www.bircu-journal.com/index.php/birci
Budapest International Research and Critics Institute-Journal (BIRCI-Journal)
Humanities and Social Sciences
ISSN 2615-3076 Online)
ISSN 2615-1715 (Print)
Budapest Institute

Doxing Phenomenon in Indonesia: Amid Waiting for Privacy Settings

Sayid Muhammad Rifqi Noval
Faculty of Law, Universitas Islam Nusantara, Indonesia
smrn.uninus@gmail.com

Abstract

The activity of privacy data dissemination in cyber world today often happens to people who allegedly made mistakes and went viral. Internet users often provide the detailed information through the easy access of various information today, as if it does not violate the law and even expected helping the process of identifying the perpetrator. In Fact, this action is close to what we call as doxing, the privacy violation. The research method of this paper is normative juridical with statute approach, case approach, analytical approach, and comparative approach. The data source of this research is secondary data. The specification of this study is analytical descriptive. The results of this study identified several regulations that could be applied on doxing perpetrators, especially the provisions set out in Law No. 19 of 2016, although the provisions do not specifically address doxing. Several concepts to be considered regarding doxing cases are to file a tort claim regarding privacy information, ie, the tort of public disclosure of private facts, or legal recovery for victims by carrying the concept of the tort of intentional infliction of emotional distress (IIED) claim that applies in some states of the United States.

Keywords
doxing; personal data; privacy

I. Introduction

The internet and social media are seen as having the potential to expand public sphere, territory or domain where discourse takes place involving citizens openly. However, the existence of the Internet public sphere tends to be seen as a contestation space where corporate and state forces try with various ways to control and dominate it. Nevertheless, the wave of digital activism has become a creative means for citizens to develop global and local discourses. They use social media as an alternative to creating autonomous public sphere, and consolidate counter power against other forces (state / corporation). (Bo'do, S. et al. 2019)

Various studies have been reported, regarding the dependence of humans to always be connected to the internet today. One of the reports released in 2020, shows the average time spent by 4.53 billion internet users in the world for each day is 6 hours 43 minutes. The data actually does not only show an increase in the number of internet users, but is an initial diagnosis of the strong potential threats that can arise due to information traffic that occurs while someone is using the internet, especially related to cyber crime. This is in line with the prediction made by IBM chairman Ginni Rometty that for the next five years, cybercrime is the biggest threat to everyone. This statement is certainly based on the fact that currently at least 30,000 websites are hacked every day, then cyber attacks occur every 39 seconds, and 95% of crimes related to data are caused by "human error".

Actually there is no single definition of cyber crime, but the term is often described as a violation or crime that occurs through electronic communication or information systems. This type of crime is basically an illegal activity involving computers and networks. The breadth of the notion of cyber crime is increasingly being felt, with the emergence of a variety of cyber crimes that are currently developing and increasing along with advances in the field of technology. Such as the four highest types of cyber crimes related to financial losses today, namely, corporate account takeover, theft of identity, data theft and ransomeware. Other reports identify similar types of cybercrimes that are common today, namely, (1) attacking computer systems (including Distributed Denial of Service (DDOS), ransomware, and other destructive attacks); (2) data theft (including hacking aimed at stealing personal information and theft of Intellectual Property Rights); (3) fraud/carding schemes; (4) crimes that threaten privacy (including sexortion, revengeporn, cyber stalking , swatting and doxing); and (5) crimes that threaten vital infrastructure.

The high quality and quantity of cyber crime that is happening today is one of the triggers for countries in the world to seek regulations that are not only intended to enforce the law, but also prioritize protecting their citizens so they can avoid becoming victims of cyber crimes. Indonesia itself actually does not have special provisions governing cyber crimes, such as those of Tanzania, Australia, Jamaica, Nigeria. and other countries. The various provisions currently in force in Indonesia are scattered in the Criminal Code, the Information Law and Electronic Transactions, as well as other regulations. Of course, this situation has an impact on the ability of law enforcement to be able to quickly apply the regulations that apply to every cyber crime that occurs in Indonesia.

