Journal of International Islamic Law, Human Rights and Public Policy
(JISHUP Journal) | ISSN(e): 3031-2280
Website https://jishup.org/index.php/ojs/index | Volumes 4 No. 2 (2026)

THE INFLUENCE OF DOXING ON THE DEVELOPMENT OF CYBERCRIME THROUGH WHATSAPP IN A CRIMINALISTIC PERSPECTIVE

Muhammad Ikhsan Khairi [1] Chairuni Nasution[2]
Universitas Pembangunan Pancabudi, Medan[1,2]
ikhsankhairi33@gmail.com , chairuninst@gmail.com

Received: 02/03/2026 | **Revised:** 11/03/2026 | **Accepted:** 01/04/2026 | **Published:**25/05/2026

Abstract

The development of information and communication technology has brought significant changes to people's interaction patterns, especially through the use of social media and instant messaging applications such as WhatsApp. On the other hand, these advances are also various forms of cybercrime, one of which is doxing. Doxing is the act of collecting, disclosing and disseminating a person's personal data without legal consent, which has the potential to cause serious harm to the victim. From a criminalistic perspective, doxing is not only understood as a violation of the law, but also as a criminal event that leaves a digital footprint that can be analyzed scientifically for the sake of legal proof. This study aims to examine the juridical regulation of cybercrime in Indonesian criminal law and analyze the influence of doxing in the development of cybercrime through WhatsApp. The research method used is normative juridical research with a literature approach. The results of the study show that although doxing has not been explicitly regulated as a separate offense, the act can be charged through the provisions of the Electronic Information and Transaction Law and the Personal Data Protection Law. Therefore, it is necessary to strengthen regulations and increase criminalistic understanding to deal with the increasingly complex phenomenon of doxing

Keywords: ***doxing, cybercrime, WhatsApp, criminalistic***

INTRODUCTION

The development of information and communication technology has brought significant transformations in various aspects of human life, including in social interaction and economic activities. However, these advances have also opened up new opportunities for various forms of cybercrime that are increasingly sophisticated and organized. WhatsApp as the most popular instant messaging platform in Indonesia with more than 100 million active users, has become one of the main mediums in people's daily communication. In the midst of easy access to digital communication, the phenomenon of doxing has emerged that is increasingly worrying. Doxing, which comes from the word "documents" or "dropping documents", is the act of distributing someone's personal information unlawfully without the victim's consent, such as full name, phone number, home address, workplace, and other sensitive data. This phenomenon is often motivated by personal grudges, political conflicts, or unhealthy commercial goals. According to Kominfo data, in 2024 there will be a significant increase in cases of personal data breaches and cybercrime in Indonesia, with WhatsApp being one of the most frequently abused platforms for the dissemination of personal information. Doxing not only violates an individual's privacy, but is also a major trigger for various other cybercrimes such as threats (cyberstalking), identity fraud, account hacking, and physical threats to victims. From a criminalistic perspective, doxing shows a systematic pattern of crime with a digital footprint that can be traced through digital forensics. Analysis of WhatsApp metadata, conversation logs, and information dissemination patterns are key in identifying perpetrators and mapping cybercrime networks. However, the main challenge faced by law enforcement officials is technical limitations in digital evidence collection and cross-agency coordination. Indonesian legal regulations have accommodated the handling of doxing through Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Information and Electronic Transactions (UU ITE) and Law No. 27 of 2022 concerning Personal Data Protection. However, law implementation still faces obstacles in terms of response speed and effectiveness of enforcement, especially against cybercrime that is cross-jurisdictional. The increase in doxing cases on WhatsApp not only causes material losses to victims, but also serious

psychological impacts such as trauma, depression, and insecurity. This phenomenon shows the need for a multidisciplinary approach that integrates digital criminalism, analysis of perpetrator behavior, and strengthening legal regulations to prevent and overcome the development of doxing-based cybercrime. Therefore, this study aims to analyze the influence of doxing in the development of cybercrime through the WhatsApp platform from a criminalistic perspective, as well as identify effective handling strategies based on the analysis of digital evidence and crime patterns.

B. PROBLEM FORMULATION

The formulation of the problem in this study is prepared to provide clear directions and limits to the discussion carried out. The formulation of this problem is important so that the research remains focused on relevant legal issues and does not deviate from the purpose of the research. The formulation of the problem in this study is as follows:

1. What is the juridical arrangement of cybercrime in criminal law in Indonesia?
2. How does doxing affect the development of cybercrime through WhatsApp?

