Tec Empresarial
P-ISSN: 1659-2395; E-ISSN: 1659-3359

Online Shaming as a Form of Digital Persecution, Legal Issue on Protection of Dignity and Privacy Rights of Victims in Indonesian Legal Framework

Rahel Octora[A], Christian Andersen[B]

Abstract

Cyberspace is a place where social interaction occurs. A person's actions carried out in the real world can be disseminated through the internet. When the action is considered inappropriate, the community then sanctions the person by humiliating him. Everyone who can access the internet can obtain information about the person's actions and then leave various derogatory comments. The act of online shaming, which seems to be a way of imposing social sanctions, is now a way to persecute. Digital persecution is carried out by attacking the person concerned with comments containing insults, threats, and/or blasphemy. In addition, the personal data of the person concerned is disseminated through the internet. This action is known as doxing. The person who is the victim of doxing then receives various terrors and threats. Online shaming followed by doxing certainly causes losses for victims. Therefore, it is necessary to examine how Indonesian law can protect the dignity of citizens from online shaming and how the government must establish a personal data protection policy to protect the right to privacy. The law needs to give strict sanctions to initiators who carry out the online shaming act. Regarding doxing actions, Indonesia needs to change the paradigm of formulation of norms, not only limited to the prohibition on the collection, disclosure and use of personal data illegally, but also needs to formulate burdensome elements if the misuse of personal data causes a serious impact on victims.

Keywords: *Online Shaming, Digital Persecution, Protection of Privacy Rights.*

INTRODUCTION

The world today is referred to as a global village. This situation was predicted by Marshal Mc Luhan, in 1960. He stated: *"We would live in a state of 'new electronic interdependence' in a "global village"* (Mc. Luhan, 1962:36). With the sophistication of information technology, everything happens at a rapid pace. The speed of this electronic media will connect us, and society can act and react to global issues instantly, continuously, and collectively (Mc. Luhan, 2021:63). Currently, the speed of information that is spread in a matter of seconds makes people so reactive. The public can comment freely on news about someone. The people who are reported can come from ordinary citizens, or public

[A]*Faculty of Law and Digital Business, Universitas Kristen Maranatha, Bandung, Indonesia, Emai: rahel.octora@law.maranatha.edu*
[B]*Faculty of Law and Digital Business, Universitas Kristen Maranatha, Bandung, Indonesia*

figures. When someone becomes the object of the news because of their bad actions, internet users (netizens) attack the person in various ways.

People who are considered to violate social norms are judged in cyberspace. His private space was then disturbed by thousands or even millions of negative comments from the public. Even more terrifying, when someone is just considered annoying by netizens, netizens can attack the person's personal through various ways, including by looking for the person's social media accounts, email addresses, or personal phone numbers. Netizens deliberately and contacted the person to make negative, insulting, threatening, and/or blasphemous comments. Someone who is being targeted by netizens is in a very risky situation. His personal data became a target, to be disseminated and become an entry point for attacks on individuals, from a crowd of internet users who were mostly unclear about their identities. It is undeniable that some internet users are also anonymous users. This situation illustrates the existence of one person who was attacked by millions of anonymous people, and he experienced persecution in cyberspace. This action is called online shaming.

Online shaming can be defined as follows: *"online shaming refers to a systematic activity aiming at silencing people or harassing them, for example, by threatening them or disseminating their private or untrue information on the internet*" (Koivukari & Korpisaari, 2021:476). With the growing use of the internet around the world, online shaming occurs in almost all parts of the world. A person who is considered guilty by the public (internet user community/netizens) is immediately attacked without the need to wait for a court decision that declares him guilty. This is contrary to the principle of "presumption of innocence", where a person is presumed innocent until there is a court decision stating otherwise. Online shaming shows that vigilante practices are starting to occur in the cyberspace.

Internet users nowadays tend to feel free to speak, so they have a habit of trolling. The word "trolling" from an English verb that portrays angling with a bedevilled line, is utilized to allude to communicative incitement outlined to incense other clients: to incite outrage and wrath or to form them feel dissatisfaction and fear. Trolling infers making a circumstance of struggle and abusing the unwritten rules of online communication (Zvereva, 2020:108). Trolling actions can trigger provocation. The activities of online provocateurs can be seen from the viewpoint of cyber-interaction morals, with analysts basically passing judgment on the trolls' "anti-social behaviour." (Shin, 2008)

Through digital means, individuals can use technology to ridicule or intimidate others. For instance, someone might circulate false information about another on Facebook or post unappealing pictures to tease someone regarding their looks. Just like traditional bullying, online or cyberbullying aims to embarrass or scare someone. However, online harassment can impact a wider group of people (Hamiltion, 2017:9).

Indonesia is a country with the largest number of internet users. According to data provided by The Indonesian Internet Service Providers Association, (apjii.or.id), Indonesian internet users in 2024 will reach about 221 million people out of a total population of 278 million. This affects the high potential for various violations of the law. The law exists to answer the needs of the community, including the need for legal protection. Thus, it is important to research whether the regulations currently in force in Indonesia are sufficient to protect the dignity and privacy of a person who is disturbed by online shaming?.

This study aims to analyze how Indonesian law can protect citizens from acts of digital persecution through online shaming. In addition, this study seeks to examine how the government should formulate and implement personal data protection policies in order to safeguard citizens' rights to privacy and dignity in the digital era. Through this analysis, the research is expected to contribute to strengthening legal protection and policy frameworks related to digital rights and personal data protection in Indonesia.

LITERATURE REVIEW

Online shaming shows the phenomenon of Vigilant Audience. A vigilant audience is defined as a judging audience. These spectators target someone, then attack him in various ways, including criticizing, humiliating, and doxing. In this article, it should be emphasized that online shaming is a different thing from doxing. Online shaming shows the activity of netizens who are massive in making comments that embarrass someone who is the target, while doxing is the activity of dismantling the personal identity of someone who is the target, to facilitate the goal of humiliating the target. According to Garrigues, *et.al.,* digital vigilantism indicates a significant change in the circumstances surrounding the use of digital media, suggesting the dissolution of a previously established separation between online actions and their offline repercussions (Garrigues, 2020:190). Social media has been chosen as the online media platform where online shaming postings are commonly found ahead of other online platform such open forums, online news, and blogs. (Mahmood et al., 20018:1132). Shenton argue about 'social media poetics' concept. Social media poetics happen when online communities of people who, relative to the state and to one another, send essentializing strategies to disgrace each other and in so doing make themselves which they contradict (Shenton, 2020:172).

John Braithwaite made a distinction between reintegrative shaming and disintegrative, stigmatizing shaming. Reintegrative shaming focuses on sending a message of disapproval about the behavior while still recognizing the individual as a decent person who has committed a wrongful act. On the other hand, disintegrative shaming associates the person entirely with their actions, viewing them as someone beyond help. Thus, the main difference that distinguishes reintegrative shaming from disintegrative shaming is the approach to "the labeling of offenders." (Rosenberg & Peleg, 2024:12). Social norms

play a crucial role in online shaming, as they establish a limit that helps to distinguish the reasons behind online shaming from other behaviors like cyberbullying or cyber harassment (Packiarajah, 2017:6).

