RECHTSVINDING
Vol. 4, 1 (January-June, 2026), pp. 391-396
EISSN: 2987-4424, DOI: https://doi.org/10.59525/rechtsvinding.1575

The Phenomenon of Cancel Culture and Doxing on Social Media X (Twitter): A Criminological Study of Digital Violence

Allifa Mutia Akbar[1], Emilia Amarda[1], Muh Arfandi[1], St. Alifyani Zahra[1], ST. Nur Hajariani[1]

[1] Universitas Negeri Makassar, Indonesia

ARTICLE INFO

Keywords:

cancel culture;
doxing;
digital violence;
ite law;
personal data protection

Article history:

Received 2026-03-09
Revised 2026-04-10
Accepted 2026-05-15

ABSTRACT

One of the types of digital violence that is increasing in the information technology era is the phenomenon of cancel culture and doxing on social media such as X (Twitter). This practice not only affects the victim's reputation but also causes psychological stress, social harm, and a threat to one's privacy and security. The high use of social media in Indonesia is not balanced with sufficient legal protection against the spread of personal data and digital intimidation, so it is important to investigate this topic. How the culture of cancel and doxing in X is considered as a form of digital violence is the purpose of this study. In addition, this study looks at how effective the law, especially the Electronic Information and Transaction Act (UU ITE) and the Personal Data Protection Act (UU PDP), in punishing people who commit street violations. This research uses a qualitative approach for normative jurispris. Laws and regulations, legal doctrines, and relevant literature are studied. Legal theory, literature, and laws and regulations are studied. The research results show that cancel culture and doxing have a pattern to put pressure on victims through the formation of public opinion, collective social punishment, and the dissemination of personal data. In addition, although the ITE Law and the PDP Law provide a basis for protecting privacy and personal data, doxing has not been regulated as a criminal offense. Therefore, this research is the basis for the development of better legal policies and digital protection to create a social media space that is safe, fair, and respects people's privacy rights.

Corresponding Author:
Allifa Mutia Akbar
Universitas Negeri Makassar, Indonesia; allfamtiaa20@gmail.com

1. INTRODUCTION

In the digital age, cancel culture and doxing on social media platforms like Twitter have become significant issues. Cancel culture involves the mass boycott of public or private figures due to mistakes or controversial views, while doxing involves the disclosure of personal data such as addresses, phone numbers, or employment history to incite further attacks. While cancel culture involves the mass boycott of public or private figures due to mistakes or controversial views, doxing involves the disclosure of

personal data such as addresses, phone numbers, or employment history to incite further attacks. On social media platforms, both techniques thrive thanks to the retweet and hashtag features, which accelerate communication, often without verification.

From a criminological perspective, this phenomenon can be viewed through the open windows theory or cultural criminology, where organized crimes such as cyberstalking and harassment can develop from minor violations in the digital space. While victims experience serious psychological impacts such as depression and social isolation, research shows that doxing perpetrators are often motivated by a sense of vigilante justice. These cases often violate Article 27 paragraph (3) of the ITE Law concerning insults and defamation in Indonesia, although law enforcement remains weak due to the difficulty of identifying anonymous perpetrators. (Tanaka, 2025)

The resulting digital violence is hybrid, involving both structural and emotional components. In this case, platform algorithms help strengthen echo chambers that polarize opinion. Etiological factors such as the lack of regulation of content moderation and online anonymity are a concern of criminological research, allowing doxing, as a continuation of cancel culture, to become a real threat to victims' physical safety. Examples in Indonesia, such as the harassment of environmental activists on X, show patterns comparable to events worldwide where victims lose their jobs or are threatened. To address the legal and social consequences of this phenomenon, reforms are needed. One such approach is strengthening the Personal Data Protection Law (PDP) to sanction doxing and platform accountability through better warning and termination mechanisms. Criminology can use a restorative justice approach to mediate perpetrators and stop the cycle of revenge on social media. (Ayunda, 2024) However, as stipulated in Article 28E of the 1945 Constitution, the balance between privacy protection and freedom of expression is a key issue.

Overall, this criminological research on digital violence is needed to build an evidence-based prevention framework that collaborates with platforms, civil society, and the government. Further research should examine empirical data from police reports and victim surveys to gauge the prevalence and effectiveness of legal responses. Thus, a deeper understanding of the dynamics of cancel culture and doxing on X can contribute to digital policy. Therefore, understanding cancel culture and doxing on X can help make digital policy in Indonesia safer and more inclusive.