This situation demands that legislators, law enforcement officers and law scholars in Indonesia strive to be able to fill the legal vacuum that occurs, especially when faced with the phenomenon of various internet users in Indonesia. As an example, it can be seen from Microsoft's report entitled Digital Civility Index (DCI) 2020 which places Indonesia as the country with the highest level of online courtesy at 29th out of 32 countries as well as being the lowest in Southeast Asia (The report was followed by respondents from 32 countries). DCI sets four online politeness benchmarks known as cyber risk, namely: first, unwanted contact; second, online bullying, harassment and violence; third, requests for intercourse and sexual contact without consent; and fourth, attack on reputation.

The report indirectly shows an unhealthy internet ecosystem in Indonesia. Despite the controversy over the results of the DCI survey, it seems that some internet users in Indonesia, knowingly or unknowingly have carried out several activities that are included in the cyber risk referred to by DCI - one of which is the activity of finding and publishing someone's personal information in cyberspace. It is said to be aware, because generally these activities are carried out on individuals who have made mistakes and are viral in cyberspace, so it is considered a moral obligation for the owner of information to help identify targets, and is said to be unconscious because, some people do not know if their activities are related to cyber crime This often happens when there is news of a problem that is viral in cyberspace, so that some internet users search for information related to the figure who is currently in the public's attention. One of them was in the case of abuse experienced by Audrey, a junior high school student in Pontianak in 2019. Several people who were suspected of being perpetrators of abuse were targeted by Indonesian internet users. The names of the suspects, social media, schools and personal photos were spread on the Internet. Several people who were suspected of being perpetrators of the persecution became targets for searching Indonesian internet users. The names of the suspects, social media, schools and personal photos were spread on the Internet. Several people who were suspected of being perpetrators of the persecution

became targets for searching Indonesian internet users. The names of the suspects, social media, schools and personal photos were spread on the Internet.

Not only that, several similar incidents have occurred, as in the case of "Email Erdogan". In July 2016, WikiLeaks released 300,000 emails called “Erdogan Emails”, allegedly to damage the reputation of Turkish President Recep Tayyip Erdogan. Blogger Michael Best later uploaded information on Turkish citizens from the email, including addresses and phone numbers on female voter lists in 79 of Turkey's 81 provinces. Another case is the bombing of the Marathon that occurred in 2013 in Boston. A man named Sunil Tripathi was accused of being the perpetrator of the bombing, so that information about Sunil and his family was then spread on cyberspace. While it was later discovered that the perpetrators were Dzokhar Tsarnev and Tamerlan Tsarnev.

This activity, currently known as doxing, is caused by the ease with which internet users find, collect and disseminate personal information. It can be used to mobilize anger for various purposes and does not rule out a situation described by Daniel Trotttier as Digital Vigilantism. , because internet users have first become someone's fault breaker through the internet user version of the virtual court.

Based on the explanation above, this paper is in the form of photographing the phenomenon of internet users in Indonesia with potential legal consequences, especially the activity of disseminating information in cyberspace by specifically using optical protection of personal data through examples of doxing.

II. Research Methods

The research method used in this paper is normative juridical with a statute approach, case approach, analytical approach, and comparative approach. The source of data used in this research is secondary data. The specification of this research is descriptive analytical.

III. Results and Discussion

3.1. Spreading Personal Data: Doxing Threat

Doxing(or Doxxing) is thought to have emerged in 1990 among Hackers. The term doxing comes from the phrase “dropping documents” or “dropping dox” on someone. This term originated when hackers would beat their competitors on the basis of revenge. In those instances, doxing focuses on identifying the hacker and his faults and handing over those details to the appropriate authorities to get him arrested . In the Oxford dictionary, doxing is defined as seeking and publishing personal or identifying information about a particular individual on the internet and generally with malicious intent. But in reality not all doxing is motivated by malicious intent, several incidents involving journalists are aimed at revealing the identity of someone who previously did not want to be known or anonymous (Pseudonymous). The term often used for unidentified doxers is 'ghost doxer'.