Some definitions of doxing to clarify the limits/scope of the activity in question, are as follows:

1. "Doxing" (or sometimes "doxxing") comes from an alternative spelling of the abbreviation of documents, i.e., "docs," prevalent in the hacker world. It originally referred to documenting, compiling, uncovering, and/or releasing personal data on an individual or group on the internet. The term was first used in the 1990s in the context of hackers doxing a rival hacker (Cooper, 2019, Cheung, 2021:579).
2. Doxing is the intentional public release onto the Internet of personal information about an individual by a third party, often with the intent to humiliate, threaten, intimidate, or punish the identified individual (Douglas, 2016:199).
3. Oxford British and World English Dictionary define *doxing* as "search for and publish private or identifying information about (a particular individual) on the Internet, typically with malicious intent" (Douglas, 2016:199).

Thus, it can be concluded that doxing is an act carried out for evil purposes, including online shaming to the person who is targeted. The phenomenon of doxing is not only a problem for certain countries. The development of the use of the internet and the shift of places of human interaction from the real world to the virtual world, has made doxing a legal problem faced by almost all countries in the world. Some of the examples below show the occurrence of doxing and online shaming, which occurs in various countries:

1. In China, the internet is often used to inform about someone whose actions are contrary to norms. The things exposed included the identity of the cheating husband, the person who committed animal violence, the identity of the student who was considered a traitor for showing sympathy for the Tibetan independence movement, and so on (Cheung, 2021:7).
2. In Korea, there was a case of a student from a university who did not want to clean the dirt on his pet dog's face while riding the subway train, she was nicknamed The Dog Poop Girl, and that story was widely spread on the internet, and published in the Washington Post (Cheung, 2021:8).
3. In the Netherlands, a 68-year-old woman was caught on camera while taking someone's wallet. Footage from the camera was spread on television programs about crime. The woman turned herself in to the police. The footage was continuously spread on the internet until it was seen by millions of people. The website that broadcasts it has a comment column, and viewers write scathing and malicious comments. Shortly after the incident, the woman committed suicide (Trottier *et al.,* 2000:2).

4. In Indonesia, a debtor who experienced a default, became a victim of doxing activities carried out by collectors from online loan companies. Doxing victims are debtors who are considered not to pay debts. Her personal data was disseminated to the public with a narrative that embarrassed the victim. The narrative that spreads is that the victim opened a sexual service (news.republika.co.id).
5. In Indonesia, there was also a case when a woman was caught stealing chocolate at a minimarket, the video went viral and then the woman sued the minimarket employee who went viral based on defamation. Netizens then increasingly attacked the woman. Her personal data was sought by netizens, then netizens attacked the perpetrator by leaving negative comments on her google business account (inet.detik.com).
6. A state-owned employee in Indonesia was involved in a quarrel with another person because he stopped his car carelessly and made the roads jammed. When reprimanded, he was angry and spat at the party who reprimanded him. The video went viral, netizens searched for the identity of the person and after his place of work was known, the information was spread to the public. Finally, he was dismissed from the company where he worked (idntimes.com).
7. Jeniffer Castro, a bank employee from Brazil, filed a lawsuit against the airline after her video went viral for refusing to switch seats with a young child on the flight. The child wanted the window seat, but Jenifer refused. Her action was recorded by another passenger and circulated online. She feels that she has experienced public shaming (nypost.com).

From the cases mentioned above, the core of the problem that occurred is that there are actions of a person that cannot be accepted by society because they are considered contrary to social norms (norms of morality, politeness, propriety, or legal norms). As a result, the community imposes 'sanctions'. The imposition of social sanctions is a natural thing to happen. A person who violates the norm will receive blasphemy and/or exclusion from the environment. However, currently social sanctions are imposed through the internet. The reach of the audience that sanctioned and witnessed the imposition of sanctions became very wide and unlimited. Therefore, it is appropriate to discuss whether we should justify the imposition of social sanctions or whether there is a right of a person who needs to be protected, then the law should provide limits on how social sanctions can be imposed.

From the point of view of sociology, sanctions are part of the social control mechanism. According to Durkheim, *social control is traditionally conceived as efforts to oppose deviance or encourage conformity to norms.* From the perspective of sociology, social control can be divided into two forms, namely informal and formal forms. Informal control refers to the internalization of norms through the process of socialization. An individual who has the potential to engage in various behaviors is guided

to develop their behavior in a limited way. Formal control, on the other hand, involves the imposition of sanctions by authorized parties, including the government, as a preventive effort to avoid chaos or anomie. Emile Durkheim referred to this form of control as regulation. (socialsci.libertext.org)

According to Jennifer Forestal: “Informal social sanctions can take many forms, including public shaming. As ‘a practice of public moral criticism in response to violations of social norms’ (Billingham and Parr 2020a, 997), the goal of public shaming is twofold. First, public shaming “motivates individuals to accept responsibility and take reparative action in the wake of violating social norms (Tangney, Stuewig, & Mashek 2007:355); it also deters future norm violations by others (Finnemore & Hollis 2020; Krain 2012; Forestal, 2024:1706).

Based on the definition above, it appears that sanctions are a good instrument in the implementation of the social control process. With the social changes that occur in the form of shifting the interaction space to the cyber space, the imposition of sanctions by internet users has deviated from the purpose of imposing sanctions. Sanctions are no longer used to encourage a person to act in accordance with applicable norms. One of the purposes of imposing sanctions is to provide a deterrent effect for someone who is considered to have violated the norm. Someone who has violated the norm will certainly feel deterred after being humiliated. The thing that needs to be paid attention to is that the "shame" felt by the perpetrators of violation of norms influences the loss of "sense of security" both physically and mentally. Low self-awareness led to consequences to emotional wellbeing, as results from violating norms, such as disgrace, blame and shame (Vasalou et al., 2006:108).

Social ontology turns into A helpful premise for describing how social tensions and instances of social media shaming might arise from people with diverse views and presumptions coexisting online (Huffman, 2016). Online shaming seems to become a way for enforcing norms without a proper mechanism. Krista K. Thomason, quotes Nussbaum statement: “Some philosophers express this concern as a need of due process. For case, Nussbaum argues that disgracing is associated to justice by the mob, which isn't deliberative, fair-minded, or impartial (Nussbaum 2004:234). Solove objects that there are no rules to guarantee that the web standard police craftsmanship exact in their assessments of who would be regarded blameworthy (Thomason, 2024:154).

Though situations revealing unlawful actions or systemic wrongs were mostly seen as warranted, instances of personal grudges, deceitful information, and public shaming were regarded with doubt and ethical uncertainty (Howes, 2024:9).