2. METHODS

This study employed a qualitative approach with a normative juridical research method. This method was used to provide a reference and allow other researchers to reproduce it. The author employed a normative juridical research method because this research is normative in nature, specifically studying positive legal norms, rights that underlie applicable legal principles and doctrines. This allows for the identification of regulatory gaps regarding the phenomenon of digital violence, including cancel culture and doxing on social media (Twitter).

3. FINDINGS AND DISCUSSION

The phenomenon of cancel culture and doxing on social media (Twitter) is a form of digital violence that operates through social pressure, shaping public opinion, and the dissemination of personal data without due legal process. From a criminological perspective, this practice resembles digital vigilantism, as society seemingly imposes its own punishment on the victim, ultimately resulting in serious impacts such as psychological trauma, loss of sense of security, reputational damage, and socio-economic losses. On the other hand, although Indonesia already has basic protections under the Electronic Information and Transactions (ITE) Law and the Personal Data Protection Law, these regulations do not explicitly classify doxing as a separate criminal offense, thus, its enforcement still faces numerous obstacles, particularly in proving and identifying anonymous perpetrators. Therefore, strengthened regulations, increased cyber law enforcement capacity, and

greater responsibility from digital platforms are needed to ensure that social media spaces are safer, fairer, and respectful of users' privacy rights.

3.1. Criminological Patterns of Cancel Culture and Doxing on X (Twitter) as a Form of Digital Violence

The cancel culture accompanied by doxing on platform X (formerly Twitter) can be seen as a form of digital violence with a specific criminological pattern, namely the collective process of "punishing" someone online through the dissemination of personal data, intimidation, and social exclusion without formal legal procedures. Substantively, this phenomenon is not just about criticism or boycotts, but exhibits characteristics of violent acts based on digital mobs, calls for moratoriums, and other violent actions. This phenomenon is not just criticism or boycotts; it exhibits characteristics of violent acts based on digital mobs, calls for moratoriums, and internet-based violence. It is more than just criticism or boycotts; it exhibits characteristics of violent acts based on digital mobs, collective emotional moral impulses, and dimensions of cybercrime, which make it worthy of inclusion in content. The combination of cancel culture and doxing on X can be understood as a type of non-physical, social media-based violence that targets the psychological integrity, reputation, and privacy of victims, in line with the concept of digital violence. This violence does not use physical force; instead, it utilizes stigma, social threats, and public opinion, causing trauma, fear, and socio-economic loss.

a. The stage of controversy formation and public opinion consolidation

The process often begins with a statement or action (such as a tweet, video, or podcast) that is deemed offensive or inappropriate. Thanks to algorithms and features that enable the spread of collective anger, such as retweets, quote tweets, and threads, content on X quickly goes viral. At this point, targets are often given direct moral labels, such as "sexual harasser," "racist," or "misogynist," thus becoming synonymous with the "crime" they are perceived to have committed (Sophia, 2024).

b. Collectivization of social punishment (digital mob)

This pattern demonstrates the hallmarks of digital vigilantism, with people taking the law into their own hands through social media, ignoring the presumption of innocence and formal legal processes. Once a controversy arises, netizens rally to withdraw support, stop sponsorships, and demand that institutions such as companies, universities, and organizations take action against suspicious actions. This pattern demonstrates the characteristics of digital vigilantism: people use social media to "take the law into their own hands," ignoring the presumption of innocence and formal legal processes (Asyifa, 2024).

c. Using doxing as a tool of pressure and intimidation

Groups typically begin collecting and disseminating personal data about targets after public opinion has been generated. Rather than simply "exposing," the actual goal is to increase psychological distress, humiliate, or force victims to leave their jobs, projects, or public positions. This data may come from past digital recordings, other social media accounts, or even online tracking, from a criminological perspective. The goal goes beyond simply "exposing"; it is to pressure, humiliate, or force victims to leave projects, jobs, or other public roles. Criminologically, there are many reasons for this, such as resentment, a desire to "punish," and the enforcement of social norms recognized by the perpetrator (Selsa, 2023).

d. Psychosocial and Economic Effects of Violence

Victims of cancel culture accompanied by doxing often experience very severe effects:

1) Experiencing psychological distress such as anxiety, fear, trauma, and even depression as a result of being "seen" and publicly criticized (Sriyana, 2025).