Currently doxing is often defined as the intentional dissemination of data to the public in cyberspace about someone's personal information, which is often intended to humiliate, threaten, intimidate or punish an identified person. David Douglas distinguishes doxing from blackmail, defamation and gossip. According to him, doxing is not done with the aim of receiving something in return, but the motive is often done out of boredom, jealousy, intimidation, protest action or exposing a wrong act.

Some doxers see their actions as a response to the failure of traditional law enforcement agencies to adapt to the needs and realities of the rapidly changing digital world. Doxing that causes victims to feel embarrassed is considered a cost-effective, adaptable, democratic

technique in combating socially undesirable behavior and can create an ethical society. However, it should be very carefully considered, if the impact of doxing can lead to the image of "lynch justice" which is inconsistent with the principle of legal justice, given the potential for abuse which is not limited in terms of duration. A study conducted by the Pew Research Center on 4,248 Americans entitled Online Harrasment 2017 revealed that 73% had been victims of doxing.

There are various tactics in doxing activities, including revenge porn and swatting. Revenge Porn is the unauthorized publication of intimate images of others. These images are generally published with negative comments about the person and often include the victim's social media links and other personal information. Swatting is a form of harassment in cyberspace, when someone will make a false report to the authorities and direct that a fully armed tactical unit be sent to the victim's house. Several states in America have criminalized Swatting, although Federal law does not explicitly address Swatting. One of the obstacles in following up on Swatting's actions is because calls to the authorities are made anonymously,

Swattingconsidered dangerous because it can cause the death of its victims, as was done by Tyler Barriss and happened to Andrew Finch. In December 2017, Barris called 911 and gave a false report that a hostage-taking was taking place, having previously clashed with his co-star in a “call of duty” game. Barris then gave the address he thought belonged to his co-star. Based on the report, the Wichita police then surrounded the given home address. When Finch leaves the house to meet the crowd of police, Finch suddenly drops his hand which causes the police to respond by dropping shots which results in Finch's death. For his actions, Barris was sentenced to 20 years in prison.

Another category of doxing described by Douglas dadalah: (1) deanonymizing, doxing is done by revealing the identity of someone who previously or from the beginning anonymized themselves; (2) targeting, doxing which is done by revealing specific information about a person that allows them to be contacted or found; (3) delegitimizing, doxing which is done by disclosing sensitive or intimate information about someone. Dissemination of such data can damage its credibility or reputation because it is so private that it is not widely known by others.

One other phenomenon that often occurs after the doxing activity occurs is the cancel culture action that is carried out on the targeted subject. Cancel Culture is defined broadly as an attempt to ostracize someone for violating social norms. Cancel Culture is narrowly understood as the practice of withdrawing support (or canceling) against public figures or companies after they have done or said something that is considered inappropriate and offensive. This practice goes hand in hand with consumer boycott tactics that attract support for brands and companies deemed unethical, a common form of political activism. The cancellation strategy usually uses social media to humiliate individuals with the intent of imposing penalties of varying degrees of punishment, ranging from restricting access to public platforms, damaging reputations, and ending careers to inciting prosecution.

Culture cancel culture allegedly inspired by the 1991 film New Jack City, when Wesley Snipes' character Nino Brown said, “Cancel that [Woman]. I'll buy another one”. Meanwhile, the boycott was inspired by Irish culture in the 1880s, which used boycotts as a social and political tool successfully used by African Americans during civil rights movements, such as the Montgomery bus boycott sparked by Rosa Parks. Cancel Culture also gave birth to understanding in politics with the question that was born, namely "if you don't have the ability to stop something through political means, all you can do is refuse to participate". Undoing is a way of acknowledging that one doesn't necessarily have the power to change structural equality.