Central results for people who were disgraced online included harm to mental and social prosperity, money related/ business misfortunes, mistreatment past the web into their every-day lives, and avoidance from development (these impacts were ordinarily show in

accounts where online disgracing was delineated as destructive) (Muir *et al.*, 2021:7).

Online shaming is a consequence of the occurrence of imaginary relationships in interactions between individuals in the virtual world. According to Norlock, (2017), social psychologists of imaginal relationships indicate that we all have relationships that we endow with imaginative content which includes their significance, meaning, and membership. Although the relationships that emerge are imaginary, when a humiliating attack occurs against someone, the victim cannot simply ignore the attack. The potential for physical and/or mental disturbances is very likely. Therefore, the law needs to be present to regulate this phenomenon.

Online shaming does not stop at the activity of shaming someone. Online shaming is often followed by doxing activities. The person's personal data is disseminated so that he or she receives terror or direct physical threats. Sanctions, which were originally used for the purpose of social control, are instead used as a tool of persecution that violates the boundaries of the right to privacy and degrades human dignity. This also affects the personal lives of people who are victims of online shaming and doxing.

According to Professor James Whitman: “this act of online shaming is an act of intuitively barbaric, as society displays its disdain or disapproval for personal errors by subjecting the offender to a unique type of vulnerability, which can strip the offender of their dignity and identity." (Cheung, 2012:1)

From a legal point of view, online shaming shows the occurrence of rights violations. Human beings have the right to be respected for their dignity. Article 1 of the Universal Declaration of Human Rights states that "All people are born free and have the same dignity and rights." Dignity can be defined as an intrinsic value in every human being that makes human beings have freedom from humiliation, and human beings have freedom in the development of physical and psychological integrity. In addition to the right to dignity, humans also have the right to privacy or personal life. Another important right is the right to private life. This covers the physical, psychological, and moral integrity of a person, as well as the right to establish and develop relationships with other human beings. The right to private life gives protection against public dissemination of a person’s private information or photos in situations where individuals can legitimately expect that that kind of information is not published without their prior consent (Koivukari & Korpisaari, 2021:474).

The existence of the law is necessary to protect these rights. Law is not only a means of regulating behavior. The law is expected to be a means to protect the community from various potential rights violations. Hadjon (1987:2) categorizes legal protection into two types: preventive and repressive. Preventive protection refers to the measures taken to avert a crime before it occurs, while repressive protection focuses on addressing conflicts, including their management within judicial entities.

Along with the development of people's lives, the concept of legal protection has also evolved. Currently, people's lives occur both in real and virtual scopes. The use of technology, especially the internet, has led to social interactions in the virtual world. According to the United Nations Human Rights Council Resolution on July 1, 2016, regarding the Promotion, Protection, and Enjoyment of Human Rights on the Internet, it was stated that the protection of human rights applies not only in real life but also in virtual interactions.

Laws in various countries still struggle to regulate the phenomenon of online shaming. In this case, there is a clash between the right or freedom of speech and the right to privacy. Uncontrolled freedom of speech can lead to potential insults and violations of others' rights. These privacy interests immediately rub against free speech rights, and we should be concerned with formulating a privacy right that drifts into the territory of regulating meanness and offence. However, the failure to address the gap in privacy law concerning the public and social dimension of privacy has left many victims without legal recourse in the face of brutal abuse (Laidlaw, 2017).

In the context of Indonesian law, online shaming has not been comprehensively regulated. A person who makes bad comments about others can be subject to criminal sanctions on the basis of insult/defamation. The problem becomes different when the party who makes bad comments is not just one person, but many people with unclear identities. People who are targeted by online shaming cannot take any legal steps, because there are too many parties they are opposing. Similarly, the disclosure of personal data also needs attention. The act of a person deliberately disclosing another person's personal data to the public domain can have serious consequences.

METHOD

This research uses a normative legal method. In other words, this study only examines legal aspects without conducting sociological or empirical studies. The materials studied are laws and regulations. This research also involves a stage of literature review to understand various legal concepts (conceptual approaches). The researcher will analyze the regulatory framework related to online shaming as a form of digital persecution, protection of dignity and privacy rights of victims in Indonesian legal framework.

RESULTS AND DISCUSSION

Analysis of Legal Protection for Victims of Digital Persecution through Online Shaming in the Framework of Indonesian Law

The Constitution of Indonesia declares that Indonesia is a Law State. The consequence of running a state of law is that the state must be able to guarantee justice for its citizens. Justice is always related to legal certainty. The existence of legal certainty provides a guarantee of the consequences of every act that is categorized as a violation of the law and/or an act that violates the rights of others. With the imposition of

sanctions for law violators, this means that the state has provided legal protection for citizens whose rights are violated. The sanctions imposed must be based on the applicable legal provisions. This is also one of the characteristics of the guarantee of legal certainty.

Law is a system. A system is a unit that operates within certain limits. A legal system in its actual operation is a complex organ in which structures, substances, and cultures interact. (Friedman, 1975:17). To solve various legal problems, a system approach is needed. Thus, the government cannot focus solely on rulemaking to cover the absence of rules. The government also needs to pay attention to how the law enforcement structure works in the context of a concrete community situation.

In this paper, the phenomenon that will be discussed is the act of online shaming and doxing. If we look at the impact caused, online shaming and doxing have a serious impact on victims. The possible impacts, explained by previous researchers, are as follows:

1. When a negative comment about someone appears on social media, it can prompt other users to do the same to the targeted person. Bad comments can appear in various forms, ranging from mockery, threats, and even the spreading of private data (Koivukari & Korpisaari, 2021: 477).
2. Perpetrators of doxing not only target the victims themselves but also the people around them, including their family and relatives. This means that the personal data being spread often includes the personal data of the victim's family or relatives. As a result, the victim feels more anxious due to threats to their own safety and that of their family (Noval, 2021:4).

Losses are not only experienced by the victims, but also their families, including: harassment, disturbances, threats directed at the targeted person, potential physical and mental/psychological disturbances, losses due to anxiety about safety, and damage to property (Uweng *et al.*, 2023:173).

Indonesia needs to ensure that there are comprehensive regulations to overcome this phenomenon. Citizens need to obtain protection from various attacks or disturbances. Citizens have the right to protect, one of which is related to their personal security. The state has a variety of legal instruments. Criminal law is one of the areas of law that regulates the actions of citizens who are considered to interfere with public interest. Criminal law establishes various prohibitions and sanctions for violations that occur.

Criminal law is public law that regulates the actions of legal subjects, containing obligations and prohibitions, rights and duties, as well as sanctions imposed when violations occur. The existence of criminal law in a country aims to provide security guarantees for the community. Criminal law as public law aims to protect the public interest. Any perpetrator who commits an act that is unlawful and detrimental to the public interest will be subject to appropriate sanctions. The suffering experienced by the perpetrator because of his

actions is expected to have a deterrent effect and prevent others from committing the same crime. In principle, criminal law aims to tackle crime.