C. RESEARCH OBJECTIVES

The purpose of research is a goal to be achieved through scientific research activities. This goal is the basis for the preparation of methods, analysis, and discussion of research results. The objectives of this study are:

1. To find out and analyze the juridical regulation of cybercrime in criminal law in Indonesia, especially related to the use of electronic systems and personal data protection.
2. To find out and analyze the influence of doxing on the development of cybercrime through WhatsApp and its implications in a criminalistic perspective.

D. BENEFITS OF RESEARCH

1. Theoretical Benefits

Theoretically, this research is expected to contribute to the development of legal science, especially criminal law and cyber law. This research is also expected to enrich the scientific treasure regarding criminal and criminalistic theories related to cybercrime, especially the practice of doxing that utilizes social media and instant messaging applications. Thus, this research can be an academic reference for students, lecturers, and researchers who are interested in studying similar issues.

2. Practical Benefits

Practically, this research is expected to provide a more comprehensive understanding and information about the problem of cybercrime in Indonesia, especially doxing through WhatsApp. The results of this study are expected to help law enforcement officials in understanding the characteristics and modus operandi of doxing as a cybercrime, so that the law enforcement process can be carried out effectively in accordance with the applicable criminal procedure law. In addition, this research is also expected to be a consideration for the government in formulating policies and regulations that provide legal certainty to the problem of doxing on social media.

E. LITERATURE REVIEW

1. Definition of Cybercrime

According to Barda Nawawi Arief, cybercrime or cyber crime is an unlawful act committed by using computers, computer networks, or electronic systems as the main means, targets, or tools to commit criminal acts. Cybercrime has special characteristics, namely being cross-border, difficult to detect directly, and taking advantage of advances in information technology. Therefore, cybercrime requires a different legal and law enforcement approach than conventional crime.

Sources:

Barda Nawawi Arief, Mayantara Crime, RajaGrafindo Persada, Jakarta, 2014.

2. Definition of Doxing

Doxing is not explicitly mentioned in Law Number 11 of 2008 concerning Information and Electronic Transactions and its amendments. However, in substance, the act of doxing can be qualified as an unlawful act because it is closely related to the misuse and dissemination of personal data without rights. Article 26 paragraph (1) of the ITE Law expressly states that the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned. This provision indicates that the protection of personal

data is part of the right to privacy guaranteed by positive law in Indonesia.[1] Furthermore, the regulation regarding doxing has gained a stronger legal basis with the enactment of Law Number 27 of 2022 concerning Personal Data Protection. This law confirms that everyone is prohibited from discloseing, disseminating or using personal data without a valid legal basis or without the consent of the data subject. In Article 1 number 1 of the Personal Data Protection Law, it is explained that personal data is any data about an individual that is identified or can be identified separately or in combination with other information.[2] Thus, the act of doxing that disseminates identity, address, telephone number, or other personal information is clearly contrary to these provisions.

Doctrinally, doxing can be understood as the act of collecting, disclosing and disseminating personal data or information of a person through digital media for a specific purpose, either for intimidation, social pressure, or other interests. Edmon Makarim explained that the misuse of personal data in cyberspace is a form of violation of human rights in the digital era, especially the right to privacy.[3] Therefore, although the term doxing is not explicitly mentioned in laws and regulations, the essence of its act has been accommodated in the legal norms governing the protection of personal data and electronic information. Based on this description, doxing can be understood as an unlawful act that violates a person's privacy rights in the digital space, and has the potential to cause both material and immaterial losses to the victim. Thus, doxing is part of cybercrime that can be subject to criminal and civil liability in accordance with the provisions of applicable laws and regulations in Indonesia.

Reference Sources

Law of the Republic of Indonesia Number 11 of 2008 concerning Information and Electronic Transactions jo. Law Number 19 of 2016.

Law of the Republic of Indonesia Number 27 of 2022 concerning Personal Data Protection. Cyber (C

Edmon Makarim, Law and Law), RajaGrafindo Persada, Jakarta, 2019

Barda Nawawi Arief, Mayantara Crime, RajaGrafindo Persada, Jakarta, 2014.

3. Definition of Media

According to Soerjono Soekanto, the media is a means or tool used to convey messages, information, and communication from one party to another in community life. In the context of law and information technology, the media functions as an intermediary that allows social interaction to occur, including in the form of electronic communication that has the potential to be misused to commit crimes.

Sources:

Soerjono Soekanto, Sociology of an Introduction, RajaGrafindo Persada, Jakarta, 2015.

4. Definition of WhatsApp

WhatsApp is an internet-based instant messaging application that allows users to send text messages, voices, images, and other data quickly and in real-time. According to Edmon Makarim, applications such as WhatsApp are included in the category of electronic systems as referred to in the ITE Law, so all activities carried out in it can have legal implications if used for unlawful acts.