Despite increasing awareness of the damaging consequences of doxing, existing legal provisions do not adequately address the underlying behavior or its consequences. However, some signs of progress are starting to emerge. A bill proposed in the U.S. House of Representatives — the Online Safety Modernization Act of 2017 (Online Safety Act) — would regulate federal criminal and civil liability for doxing. The bill is a step forward, but does not address the lack of legal recourse for victims if the person posting the information cannot be identified.

The State of Utah proposed a draft Anti-Doxxing Act in 2016, which included a provision that prohibits mentioning someone's name online with the intent to offend'. Doxing is considered one of the crimes of online stalking (cyberstalking). The US Attorney's Office (USAO) released a report in 2016 which stated that "cyberstalking" includes any action taken by a perpetrator on the internet that puts the victim in fear placing the victim in reasonable fear of death or serious bodily injury, or its causes, attempts to to cause, or could reasonably be expected to cause great emotional distress to the victim or the victim's immediate family. The federal law often used to deal with doxing is 18 usc ss 2261A (Title 18, Meanwhile, Lisa Bei recommended three federal laws that can be used in the event of doxing, namely The Communications Decency Act (CDA), The Computer Fraud and Abuse Act (CFAA) and The Stored Communications Act (SCA). CDA offers a safe and respectful online environment, especially for children, while the CFAA is specifically for private organizations, and the SCA is intended for criminals who destroy data stored and controlled by internet service providers.

Some of the doxing cases that have received public attention and international coverage, are the incidents experienced by Brianna Wu in October 2014. A Twitter account called "Death to Brianna" began writing tweets containing threats of rape to attempted murder of Brianna. The photo used on the account is a photo of Brianna with her husband. The account graphically describes the details of the planned rape, murder of Brina and her child, mutilation, and torture of her husband. Subsequent tweets even clearly provided Brianna's home address, causing the family to leave the house in the middle of the night.

Another case, known as the “Dog Poop Girl” incident occurred in 2015 in South Korea. The incident took place in a subway carriage, when a dog belonging to a young woman was pooping inside the train. One of the passengers took a photo of the woman, after the previous refusal to clean the dirt that was requested by another passenger on the train. The photo was then spread in cyberspace, until finally the woman was identified and her personal data was widely spread. As a result of the bullying experienced, the woman finally decided to resign from her college.

3.2. Doxing in Indonesia and Expectations of its Regulation

The protection of personal data and the right to privacy are closely related. Since at least 1988, the Human Rights Committee has seen data protection laws as an important part of safeguarding the right to privacy as recognized in Article 17 of the international Covenant on Civil and Political Rights (ICCPR). Alan Westin defines the right to privacy as the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others. The concept of privacy was further formulated by William Posser by describing four forms of disturbance to a person, namely: (1) interference with one's actions in isolation or isolation, or interference with personal relationships; (2) public disclosure of embarrassing personal facts; (3) publicity that places a person wrongly in public; (4) unauthorized control over one's likeness for the benefit of another.

Doxing is certainly closely related to the protection of the right to privacy, considering that the information published is personal data. Personal data can be broadly defined as any form of information related to the data subject, whether in the sphere of personal,

professional, or public life. The information can be in the form of names, photos, e-mail addresses, bank details, posts on social networking sites, medical information, to Internet Protocol (IP) addresses. Article 28G of the 1945 Constitution of the Republic of Indonesia has actually explicitly mandated the protection of privacy in Indonesia. Although until now the provisions that specifically regulate the protection of the right to privacy are still being awaited, one of which is the Personal Data Protection Bill.

In general, the processing of personal data is only allowed and legal if it is based on a legal ground for a number of reasons, namely: (1) there is consent from the data subject; (2) execution of a contract (performance of contract) in which the data subject is a party or to take steps at the request of the data subject before entering into a contract; (3) for legal compliance and obligations (legal obligations); (4) to protect the vital interests of the data subject or other people; (5) for the implementation of public interest tasks or in the exercise of the official authority of data controller; (6) for the purpose of legitimate interests carried out by the controller or third parties, unless such interests are overridden by the interests, rights or freedoms of the data subject.