Different crimes, of course, must be tackled with different approaches. Criminal law as a system does not only contain rules with sanctions. These rules were born as an implementation of a policy. In criminal law, we know the term "criminal law policy." Criminal law policy is also an important thing to discuss considering that the purpose of criminal law implementation is to overcome crime. One part of the criminal law policy formulation stage is the formulation stage or the rule preparation stage. The preparation of rules must pay attention to the characteristics of the crime to be regulated. Criminal law policies in the context of countering cybercrime certainly need to be carefully prepared and consider whether the policies prepared in the form of rule formulation can be implemented properly until the execution stage. The term cybercrime refers to a criminal activity that uses a computer or internet network as a tool to carry out criminal acts.

It should be noted that criminal law events can occur even without a meeting between the perpetrator and the victim. Indonesia's criminal law system regulates internet use activities in Law Number 11 of 2008 as amended by Law Number 19 of 2016 and finally with Law Number 1 of 2024 concerning Information and Electronic Transactions (IET Law).

The criminalization of unlawful acts in the use of information technology in Indonesia is based on various considerations that are explicitly mentioned in the EIT Law considerations, including:

1. Technological advancements have changed human activity patterns and have given rise to various new legal actions.
2. The digital space must be clean, healthy, ethical, productive, and fair. Rules regarding the use of information technology and electronic transactions must be able to create justice and legal certainty and protect the public from potential harm caused by misuse.

In this consideration, it appears that technology is causing new legal acts, including new crimes. This research discusses how a person who is considered to violate norms, then subjected to digital persecution, by being humiliated, having his personal data disseminated, threatened, scared, and so on. To answer the needs of the community to overcome this phenomenon, the Indonesian ITE Law still has many limitations. The new Indonesian ITE Law regulates the crime of defamation, extortion, and intimidation, with the following formulation:

1. Article 27 paragraph (3) of Law Number 11/2008: Every Person intentionally and without the right to distribute and/or transmit and/or make accessible Electronic Information and/or Electronic Documents that have insulting and/or defamatory content.
   Explanation of article 27 Paragraph (3): The provisions in this paragraph refer to the provisions of defamation and/or defamation regulated in the Criminal Code (KUHP).
2. Article 27 paragraph (4) of Law Number 11/2008: Every Person

deliberately and without rights distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents that have extortion and/or threatening content.
Explanation of Paragraph (4): The provisions in this paragraph refer to the provisions of extortion and/or threats regulated in the Criminal Code (KUHP).

3. Article 29 Number 11/2008: Every Person knowingly and without rights sends Electronic Information and/or Electronic Documents containing threats of violence or intimidation aimed at individuals.
4. The rules have undergone changes based on Law Number 1 of 2024. Currently formulated: Any Person knowingly and without rights sends Electronic Information and/or Electronic Documents directly to victims that contain threats of violence and/or intimidation.
   Article 27A of Law Number 1/2024: Every Person deliberately attacks the honor or reputation of another person by accusing a matter, with the intention that it is publicly known in the form of Electronic Information and/or Electronic Documents carried out through the Electronic System.

From the four articles mentioned above, we know that Indonesia's criminal law is still unable to reach the massive online shaming action. The article on insult/defamation has limited reach. The article of insult/defamation is regulated in the Criminal Code. In the Criminal Code, it is stated that insult/defamation can be prosecuted based on victim's complaint.

In the case of online shaming, it will be very difficult for the victim to process the insult carried out by a large number of people whose identity is unknown. Thus, the law is confronted with the following problems: 1) The limitations of the law enforcement system in reaching so many perpetrators; 2) Many of the perpetrators are anonymous internet users.

The phenomenon of using anonymous accounts shows a change in people's behavior patterns. Anonymous account users feel free to act because no one knows their identity. The number of anonymous accounts is very large; it is very possible to send electronic information containing threats to one target. Another proposed contributing factor of online disgracing is online disinhibition, which could be a condition whereby individuals feel less limited and are more willing to show themselves openly on the web than in private space. Many ponders have illustrated expanded animosity and threatening practices in computer-mediated interaction compared to face-to-face interaction which may contribute to the "mob mentality" frequently seen online (Muir, *et al.*, 2023:15).

Psychologists point to several factors' online cruelty to flourish: 1) The anonymity of the internet; 2) The distance or lack of face-to-face contact with a victim; 3) Mob mentality; 4) Lack of gatekeepers; 5) Lack of consequences (Lewinsky, 2017).

Criminal law enforcement procedures (that are bound by the provisions of the criminal procedure law), will certainly face many obstacles when faced with cases of insults and threats that occur through social media. The victim must report to the police. The police who received the report could not easily determine who should be designated as a suspect.

Not only in Indonesia, but European people also find the same difficulties in overcoming the phenomenon of online shaming. From the perspective of European society, the criminalization of online shaming clashes with the principles of legality, individual autonomy, and the protection of freedom of expression. This was expressed by the previous researcher in the following statement:

1. "The possibility or even need to criminalize shaming actions is examined through restrictions that the principles of legality and individual autonomy along with the requirements of freedom of expression, provide when criminalizing conduct initiating shaming or participating in shaming. The starting point must be freedom of expression as protected by Article 10 of the ECHR, and the fact that according to the ECtHR, this protects expressions broadly, including even expressions "that offend, shock or disturb the State or any section of the population" (Koivukari & Korpisaari, 2021:480).
2. "Although restricting freedom of expression is possible, restrictions are limited inter alia to those necessary in a democratic society. As for the idea or principle of legality, this is a fundamental part of any democratic Rule of Law Country, and is written, for example, into the European Convention on Human Rights (Article 7) as well as national constitutions and criminal laws" (Koivukari & Korpisaari, 2021:480).

Moreover, the principle of individual autonomy presumes that "each individual should be treated as responsible for his or her own behavior", which in turn must be respected in criminalizing any conduct" (Asworth, 2009:23). Each state has different regulations in its criminal laws related to acts of online shaming. Often, the rules regarding such violations are broad and may involve more than one party. Acts of online shaming are complex, and because the rules are spread across various regulations, these cases are difficult to handle (Koivukari & Korpisaari, 2021:478).

Criminal law cannot be fully relied on to overcome new crime phenomena, especially in the field of cybercrime. Digital persecution through online shaming is an act that harms a person. A person who is humiliated through the internet media will find it difficult to get legal protection, considering that the perpetrators of online shaming are unknown people, namely anonymous account users who have a very large number. It is impossible to act against all internet users who write bad comments against someone.

The aggrieved party can only process a few perpetrators who are considered the most detrimental. The perpetrator who is considered the

most detrimental is someone who is the initiator of online shaming. An initiator is a person who starts the process of spreading information. The actions taken by the initiator can trigger others to join in attacking the target. Attacks can take the form of comments, sending messages, sharing other people's comments, liking posts, and other actions that result in interaction with the link. These actions are aimed at attacking the target, embarrassing them, expressing negative emotions, and so on (Koivukari & Korpisaari, 2021:478).