Sources:

Edmon Makarim, Introduction to Telematics Law, RajaGrafindo Persada, Jakarta, 2016.

5. Definition of Criminalistic

Criminalistics is a branch of criminal law that studies scientific techniques and methods in uncovering a criminal act through the analysis of evidence and traces of crime. According to Topo Santoso, criminalism plays an important role in the evidentiary process because it helps law enforcement to uncover legal facts objectively and scientifically.

Sources:

Topo Santoso, Criminalistics, RajaGrafindo Persada, Jakarta, 2017.

METHOD

1. Types of Research

The type of research used in this study is descriptive research, which is research that aims to describe systematically, factually, and accurately the phenomenon of cybercrime and doxing through WhatsApp. Descriptive research was chosen because this research does not aim to test hypotheses, but rather to explain and analyze existing legal problems.

Sources:

Sugiyono, Quantitative, Qualitative, and R&D Research Methods, Alfabeta, Bandung, 2019.

2. Research Type

The type of research used is normative juridical research, which is research that examines law as a norm or rule that applies in society. This research focuses on the analysis of laws and regulations, legal principles, and legal doctrines related to cybercrime and doxing.
Sources:
Peter Mahmud Marzuki, Legal Research, Kencana, Jakarta, 2016.
3. Research Methods
The research method used is the library research method, which is a research method that is carried out by examining various written sources such as books, scientific journals, laws and regulations, and internet sources that are relevant to the research topic.
Sources:
Soerjono Soekanto and Sri Mamudji, Normative Law Research, Rajawali Press, Jakarta, 2018.
4. Secondary Data
The type of data used in this study is secondary data, namely data obtained indirectly from the object of research, but through literature studies on various legal materials and literature that are relevant to the problem being studied. The secondary data is used to analyze the juridical arrangements and the influence of doxing on the development of cybercrime through WhatsApp from a criminalistic perspective.
The secondary data in this study consisted of: Primary Legal Materials, which are legal materials that are binding and have legal force, consisting of:
the Constitution of the Republic of Indonesia in 1945;
Law of the Republic of Indonesia Number 11 of 2008 concerning Information and Electronic Transactions and its amendments;
Other laws and regulations related to personal data protection and cybercrime.
Secondary Legal Materials, which are legal materials that provide explanations and interpretations of primary legal materials, which include legal textbooks, accredited scientific journals, scientific works, research results, opinions of legal experts, and legal materials obtained from internet sources that are relevant to discussions about cybercrime, doxing, WhatsApp, and criminalistics.
Tertiary Legal Materials, which are legal materials that function as a support and complement to provide an understanding of legal terms, which include legal dictionaries, legal encyclopedias, and Indonesian dictionaries related to legal terminology and information technology.
5. Qualitative Data Analysis
Qualitative data analysis is a systematic process to understand, interpret, and draw the meaning of non-numerical data obtained through literature studies, legal documents, court decisions, scientific journals, and credible internet sources. In this study, qualitative data analysis was used to examine in depth the phenomenon of doxing as part of cybercrime that develops through the WhatsApp application, both from legal, social, and technological perspectives. According to Sugiyono (2019), qualitative data analysis is carried out interactively and continues until the data is considered saturated. The data that has been collected is not processed in the form of statistical numbers, but is analyzed through logical and interpretive reasoning to find patterns, relationships, and meanings that are relevant to the focus of the research. This approach is very appropriate to be used in normative and socio-legal legal research that focuses on legal norms, concepts, and practices in society.

The stages of qualitative data analysis in this study refer to the Miles and Huberman model which consists of three main stages, namely data reduction, data presentation, and conclusion drawn. a. Data Reduction Data reduction is the initial stage of analysis that is carried out by selecting, focusing, simplifying, and abstracting data that is relevant to the research problem. In the context of this study, data in the form of laws and regulations (ITE Law and Personal Data Protection Law), cyber law literature, scientific journals, and internet articles discussing doxing and misuse of personal data through WhatsApp were selected and classified based on their relevance. Soerjono Soekanto and Sri Mamudji (2018) explained that data reduction in legal research aims to separate primary, secondary, and tertiary legal materials so that the analysis can be carried out in a structured manner and does not deviate from the formulation of the problem. With data reduction, researchers can avoid irrelevant information and focus on the legal aspects of doxing as a form of cybercrime.
b. Presentation of Data
The next stage is data presentation, which is the process of compiling data that has been reduced to the form of narrative descriptions, conceptual tables, or thematic classifications so that they are easy to understand and analyze. In this study, data is presented in the form of a systematic description of the meaning of doxing, the modus operandi of doxing through WhatsApp, the legal and social impacts it causes, and its legal regulation in Indonesia.

