse Analysis (CDA) on Qualitative Research: A Review.* Journal of Research and Innovation in Language, 1(1), 29-24.

Bei Li, L. (2018). *Data privacy in the cyber age: Recommendations for regulating doxing and swatting.* Fed. Comm. LJ, 70, 317.

Budiharto, W., & Meiliana, M. (2018). *Prediction and analysis of Indonesia Presidential election from Twitter using sentiment analysis*. Journal of Big data, 5(1), 1-10.

Carley, K. M., Malik, M., Landwehr, P. M., Pfeffer, J., & Kowalchuck, M. (2016). *Crowd sourcing disaster management: The complex nature of Twitter usage in Padang Indonesia*. *Safety science, 90*, 48-61.

Cheng, I. K., Heyl, J., Lad, N., Facini, G., & Grout, Z. (2021). *Evaluation of Twitter data for an emerging crisis: an application to the first wave of COVID-19 in the UK.* Scientific Reports, 11(1), 19009.

Chen, M., Cheung, A. S. Y., & Chan, K. L. (2019). *Doxing: What adolescents look for and their intentions.* International journal of environmental research and public health, 16(2), 218.

Douglas, D. M. (2016). *Doxing: a conceptual analysis.* Ethics Inf Technology 18, 199-210.

Douglas, D. M. (2020). *Doxing as Audience Vigilantism against Hate Speech*. In D. Trottier, R. Gabdulhakov, & Q. Huang, *Introducing Vigilant Audiences* (pp. 259 - 279). Open Book Publishers.

Fadhila, Z. (2022). *Two Wrongs Don't Make a Right: How Indonesia Netizens Use Doxing as a Weapon to Attack Others*. Retrieved from CfDS (Centre for Digital Society): https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiIpf_4vtv6AhUCS2wGHUigA6gQFnoECAsQAQ&url=https%3A%2F%2Fcfds.fisipol.ugm.ac.id%2F2022%2F06%2F21%2Ftwo-wrongs-dont-make-a-right-how-indonesia-netizens-use-doxing-as-a-w

Fauzi, M. A., & Yuniarti, A. (2018). *Ensemble method for indonesian twitter hate speech detection.* Indonesian Journal of Electrical Engineering and Computer Science, 11(1), 294-299.

Fitri, V. A., Andreswari, R., & Hasibuan, M. A. (2019). *Sentiment analysis of social media Twitter with case of Anti-LGBT campaign in Indonesia using Naïve Bayes, decision tree, and random forest algorithm.* Procedia Computer Science, 161, 765-772.

Habibie, A. (2018). *Comparison Between Discourse Analysis and Critical*

Discourse Analysis From Linguistics View. Al-Lisan: Jurnal Bahasa (e-Journal), 1(1), 1–14. https://doi.org/10.30603/al.v1i1.317

Irawati, Z. M. (2022). *Profil Afi Nihaya Faradisa, Sosok di Balik Akun Twitter Natalie?* Retrieved from Popbela.com: https://www.popbela.com/career/working-life/zikra-mulia-irawati/profil-afi-nihaya-faradisa-sosok-di-balik-akun-twitter-natalie/5

Giachanou, A., & Crestani, F. (2016). *Like it or not: A survey of twitter sentiment analysis methods.* ACM Computing Surveys (CSUR), 49(2), 1–41.

Karimi, Y., Squicciarini, A., & Wilson, S. (2022). *Automated detection of doxing on twitter*. Proceedings of the ACM on Human-Computer Interaction, 6(CSCW2), 1-24.

Kemp, S. (2022). *DIGITAL 2022: INDONESIA*. Retrieved from Data Reportal: https://datareportal.com/reports/digital-2022-indonesia

Khanna, P., Zavarsky, P., & Lindskog, D. (2016). *Experimental analysis of tools used for doxing and proposed new transforms to help organizations protect against doxing attacks.* Procedia Computer Science, 94, 459-464.