Although the initiator was processed according to the rules of criminal law, this did not stop online shaming that has occurred massively. Criminal law policies are certainly different in each country. European countries provide protection for the right to express criticism. There are unclear boundaries when someone writes a comment in the form of criticism of someone's behavior. The criticism may get the attention of many people and then provoke an angry reaction from many people. The act of initiating the writing of criticism cannot be categorized as online shaming.

Similarly, in Indonesia, based on the Joint Decree between the Minister of Communication and Information of the Republic of Indonesia, the Attorney General of the Republic of Indonesia, and the Chief of the National Police of the Republic of Indonesia on the Guidelines for the Implementation of the EIT Law, defamation must be assessed based on what the perpetrator has done. The focus of punishment is associated with the perpetrator's actions, not the feelings of the victim. In principle, criticism cannot be criminalized. The feelings of the person being criticized, whether he is disturbed and so on, cannot be used as a basis for criminalizing such actions. In practice, it will be difficult for law enforcement to distinguish between statements made by a person to criticize, or to embarrass.

Online shaming as a form of persecution clearly causes problems for the victims who are targeted, but using criminal law rules to provide protection for victims is not the right way. The author argues that the phenomenon of online shaming leads to a social problem, namely a change in people's behavior patterns and changes in people's reactions to acts of violating the law, violating morals and/or propriety committed by others. The phenomenon of vigilant audiences is a social problem.

Therefore, other policies are needed to solve this problem. The policy in question is a non-penal policy. Non-penal policy is a crime prevention by removing the conditions that cause crime, or it can be said that crime prevention efforts must be based on handling problems or social conditions. (Frens & Zulyadi, 2023:73). According to Barda Nawawi Arief, there must be an integration between the attempt of overcoming crimes and using the means of penal policy as well as the means outside the criminal law or non-penal policy (Arief, 1992:149).

The non-penal policy refers to various efforts to prevent violations of the law. To overcome this problem, education is needed for internet users, related to the ethics of using the internet. On the other hand, there is a need for a content filter mechanism. Until now, electronic system

operators, especially social media applications, have not screened comments on news content uploads. Comments containing the disclosure of a person's personal data are still so accessible. The electronic system operator needs to establish terms and conditions of use, where the application operator has the right to block users who disclose the personal data of other parties.

Comments that contain hate speech and bullying can be overcome with a technological approach. There is various software such as *Bully Button, ReThink Stopcyberbullying, take a Stand Together, Safe Eyes Mobile, Knowing Bullying, dan Bullying Block* (Thun *et al.,* 2022). Software such as ReThink Stopcyberbullying aims to protect internet users from acts of bullying in cyberspace. The software aims to warn users not to commit acts of bullying in cyberspace and to filter (filter) every typed text if it has offensive content. With software that prevents bullying in cyberspace, it will create a safer and more comfortable cyberspace (Frens & Zulyadi, 2023:76).

Based on the explanation, it can be concluded that the phenomenon of online shaming is a form of social sanction against someone whose actions are contrary to the norm. The law cannot provide protection to victims of digital persecution. Criminal law and the threat of sanctions will never be able to stop the circulation and spread of bad comments that have already been circulated. Criminal law needs to define the terminology of "initiator", to be able to sanction parties who meet the category of initiators of digital persecution. The determination of the initiator category can be based on:

1. Who first uploaded the news about someone's (victim's) actions.
2. Users with a significant number of followers, who if they upload or repost a piece of content, can bring in a large number of provoked netizens as well.

China regulates insult/defamation activities quite specifically. In Article 246 of the Criminal Law, it is stated: Acts of violence or other actions intended to insult or demean another person; or acts of spreading false information to defame someone, if meeting the criteria of a serious situation, are punishable by a maximum of three years in prison, short-term detention, controlled release, or revocation of political rights.

A 2013 judicial interpretation jointly released by the Supreme People's Court and Procuratorate concerning the online defamation under article 246 made international news because it considered the number of 'clicks' and 'views' as a measure of how serious the offense was. Specifically, it defined 'serious circumstances' as requiring:

1. 5,000 or more clicks or views, or 500 transmissions.
2. Serious harm to the victim, such as suicide, psychological aberration etc.
3. An offender who has previously received an administrative punishment for defamation in the last two years, or
4. Other serious circumstances.

Indonesia can regulate online shaming as a mode of digital persecution, by modifying the defamation/insult article. Initiators can be

punished with heavier sanctions if their actions cause consequences including:

1. Widespread and uncontrolled (viral) spread of electronic information
2. Serious losses for the victim, e.g. suicide, psychological disorders, etc.

Analysis of the Personal Data Protection Policy to Protect the Right to Privacy and Dignity of Citizens

The core difficulty in assessing directors' liability in state owned enterprises lies in the collision of two evaluative grammars that were designed for different objects and different anxieties. The Business Judgment Rule is built to protect informed managerial discretion under uncertainty, because corporate value creation presupposes calculated risk, probabilistic forecasting, and occasional failure.

In this sub-section, it will be described how the government must establish a personal data protection policy in order to protect the right to privacy and dignity of citizens. The phenomenon of doxing activities raises problems related to the protection of a person's personal data. A person's personal data is widely spread without the permission of the owner, which can raise the problem of misuse of personal data that will cause losses.

The General Data Protection Regulation (GDPR) is a regulation that is the basis for regulating personal data protection in various countries. Based on Article below:

> Article 1(2): This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
>
> Article 5(1) b: Personal data shall be: collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

From the two articles above, we can see that the GDPR provides the principle of personal data management, namely the principle of protection of personal data, and the principle of collection and processing of personal data must be based on legitimate purposes, and not for unlawful purposes. Along with the development of social interaction patterns, the imposition of social sanctions for a person is currently carried out in cyberspace. Cyberbullying is one of the rampant actions that occur in cyberspace. Cyberbullying is a repetitive behavior aimed at scaring away, angering, or humiliating those targeted.

Cyberbullying is often followed by doxing. In simple terms, doxing can be interpreted as the activity of disclosing someone's personal data without the consent of the data owner. Doxing perpetrators have a negative purpose, namely, to embarrass someone, intimidate, threaten, and so on. This shows that there has been a deviation from the principles

of data collection and processing as mandated in the GDPR. This deviation must certainly have legal consequences.

Doxing is divided into: deanonymization, targeting, and delegitimization. Deanonymization is the disclosure of the identity of an individual or a group of people who were previously unknown (anonymous), or who appeared under a pseudonym. This action reveals the real name of the target. Targeting is the act of searching for and finding specific information about someone, including specific locations occupied or visited by the target, enabling the target to be subjected to direct physical attacks. Delegitimization is the act of sharing someone's personal information. The purpose of delegitimization is to damage the credibility, reputation, and character of the victim. Doxing is carried out to embarrass and harasses the victim.