2) Socio-economic effects, such as job termination, loss of contracts, boycotts, or the termination of career projects, even though there has been no legal decision.

From a criminological perspective, this suggests that digital violence can cause the same harm as conventional crimes, even without direct contact.

e. Patterns of Perpetrators and Victims

1) Perpetrators are usually unidentified mass networks operating in X; they act for various reasons, such as respect, revenge, political reasons, or a desire to strengthen their group identity.
2) Victims can be ordinary people, activists, or public figures. However, numerous studies show that women, activists, and minorities are more vulnerable to cancel culture and doxing. This is due to imbalanced social norms and power structures. (Faisal, 2024)

f. Legal Dimensions and Cybercrime

From a criminal law perspective, the concept of cancel culture is not yet clearly regulated, but several elements can be linked to cybercrime. One form of privacy violation and defamation is the dissemination of embarrassing or threatening personal data. In Indonesia, this can be verified through the ITE Law (now Law No. 1/2024 concerning the Second Amendment to Law No. 11/2008) and the Personal Data Protection Law of 2022. These laws create a foundation to prevent the unauthorized dissemination of personal data and enhance protection of individual privacy and reputation (Riska, 2025).

3.2. The Effectiveness of the Electronic Information and Transactions Law (ITE Law) and the Personal Data Protection Law in Ensnaring Doxing Perpetrators on X (Twitter) with Enforcement Loopholes

Daily life benefits greatly from today's rapid advances in technology and information. One such advantage is the ability to access information anytime and anywhere. However, we must not ignore the fact that technological advancements can have detrimental effects, such as the rise of cybercrime. Cybercrime is a criminal act that uses computers as a tool to commit acts such as theft, hacking, fraud, spreading viruses, and others. There are many types of cybercrime, but phishing, hacking, cyberstalking, and cyberbullying are the four most common (Suhaemin, 2023). New types of cybercrime emerge with technological advancements. Doxing is currently a popular type of cybercrime. The number of online harassment cases continues to increase annually; data from Safanet shows a twofold increase from the previous year. Therefore, we must be more vigilant against cybercrime because it can have a detrimental impact on our lives. 56% of people targeted by doxing are journalists or reporters, 22% are activists, and 22% are civilians. It's often seen that the public is unaware of doxing cases on various social media platforms, such as Twitter. People from various backgrounds gather on Twitter to discuss various issues. (Marini, 2023) However, when people disagree, they often attack each other, one example being by hitting the other person.

Depending on the applicable law, the penalties imposed on individuals who commit doxing can vary. Sanctions can include fines, imprisonment, or both. Victims of doxing can also file a civil lawsuit for compensation.

In Indonesia, doxing is regulated by several laws related to privacy, personal data theft, and computer crime. Here are some relevant regulations:

a) Article 26 Paragraph (1) of Law No. 19 of 2016 concerning Electronic Information and Transactions (ITE Law)
b) Article 27 Paragraph (4) of Law No. 19 of 2016 concerning Electronic Information and Transactions (ITE Law)
c) Article 45 Paragraph (1) of Law No. Law No. 19 of 2016 concerning Electronic Information and Transactions (ITE Law)
d) Law No. 27 of 2022 concerning Personal Data Protection (PDP Law)

Article 26 Paragraph (1) of the ITE Law states that the use of a person's personal information through electronic media must be with the consent of the person concerned. This article aims to protect individuals' privacy rights from unauthorized use of information.

Article 27 Paragraph (4) of the ITE Law regulates insults and defamation through electronic media. This article states that perpetrators who intentionally distribute information containing insults and/or defamation can be punished with a maximum of four years' imprisonment and/or a maximum fine of IDR 750,000,000.