Lee, C. (2020). *Doxxing as discursive action in a social movement.* Critical Discourse Studies, 1 - 19.

Leeuwen, T. V. (2009). *Discourse as the recontextualization of social practice: A guide.* In R. Wodak, & M. M. (Eds), *Methods of critical discourse analysis 2nd Ed* (pp. 144- 161). Thaousand Oaks: Sage Publications.

Li, Y. T., & Whitworth, K. (2022). *Data as a weapon: The evolution of hong kong protesters' doxing strategies*. Social Science Computer Review, 08944393221111240.

Miranda, E., Aryuni, M., Hariyanto, R., & Surya, E. S. (2019). *Sentiment Analysis using Sentiwordnet and Machine Learning Approach (Indonesia general election opinion from the twitter content).* In 2019 International Conference on Information Management and Technology (ICIMTech) (Vol. 1, pp. 62-67). IEEE.

Mullet, D. R. (2018). *A General Critical Discourse Analysis Framework for Educational Research*. Journal of Advanced Academics, 29(2), 116–142.

Moselo. (2022). *Macam-Macam Kain Jarik dan Manfaatnya*. Retrieved from Moselo: https://moselo.com/blog/kain-jarik/#:~:text=Kain%20jarik%20adalah%20salah%20satu,motif%20batik%20dengan%20beragam%20corak.

Ridho, M. (2022). *Viral di Twitter, Jejak Digital Rizky Billar Terungkap, Benarkah Pernah Jadi Gigolo?* Retrieved from Serangnews.com : https://serangnews.pikiran-rakyat.com/ragam/pr-1205605804/viral-di-twitter-jejak-digital-rizky-billar-terungkap-benarkah-pernah-jadi-gigolo?page=2

Rizaty, M. A. (2022). *Pengguna Twitter di Indonesia Capai 18,45 Juta pada 2022*. Retrieved from DataIndonesia.id: https://dataindonesia.id/digital/detail/pengguna-twitter-di-indonesia-capai-1845-juta-pada-2022

Schoellner, Karsten. (2016). *Towards a Wittgensteinian Metaethics*. (Dissertation Universität Potsdam Institut für Philosophie). https://publishup.uni-potsdam.de/opus4-ubp/frontdoor/deliver/index/docId/40928/file/schoellner_diss.pdf

Silva, C. S. (2021). *Doxing: Painting a Target on Someone's back: Characterization and Mitigation Practices.* Sri Lanka: Sri Lanka Institute of Information Technology.

Snyder, Peter., Kanich, Chris. (2017). *Fifteen Minutes of Unwanted Fame: Detecting and Characterizing Doxing.* IMC '17, November 1–3, 2017, London, United Kingdom. https://dl.acm.org/doi/pdf/10.1145/3131365.3131385

Tao W., Wilson C. (2015). *Fortune 1000 communication strategies on Facebook* *and Twitter*. Journal of Communication Management, 19(3), 208–223. Crossref.

Trottier, D. (2017). *Digital Vigilantism as Weaponisation of Visibility*. *P*hilosophy & Technology volume 30, 55–72.

Wauters, E., Lievens, E., & Valcke, P. (2014). *Towards a better protection of social media users: A legal erspective on the terms of use of social networking sites.* International Journal of Law and Information Technology, 22(3), 254-294.

Widiyani, R. (2020). *Gilang Bungkus Kain Jarik: Awal Kasus, Fetis, dan Perkembangan Terkini*. Retrieved from Detik Health: https://health.detik.com/berita-detikhealth/d-5120080/gilang-bungkus-kain-jarik-awal-kasus-fetis-dan-perkembangan-terkini

Zhang, S., Gosselt, J.F., & de Jong, M.D.T. (2020). *How Large Information Technology Companies Use Twitter: Arrangement of Corporate Accounts and Characteristics of Tweets.* Journal of Business and Technical Communication, 34(4), 364 - 392.