Snyder and colleagues (2017) highlight four main reasons for doxxing through their study: (1) competitiveness: showcasing greater skills in A specific subculture; (2) retaliation: doxxing as a form of vengeance for a perceived wrong done to the attacker; (3) justice: doxxing in reaction to someone performing an action considered unethical or unjust; and (4) political: doxxing to support a cause that transcends simply targeting one individual (Anderson & Wood, 2021:215).

Based on the above understanding, doxing is an act that can cause consequences for the victim. Victims can suffer serious losses. Doxing can have an impact on cancel culture. Cancel culture can be defined as the action of society to isolate or ostracize someone who violates social norms. This action is an act of exclusion. Doxing on social media is related to cancel culture because it involves a large and open public and aims to humiliate individuals, to bring down doxing victims, to damage reputations, to end careers, and to incite the masses to take certain actions. (Noval, 2021, p. 363). Exclusion is felt by the victims in their real-life experiences. For example, they may lose relationships with others, lose their job, have difficulty earning money, and struggle to make a living.

Doxing refers to the act of gathering and revealing private information, which falls under data processing according to privacy regulations. Typically, personal information can be handled only with the clear approval of the individual involved and under specific circumstances. Nevertheless, online harassers often argue that they utilize information that the individual has already made public, which they believe means they do not need to secure the individual's consent. Contrary to such assertions, this article clarifies that the principle of purpose limitation forbids the use of personal data for doxing, irrespective of whether that information is available to the public (Kukul, 2023:192). Doxing discussions can be broadened in relation to the diversity of society, the behavior of governments, and the restrictions on free speech in public spaces (Novianty *et al.*, 2023:10).

In Indonesia, while the laws on personal data protection and electronic information along with transactions lay a legal groundwork to combat doxing, the enforcement is still inadequate due to restricted

investigative abilities and a lack of public understanding of the law. Such circumstances present major challenges in recognizing and taking action against offenders, particularly in instances that involve anonymity or cross-border legal issues (Utami, 2025:160).

Related to doxing activities, the laws and regulations in Indonesia that regulate include:

1. Law Number 24 of 2013 concerning Citizenship Administration
   Article 95 A: Anyone who disseminates Population Data without authorization as outlined in Article 79 paragraph (3) and Personal Data mentioned in Article 86 paragraph (1a) shall face a prison sentence of up to 2 (two) years and/or a maximum fine of twenty-five million rupiah.
2. EIT Law
   Article 26 paragraph (1) of the EIT Law which emphasizes that: "The use of any information through electronic media that concerns a person's personal data must be done with the consent of the person concerned". In the EIT Law, there are no rules related to sanctions for the actions of a person who violates the provisions of Article 26 paragraph (1) of the EIT Law.
3. Personal Data Protection Law (Law Number 27/2022)
   Article 1 point 1 of the Law states that personal data is data about an individual that can be identified either separately or in combination with other information. Identification can be carried out directly or indirectly, through or without the use of electronic systems. Article 1 point 2 states that Personal Data Protection is an integrated effort to protect personal data, in order to safeguard the constitutional rights of citizens.

Some important things related to the Personal Data Protection Law (PDP) are that the PDP Law regulates the relationship between the owner of personal data and the controller of personal data. Thus, the rules contained in the PDP Law are dominated by rules related to the rights and obligations of personal data subjects and personal data controllers. Some of the terminology explained in the PDP Law includes:

1. A Personal Data Controller refers to any person, governmental entity, or international organization that independently or collaboratively decides the objectives and manages the handling of Personal Data.
2. A Personal Data Processor refers to any person, legal entity, or international organization that operates independently or collaboratively in handling Personal Data for the Personal Data Controller.
3. A Personal Data Subject refers to a person who possesses Personal Data associated with them

Regarding the act of doxing carried out by an individual, the regulation is contained in Article 65 PDP Law which states:

1. No individual is allowed to illegally acquire or gather Personal Data that isn't their own for personal gain or for the benefit of others, which may lead to harm for the Personal Data Subject.

2. No individual is allowed to unlawfully reveal Personal Data that is not their own
3. Any Person is prohibited from unlawfully using Personal Data that does not belong to him.

For these acts, criminal sanctions may be imposed as stipulated in Article 67 of the PDP Law as follows:

1. A maximum sentence of five years in prison and/or a maximum fine of Rp 5,000,000,000,000 (five billion rupiah) will be imposed on anyone who willfully and illegally obtains or collects Personal Data that does not belong to them or others with the intention of causing losses to the Personal Data Subject as intended in Article 65 paragraph (1).
2. A maximum penalty of four years in jail and/or a maximum fine of Rp 4,000,000,000.00 (four billion rupiah) will be imposed on anybody who willfully and illegally exposes personal information that does not belong to him as intended under Article 65 paragraph (2).
3. A maximum penalty of five years in jail and/or a maximum fine of Rp5,000,000,000.00 (five billion rupiah) will be imposed on anybody who willfully and illegally utilizes personal data that does not belong to him as intended under Article 65 paragraph (3).

Indonesia has formulated the act of doxing as a criminal offense. The criminalization of doxing has not effectively stopped the rampant act. Many factors trigger the ease with which doxing perpetrators spread someone's personal data. Users of various social media platforms such as Instagram, Facebook, Linked In, often publish their identities. Anyone can easily know a person's name, where he lives, where he goes to school, where he works, and even his family identity.

The issue of doxing in Indonesia is further aggravated by the insufficient digital literacy (Bulya & Izzati, 2024). A significant number of people are unaware of the necessity of protecting their information, leading to the spread and abuse of private data by those without permission (Sihidi, 2025; Ayu, 2025).

Oversharing has become a major obstacle in preventing the crime of doxing. Everyone has the potential to become a victim, and they consciously provide their personal data to be easily accessed by others. Accoding to Gupita (2023), in the context of excessive sharing cases, the relationships between the actors should be as follows:

1. Relationship between citizens and the government: 1) Government to citizens: providing protection and empowerment to citizens, 2) Citizens to the government: reporting mechanisms for follow-up actions.
2. Relationship between Social Networking Sites (SNS) and the government: 1) Government to SNS: they must be regulated to protect citizens from harm., 2) SNS to the government: platform compliance and reporting mechanisms for follow-up actions.
3. Relationship between citizens and SNS: 1) SNS to citizens: implementing government regulations as well as additional

protection and privacy frameworks for safer social media use. 2) Citizens to SNS: direct reporting mechanisms to the social media platform in case of violations or personal data issues".

Stamos (2019) highlights the necessity of strong password habits, using multiple authentication methods, and careful sharing of information online, including notifying law enforcement, keeping a careful eye on one's online presence, and protecting any sensitive data that has been breached (Zhou & Bottlapally, 2025:2429).

Given the rampant misuse of personal data in various parts of the world, countries have also developed personal data protection regulatory systems with various formulations.