One of the doxing incidents in Indonesia was experienced by Kartika Prabirini in 2018. This Kumparan.com journalist received a series of threats on his social media accounts due to the news he did with the title "Tame Rizieq". Threats were made by the supporters of the mass organization, because Kartika was considered negligent in putting the word "habib" before the name of their lord in the news. Not only did Kartika's gender identity and appearance become the subject of harassment on Instagram, but her personal identity was also exposed.

Another doxing incident that occurred in Indonesia was the case of the death of 3 Saint Bernard dogs in 2011 in Jakarta. Previously, it is necessary to convey in advance that it is necessary to separate the discussion between the event that resulted in the death of 3 dogs and the doxing incidentwhich was received by Johanes Indrajaya (one of the defendants) as the owner of a pet shop. Based on court decision No.420/PdtG/2011/PN.JKU.PST, the defendants were declared to have committed unlawful acts that resulted in the death of 3 dogs and were sentenced to pay material compensation of Rp.90,000,000. Doxing eventsWhat happened to Johanes Indrajaya took place in one of the online discussion forums. The reaction given by forum members to the case of the death of the 3 dogs led to Johanes Indrajaya's upload of information in the form of personal photos, photos of his wife and children, home addresses (at that time the legal process was in progress in court).

There are no specific regulations governing doxing in Indonesia, but in certain circumstances doxing can be charged with several legal provisions that have been in force. The provisions of Article 26 Paragraphs (1) and (2) of Law no. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Information and Electronic Transactions (UU ITE) stipulates that the use of information concerning a person's personal data must be carried out with the consent of the person concerned and a lawsuit for those who violate these rights. As for the sanctions as regulated in Article 45 of the ITE Law, if the personal information distributed contains insults and/or defamation, it can be punished with imprisonment for a maximum of 4 (four) years and/or a fine of a maximum of Rp.750. million.

Other sanctions in Article 45A of the ITE Law stipulates that if personal information that is disseminated causes hatred or hostility to certain individuals and/or community groups based on ethnicity, religion, race and intergroup (SARA) can be punished with imprisonment for a maximum of 6 (six) years and / or a maximum fine of 1 billion Rupiah. Meanwhile, if the personal information that is distributed contains threats of violence or intimidation aimed at personally, it can be sentenced to a maximum imprisonment of 4 (four) years and/or a maximum fine of Rp. 750,000,000 as stipulated in Article 45B of the ITE Law.

One example of a doxing case that has been legally processed in Indonesia is the doxing case against Deny Siregar in July 2020. This case is interesting, because the perpetrators are not only charged with the ITE Law, but are threatened with Article 362 of the Criminal Code and Article 95 of Law Number 24 Years 2013 concerning Population Administration. This case began with the actions of the perpetrators who "broke data" and provided screenshots of Denny Siregar's personal information such as name, address, NIK, KK, IMEI, OS to type of device to the Twitter account @opposite6890, and then republished it on social media along with the narrative. The perpetrator, who is a former outsourced Telkomsel employee, has been arrested, and the Police are currently trying to arrest the owner of the @opposite6890 account.

Doxingcertainly cannot be relied upon as an effort to demand proportional justice, because: (1) The punishment is too determined by uncertain social meanings; (2) There is no definite measure used in punishing; (3) Low or questionable accuracy of who and what the punishment is. So, doxing should certainly be avoided given the close proximity of these activities to unlawful acts. Although currently, several parties have tried to legitimize the act of doxing as the right activity to be carried out on the basis of considerations including: (1) Rationalization, by rationalizing the action through the presence of reasons based on the principles of right or wrong, or conformity to norms; (2) Redefiniton, by redefining to be morally acceptable. This is often done by structuring the controversial action taken to fit a morally acceptable framework of action; (3) Construction of negative-other, by linking negative images to other groups, thus positioning themselves as the right group; and (4) Victimizing 'US'.