Legally, Indonesia has laws that protect personal data and privacy rights, as stated in Article 28G paragraph (1) of the 1945 Constitution, which states that everyone has the right to protection of themselves, their families, their honor, dignity, and their property. (Uweng, 2023) Everyone also has the right to feel safe and protected from fear, including threats that force them to make decisions. Article 26 paragraph (1) of Law Number 19 of 2016, concerning amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), also states this protection. According to the law, people must provide consent for the use of personal data in electronic media; however, the law does not explicitly mention doxing as a separate crime. This makes the law unclear when prosecuting doxing perpetrators, and victims lack adequate legal protection. As a result, Indonesian law remains unclear regarding complex digital crimes such as doxing. The law becomes less effective as a tool to control and maintain justice in the digital world if current regulations cannot firmly regulate the practice of doxing. Consequently, new criminal laws must be urgently created to address IT-based crimes. Our legal system also lacks a clear distinction between intentional doxing and negligent doxing. As a result, both perpetrators of intentional doxing and those who do so negligently face the same criminal penalties. This is undoubtedly unfair because it fails to consider the actual wrongdoing and the appropriate sanctions. Furthermore, victims of sexual violence lack adequate protection from the Indonesian criminal justice system, both legally and psychologically. As a result, victims of sexual violence lack the rights to the protection and justice they need. Doxing can actually cause serious mental suffering, such as anxiety, loss of a sense of security, and lasting trauma.

4. CONCLUSION

The phenomenon of cancel culture and doxing on social media platform X (Twitter) demonstrates the development of digital violence through social pressure, public opinion, and the significant dissemination of personal data. From a criminological perspective, these actions are akin to digital vigilantism—the act of society "punishing" individuals without going through formal legal processes. Controversy is initiated, public opinion is generated, and then doxing is used as a means of intimidation and social pressure. Victims not only lose their dignity but also experience trauma, psychological stress, a sense of security, and socio-economic losses. Therefore, cancel culture accompanied by doxing can be categorized as digital violence, with characteristics comparable to other cybercrimes.

Conversely, Indonesian laws remain ineffective in punishing those who commit doxing. Neither the Electronic Information and Transactions (ITE) Law nor the Personal Data Protection Law explicitly state that doxing is a criminal offense. This raises law enforcement issues, particularly in terms of establishing evidence, identifying anonymous perpetrators, and protecting victims. Furthermore, current laws are inadequate to address the complexities of digital violence on social media, as they focus solely on the violation and dissemination of personal data. Consequently, legal changes that better align with technological advances are needed to protect victims and improve the systems that protect them. This also requires increasing the responsibility of digital platforms to create a safe, fair, and free-of-expression digital environment.

REFERENCES

Asyifa, H. (2024). Cancel Culture pelaku pelecehan seksual di media sosial. *Jurnal Kajian Sosiologi*.

Ayunda, M. (2024). Perspektif Perilaku Doxing Sebagai Bentuk Cancel Culture pada Pengguna Media Sosial X. *Jurnal Ilmu Hukum, Humaniora dan Politik (JIHHP)*.

Faisal, S. (2024). FENOMENA PERILAKU CANCEL CULTURE DI MEDIA SOSIAL DALAM PERSPEKTIF FIQIH SIYASAH. *At-Thullab Jurnal*.

Marini, S. (2023). Wacana Etis Doxing Pada Pengguna Twitter Indonesia. *Jurnal InterAct*.

Riska, R. (2025). RELEVASI HUKUM PIDANA DALAM MENGAKOMODASI CANCEL CULTURE SEBAGAI TINDAK PIDANA DI MEDIA SOSIAL. *Andrew Law Journal*.

Selsa, A. (2023). PERSPEKTIF ETIKA KOMUNIKASI DALAM PRAKTEK DOXING DAN CANCEL CULTURE DI MEDIA SOSIAL TWITTER SEBAGAI SANKSI SOSIAL. *Universitas Gadjah Mada*.

Sophia, H. (2024). FENOMENA CANCEL CULTURE DI TWITTER/X: STUDI KASUS PLAGIARISME. *Institut Seni Budaya Indonesia* .

Sriyana. (2025). Fenomena Cancel Culture dan Dampaknya Terhadap Kebebasan Berekspresi. *Jurnal Pengabdian Masyarakat dan Riset Pendidikan*.

Suhaemin, A. (2023). Karakteristik Cybercrime Di Indonesia. *Edulaw: Journal Of Islamic Law And Yurisprudance*.

Tanaka, V. (2025). Kriminalitas Di Era Digital: Kajian Kriminologi Terhadap Kejahatan Online. *Jurnal Pendidikan, Sosial, dan Humaniora*.

Uweng, I. (2023). Perlindungan Hukum Pidana Terhadap Doxing Menurut Undang-Undang Informasi dan Transaksi Elektronik. *Pattimura Law Study*.