1. China
   Article 253-1: Breach of Personal Information of Citizens: Breaching state regulations by selling or sharing citizens' personal information in severe circumstances may result in imprisonment for up to three years or short-term detention, and/or a fine; if circumstances are particularly serious, the punishment ranges from 3 to 7 years of imprisonment along with a concurrent fine.
   Definition of "circumstances are serious": Selling or providing citizens' personal information to others that one knows, or should know, will be used to perpetrate crimes;
   Definition of "circumstances are especially serious": leads to death, serious injury, trauma, or kidnapping; causes major economic loss or vile social impact.
2. Singapore
   Skoric, *et al.*, in their research on Online Shaming in the Asian Context, highlighted the societal paradigm of Singapore as follows: "In the context of Singapore, we see online shaming as a generally kind shape of civic peer checking, which is however to form a significant stamp on society. The overwhelming technophilic talk is clear in our interviews with the law requirement authorities as well as with the "online watchers". New technologies are largely seen as participatory and capable of promoting greater community involvement. In this paradigm, technology-enabled peer surveillance serves to reinforce informal societal institutions (i.e. socio-cultural norms) and hence reduces the need for the "hard power" to be exercised. Still, such norm-enforcing surveillance schemes could potentially spin out of control and lead to a range of abuses, caused by the individuals acting like "civic vigilantes" online." (Skoric, *et al*, 2010, p.197)
   Since 1 January 2020, laws have been implemented in Singapore to criminalize "doxxing". These doxxing regulations are located within the Protection from Harassment Act (POHA). The new legislation creates three distinct categories of doxxing crimes.
   a. Publicizing private information with the goal of upsetting, frightening, or harassing people
   b. Publicizing private information to incite violence
   c. Disclosing private information to encourage the use of violence

Article 3:
(1) No person or organization may intentionally harass, frighten, or upset another individual (referred to as the target person in this section) by any means:
a. employ any derogatory, abusive, or menacing language or actions;
b. communicate in a threatening, abusive, or derogatory manner; or
c. disseminate any information about the target person's identity or that of a linked person, and thus cause harassment, anxiety, or distress to the target person or any other individual (referred to as the victim in this section).
(2) Any person or organization that violates subsection (1) shall commit an offense and, in accordance with section 8, shall be subject upon conviction to a fine of up to $5,000 or imprisonment for a period not exceeding 6 months, or both.
(3) In any case for an offence under subsection (2), it is a defense for the accused individual or entity (referred to in this section as the accused) to demonstrate that the accused's actions were reasonable
Article 5 (1A):
(1A) No person or entity shall, by any means, disclose any identity information of another individual (referred to in this subsection as the victim) or a connected individual of the victim, either -with the intent-
a. to make the victim think that illegal force will be employed against
b. the affected individual or any other individual; or
c. to promote the application of illegal violence against the victim or any other individual; or
d. aware or having justifiable reason to think that it is probable —
e. to make the victim think that illegal force will be employed against the victim or someone else; or
f. to enable the application of illegal aggression towards the victim or any other individual.
(2) Any person or organization that violates subsection (1) or (1A) shall commit an offence and, according to section 8, may be subject upon conviction to a penalty not exceeding $5,000 or imprisonment for a period not exceeding 12 months or both.

3. Hongkong
The anti-doxxing law was implemented in Hong Kong with the enforcement of the Personal Data (Privacy) (Amendment) Ordinance 2021 (PCPO) on 8 October 2021. According to section 64(3A) of the PCPO, an individual commits an offence if they reveal any personal data of a data subject without the necessary consent from the data subject: With the intention of causing any specified harm to the data subject or to any family member of the data subject; or acting recklessly regarding whether any specified harm

would be, or is likely to be, inflicted on the data subject or any family member of the data subject. As per section 64(6) of the PDPO, designated harm concerning an individual signifies: Bullying, assault, annoyance, coercion, or intimidation towards the individual.

a. Physical injury or emotional distress to an individual
b. Harm that causes the individual to justifiably worry about their safety or well-being, or
c. Harm to the individual's property

Of the various rules that apply in these countries, it is worth noting that in the countries mentioned above, the laws governing doxing are formulated specifically and in detail. The formulation of these articles also regulates the consequences that may arise from doxing activities. In Indonesia, the applicable articles in the Personal Data Protection Law are still formulated in a very general way. The article only states a prohibition on the collection, disclosure, and use of personal data. Doxing activities as a follow-up to digital persecution that have an impact on physical or psychological losses or suffering experienced by the victim have not yet obtained a clear regulation. Indonesia needs to complement the laws and regulations with provisions on initiators/perpetrators who first disclose the personal data illegally and regulate the imposition of sanctions if the misuse of personal data has a serious impact on the victim.

CONCLUSION

The problem of digital persecution is more of a social problem, so a non-penal approach is needed to overcome it. The non-penal policy in question is the implementation of user education for internet users which is carried out systematically by the government, through authorized institutions. In addition, an approach from the technology side is needed. Electronic system operators, especially social media, need to implement a comment filtering mechanism, so that comments that have the potential to leak someone's personal data cannot be displayed. On the other hand, the law also cannot ignore this phenomenon. The law needs to give strict sanctions to initiators who carry out the online shaming act. The law needs to formulate which party meets the criteria as the initiator. Regarding doxing actions, Indonesia needs to change the paradigm of criminal act formulation, not only limited to the prohibition on the collection, disclosure and use of personal data illegally, but also needs to formulate burdensome elements if the misuse of personal data causes a serious impact on victims.

REFERENCES

Anderson, B., & Wood, M. A. (2021). *Doxxing: A scoping review and typology*. Emerald Publishing Limited.

APJII. (2024). *APJII: Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang*. Retrieved from: https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang

Arief, B. A. (1992). *Bunga Rampai Kebijakan Hukum Pidana*. Bandung: Alumni.

Ashworth, A., & Horder, J. (2009). *Principles of criminal law*. Oxford: Oxford University Press.

Bottlapally, T., & Zhou, L. (2025). Beyond Privacy: Understanding and Mitigating Doxing in the Digital Environment. In *Proceedings of the 58th Hawaii International Conference on System Sciences*.

Cancig-Rosenberg, H., & Peleg, A. (2024). Online shaming and the power of informal justice. *Harv. JL & Gender*, *47*, 1.

Cheung, A. (2021). Doxing and the challenge to legal regulation: When personal data become a weapon. In *The Emerald international handbook of technology-facilitated violence and abuse* (pp. 577-594). Emerald Publishing Limited.

Cheung, A. S. (2014). Revisiting privacy and dignity: Online shaming in the global e-village. *Laws*, *3*(2), 301-326.

detikInet. (2022). *Pencuri Coklat Vs Pegawai Alfamart, Toko Ponsel Dibom Review di Google*. Retrieved from: https://inet.detik.com/cyberlife/d-6235331/pencuri-coklat-vs-pegawai-alfamart-toko-ponsel-dibom-review-di-google

Douglas, D. M. (2016). Doxing: A conceptual analysis. *Ethics and information technology*, *18*(3), 199-210.