One of the legal practices that can be considered in doxing cases is to file a tort lawsuit related to personal information, namely The tort of public disclosure of private facts, or legal remedies for victims by using the concept of the tort of intentional infliction of emotional distress (IIED) lawsuit that applies to several states of the United States. Based on the concept of the first tort, a person is responsible for publishing personal information with the effect of being "highly offensive" and "not including information of public concern" . Although there are several things that need to be considered, one of them is when the information concerns a public figure and the public has an interest in knowing it. The tort of intentional infliction of emotional distress (IIED) is an instrument of legal recovery for doxing victims because it allows the plaintiff to impose responsibility for extreme and “outrageous” behavior that causes heavy emotional losses for the victim. Although, Victoria McIntyre considered it difficult to be able to prove this lawsuit, at least the judge could consider five factors to identify it, namely: (1) The history of the relationship of the parties; (2) Sayings accompanying published information; (3) Place of published information; (4) The amount of information published.

IV. Conclusion

Although the protection of the right to privacy has been mandated in the 1945 Constitution of the Republic of Indonesia, until now there is no specific regulation that regulates the act of doxing in Indonesia. Several provisions that can ensnare doxing perpetrators are scattered in various laws and regulations. However, the provisions contained in the ITE Law are a good initial foundation for taking action against doxing perpetrators. In order to complement the doxing arrangements, Indonesia can adapt the legal practices that apply in several states of the United States to: file a tort lawsuit related to personal information, namely the tort of public disclosure of private facts, or legal remedies for victims by using the concept of the tort of intentional infliction of emotional distress (IIED) lawsuit. Regarding the obstacles faced by judges in identifying doxing cases.

References

Achmad, W. RW (2021). Conflict Resolution of Remote Indigenous Communities (Overview of The Sociology Communication). LEGAL BRIEF, 10(2), 280-286.

Al-Suwaidi, Noura, Nobanee, Haitham and Jabeen, Fauzia. "Estimating Causes of Cyber crime : Evidence from Panel Data FGLS Estimator". International Journal of Cyber Criminology, Vol 12, Issue 2 (2018) : 392-407. https://doi.org/10.5281/zenodo.3365895

Banimal, Abu Hasan., et.al. (2020). "Peningkatan Serangan Doxing dan Tantangam Perlindungannya di Indonesia," Southeast Asia Freedom of Expression Network, 22 Desember.

Bo'do,S. et al. (2019). Social Media, Public Sphere and Movement Discussion of Urban Farming in Indonesia. Budapest International Research and Critics Institute-Journal (BIRCI-Journal). P. 250-261.

Bossler, Adam M, and Berenblum, Tamar. (2019). "Introduction : New Direction in Cybersrime Research". Journal of Crime and Justice, Vol.42, No.5: 495-499. https://doi.org/10.1080/0735648X.2019.1692426

Corbride, Aste. "Responding to Doxing in Australia : Towards a Right to Informational Self-Determination ?". UniSA Student Law Review, Vol.3 (2018) : 1-28.

David, Douglas M. (2016) "Doxing : A Conceptual Analysis". Ethics and Information Technology,Volume 18: 199-210. https://doi.org/10.1007/s10676-016-9406-0

Decker, Eileen. "Full Count ? : Crime Rate Swings, Cybercrime Misses and Why We Don't Really Know the Score". Journal Of National Security Law & Policy, Vol. 10, Number 3 (2020) : 583-604.

Djafar, Wahyudi and Santoso, M Jodi. (2019). "Perlindungan Data Pribadi : Mengenali hak-hak subjek data, serta kewajiban pengendali dan prosesor data". Lembaga Studi dan Advokasi Masyarakat (ELSAM).

Djafar, Wahyudi. (2014). "Memerhatikan perlindungan hak atas privasi dalam pengaturan dan praktik penyadapan di Indonesia".Seminar Kewenangan Badan Pemerintah dalam melakukan penyadapan serta korelasinya dengan pelanggaran HAM. Komunitas Peradilan Semu Atma Jaya Moot Court Guild (AMG) Fakultas Hukum Universitas Katolik Indonesia Atma Jaya, 21 Maret.

Hawkes. Rebecca. (2017). "Local Nazis in your area : Public Shaming and communal disgust in the doxing of white nationalists at Charlottesville". Journal of Undergraduate Research in the Creative Arts and Industries, Unitec Institute of Technology, Volume 1, No 1: 58-69.

Homchick, Natalia. (2019). "Reaching Throught the "Ghost Doxer :" An Argument for Imposing Secondary Liability on Online Intermediaries". Washington and Lee Law Review, Vol.76, Issue 3, Article 7: 1307-1344.

Kuskridho Ambardi (et.al). (2019). Jurnalisme, "Berita Palsu", & Disinformasi Konteks Indonesia. Departemen Ilmu Komunikasi Universitas Gadjah Mada, Yogyakarta.

Li, Lisa Bei. (2108) "Data Privacy in the Cyber Age : Recommendations for Regulating Doxing and Swatting". Federal Communicagions Law Journal, Vol.70, Issue 3: 317-328. http://dx.doi.org/10.2139/ssrn.3012266

MacAllister, Julia M. (2017). "The Doxing Dilemma : Seeking a Remedy for the Malicious Publication of Personal Information". Fordham Law Review, Volume 85, Issue 5, Article 44: 2451-2483.

McIntyre, Victoria. (2016). ""Do(x) You Really Want to Hurt Me ?" Adapting IIED as A Solution to Doxing by Reshaping Intent". Tulane Journal of Technology & Intellectual Property, Vol.19: 111-134.

Microsoft. (2020). "Digital Civility Index 2020 : Civility, Safety & Interaction online". 5th Edition, February 2021. Lee, Carmen. "Doxxing as Discursive Action in a Social Movement". Critical Discourse Studies, Vol. 17, Number 3: 1-19. https://doi.org/10.1080/17405904.2020.1852093

Noval, Sayid Mohammad Rifqi. (2020). "Menimbang Kembali Hak Untuk Dilupakan : Penerapan dan Potensi Ancaman". Jurnal Legislasi,Vol.17 No.3: 366-379.

Norris, Pippa. (2020). "Closed Minds ? Is a 'Cancel Culture' Stifling Acedemic Freedom and Intelectuall Debate in Political Science ?". Faculty Research Paper. Series. Harvard Kennedy School John F. Kennedy School Of Government, August.

Ritchey, Andrew J, and Ruback, R. Barry. (2018). "Predicting Lynching Atrocity : The Situational Norms of Lynchings in Georgia". Personality and Social Psychology Bulletin, Vol. 44, No. 5: 619-637. https://doi.org/10.1177/0146167217733075

Sarmah, Animesh, Sarmah, Roshmi, and Jyoti Baruah, Amlan. (2017). "A Brief Study on Cyber Crime and Cyber Laws of India". International Research Journal of Engineering and Technology (IRJET), Vol.4, Issue 6: 1633-1640.

Trottier, Daniel. (2020). "Denunciation and doxing : Toward a Conceptual model of digital vigilantism". Global Crime, Vol.21, NOS. 3-4: 196-212. https://doi.org/10.1080/17440572.2019.1591952

Weaver, Michael. (2019). "Judge-Lynch in the Court of Public Opinion : Publicity and the De-Legitimation of Lynching". American Political Science Review, Cambridge University Press, Volume 113, Issue 2: 293-310. https://doi.org/10.1017/S0003055418000886

Yar, Majid and Drew, Jacqualine. (2019). "Image-Based Abuse, Non-Consensual Pornography Revenge Porn : A Study of Criminalization and Crime Prevention in Australia and England & Wales". International Journal of Cyber Criminology, Vol. 13, Issue 2: 578-594. https://doi.org/10.5281/zenodo.3709306