Favarel-Garrigues, G., Tanner, S., & Trottier, D. (2020). Introducing digital vigilantism. *Global Crime*, *21*(3-4), 189-195.

Forestal, J. (2024). Social media, social control, and the politics of public shaming. *American Political Science Review*, *118*(4), 1704-1718.

Frensh, W., & Zulyadi, R. (2023). Kebijakan Non-Penal Dalam Upaya Penanggulangan Perundungan di Ruang Siber. *Journal Justiciabelen (JJ)*, *3*(02), 70-79.

Friedman, L. M. (1975). *The legal system: A social science perspective*. Russell Sage Foundation.

Gupita, R. (2024). Tackling the Problem of Personal Data Oversharing on Social Networking Sites (SNS) and its Misuse in Indonesia. *The Public Sphere: Journal of Public Policy*, *12*(1).

Hadjon, P. M. (1987). *Perlindungan Hukum Bagi Rakyat Indonesia*. Makassar: Bina Ilmu.

Hamiltion, T. B. (2017). *Combatting Internet Shaming, Combatting Shaming and Toxic Communities*. New York: The Rosen Publishing Group.

Howes, R. M. (2024). Exploring Digital Vigilantism: Facebook Users' Perspectives on Online Naming and Shaming. *International Journal of Law and Criminology*, *04*(02), 6-11. https://doi.org/10.37547/ijlc/Volume04Issue02-02

Huffman, E. M. (2016). *Call-out culture: How online shaming affects social media participation in young adults*. Gonzaga University.

Koivukari, K., & Korpisaari, P. (2021, November). Online Shaming-A New Challenge for Criminal Justice. In *Perspectives on Platform Regulation* (pp. 473-488). Nomos Verlagsgesellschaft mbH & Co. KG.

Kukul, B. (2023). Personal data and personal safety: re-examining the limits of public data in the context of doxing. *International Data Privacy Law*, *13*(3), 182-193.

Laidlaw, E. B. (2017). Online Shaming and the Right to Privacy. *Laws, 6*(1), 3. https://doi.org/10.3390/laws6010003

Lidyana, V. (2024). *Pertamina Copot Jabatan Arie Febriant yang Viral Meludah*. Retrieved from: https://www.idntimes.com/business/economy/pertamina-copot-jabatan-arie-febriant-yang-viral-meludah-00-3m8tp-q8n8y3

Mahmood, A., Hashim, H. N. M., Zain, F. M., Suhaimi, N. S., & Yahya, N. A. (2018). A survey on the culture of online shaming: A Malaysian experience. *International Journal of Academic Research in Business and Social Sciences*, *8*(10), 1125-1134.

Marshall, H. (1962). *Gutenberg galaxy. The making of typographic man*. University of Toronto press.

McLuhan, M. (2001). *The Medium is the Massage: An Inventory of Effects*. California: Gingko Press.

Muir, S. R., Roberts, L. D., & Sheridan, L. P. (2021). The portrayal of online shaming in contemporary online news media: A media framing analysis. *Computers in human behavior reports*, *3*, 100051.

Muir, S. R., Roberts, L. D., Sheridan, L., & Coleman, A. R. (2023). Examining the role of moral, emotional, behavioural, and personality factors in predicting online shaming. *PLoS One*, *18*(3), e0279750.

Norlock, K. J. (2017). *Online shaming*. Social Philosophy Today.

Noval, S. M. R. (2021). Doxing phenomenon in Indonesia: Amid waiting for privacy settings. *Budapest International Research and Critics Institute-Journal (BIRCI-Journal)*, *4*(3), 3636-3644.

Novianty, S. M., Wijayanti, S., & Muamar, J. (2023). Ethical Discourse of Doxing in Indonesian Twitter Users. *Jurnal InterAct*, *12*(1), 1-13.

Packiarajah, T. S. (2017). *Online shaming: Exploring factors behind online shaming perpetration as well as its prevalence in adults* (Thesis, Tilburg Law School).

Puspita, R. (2022). *Cara Debt Collector Pinjol Mengintimidasi: Ancam Hingga Tuduh Debitur Open BO*. Retrieved from: https://news.republika.co.id/berita/rli0sr428/cara-debt-collector-pinjol-mengintimidasi-ancam-hingga-tuduh-debitur-open-bo

Rizky, M., Hamdani, F. M., & Anggraeni, H. Y. (2025). Comparative analysis of doxing regulations and privacy protection in Indonesia and global perspectives. *Research Horizon*, *5*(4), 1555-1564.

Scheff, S., Schorr, M., & Lewinksy, N. (2017). *Shame Nation: Choosing Kindness and Compassion in an Age of Cruelty and Trolling*. Sourcebooks.

Shenton, J. E. (2020). Divided we tweet: The social media poetics of public online shaming. *Cultural Dynamics*, *32*(3), 170-195.

Shin, J. (2008, March). Morality and Internet Behavior: A study of the Internet Troll and its relation with morality on the Internet. In *Society for information technology & teacher education international conference* (pp. 2834-2840). Association for the Advancement of Computing in Education (AACE).

Skoric, M. M., Wong, K. H., Chua, J. P. E., Yeo, P. J., & Liew, M. A. (2010). Online shaming in the Asian context: Community empowerment or civic vigilantism?. *Surveillance & Society*, *8*(2), 181-199. https://doi.org/10.24908/ss.v8i2.3485

SWNS. (2025). *Flyer who went viral after refusing to give seat to crying child sues airline, passenger who filmed her.* Retrieved from: https://nypost.com/2025/03/11/lifestyle/i-refused-to-swap-plane-seats-with-a-crying-toddler-and-was-publicly-shamed-on-video-so-im-suing-the-airline/

Thun, L. J., Teh, P. L., & Cheng, C. B. (2022). Cyber Aid: Are your children safe from cyberbullying?. *Journal of King Saud University-Computer and Information Sciences*, *34*(7), 4099-4108.

Trottier, D., Gabdulhakov, R., & Huang, Q. (2020). *Introducing vigilant audiences*. Open Book Publishers.

Utami, S. S. K. (2025). Doxing As a Digital Crime: A Human Rights and Privacy Protection Perspective Under Indonesian Law. *Domus Legalis Cogitatio*, *2*(2), 147-164.

Uweng, I. S., Wadjo, H. Z., & Saimima, J. M. (2023). Perlindungan Hukum Pidana Terhadap Doxing Menurut Undang-Undang Informasi dan Transaksi Elektronik. *Pattimura Study Review*, *1*, 168-79.

Vasalou, A., Joinson, A., & Pitt, J. (2006). The role of shame, guilt and embarrassment in online social dilemmas. In *Proceedings of the 20th BCS HCI Group Conference: Engage, HCI 2006* (pp. 108-112).

Zvereva, V. (2020). Trolling as a digital literary practice in the Russian language Internet. *Russian Literature*, *118*, 107-140.