According to Miles, Huberman, and Saldaña (2014), the presentation of data helps researchers to see the complete picture of the phenomenon being studied and makes it easier to find cause-and-effect relationships. With the presentation of the data, analysis of the relationship between the development of WhatsApp communication technology and the increasing practice of doxing can be carried out more comprehensively. c. Conclusion Drawing and Verification The last stage is drawing conclusions and verification, which is the process of formulating the meaning of the data that has been analyzed and testing the consistency and validity of research findings. Conclusions in qualitative research are not final from the beginning, but develop as the researcher's understanding of the data increases.

Sugiyono (2019) states that conclusions in qualitative data analysis must be supported by strong and consistent evidence from various data sources. Therefore, in this study, a comparison was made between legal provisions, expert opinions, and empirical facts reported in journals and online media. This aims to ensure that the conclusion regarding doxing as a cybercrime through WhatsApp has a strong academic and juridical basis. By using qualitative data analysis, this study is expected to be able to provide an in-depth understanding of the characteristics of doxing, the driving factors for doxing on the WhatsApp platform, and the effectiveness of Indonesia's positive laws in tackling cybercrime.

: Sugiyono. (2019). Quantitative, Qualitative, and R&D Research Methods. Bandung: Alfabeta.
Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). Qualitative Data Analysis: A Methods Sourcebook. Sage Publications.
Soekanto, Soerjono & Mamudji, Sri. (2018). Normative Law Research. Jakarta: Rajawali Press.
Abraham, Johnny. (2017). Normative Law Research Theory and Methodology. Malang: Bayumedia.

RESULTS AND DISCUSSION

1. Juridical Regulation of Cybercrime in Criminal Law in Indonesia

The development of information technology has encouraged the birth of various new forms of crime committed through electronic systems, known as cyber crime. In the context of Indonesian criminal law, cybercrime has basically been accommodated through Law Number 11 of 2008 concerning Information and Electronic Transactions as amended by Law Number 19 of 2016. This law regulates various acts that are prohibited in the use of information technology, including illegal access, illegal interception, manipulation of electronic data, and misuse of electronic information that harms others. However, the regulation regarding doxing has not been explicitly regulated as a separate criminal offense. However, juridically, the act of doxing can be qualified as an unlawful act based on the provisions of Article 26 of the ITE Law which regulates the protection of personal data. The article emphasizes that the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned. Therefore, the unauthorized dissemination of personal data may be considered a violation of the privacy rights protected by law.

In addition to the ITE Law, the birth of Law Number 27 of 2022 concerning Personal Data Protection strengthens the legal position of doxing victims. This law provides a more comprehensive legal basis regarding the rights of data subjects, the obligations of data controllers and processors, as well as criminal sanctions for personal data protection violations. In this context, doxing can be categorized as an act that violates the principle of personal data protection because it is carried out without a valid legal basis and without the consent of the data subject. From a criminalistic perspective, the juridical regulation of cybercrime is also related to proving criminal acts.Cybercrime, including doxing, leaves digital footprints that can be scientifically analyzed for the purpose of investigation and proof in court. Therefore, clear and firm legal arrangements are needed so that law enforcement officials have a strong basis in uncovering and taking action against cybercrime perpetrators.

2. The Influence of Doxing in the Development of Cybercrime through WhatsApp

Doxing has a significant influence on the development of cybercrime, particularly through the use of instant messaging applications such as WhatsApp. WhatsApp as one of the most widely used communication media in Indonesia allows the dissemination of information quickly, widely, and difficult to control. The characteristics of instant and massive digital communication make WhatsApp an effective means for doxing perpetrators to disseminate victims' personal data without consent. According to Edmon Makarim, the development of information technology has created a new space for cybercrime to occur that is difficult to control if it is not balanced with adequate legal and regulatory awareness.[1] In practice, personal data obtained through doxing is often disseminated through private messages, WhatsApp groups, and broadcast features, so that the potential loss experienced by victims is even greater. The dissemination can include identity information, phone numbers, addresses, and personal documents that are protected by law. This action is contrary to the principle of personal data protection as stipulated

in Law Number 27 of 2022 concerning Personal Data Protection, which affirms that any processing of personal data must be carried out on the basis of the consent of the data subject.[2] The influence of doxing in the development of cybercrime is not only limited to privacy violations, but also opens up opportunities for other cybercrimes, such as fraud, extortion, threats, and identity theft. Barda Nawawi Arief explained that cybercrime has a multidimensional nature, where one criminal act can be an entrance to another.[3] Personal data that has been disseminated can be used by perpetrators to carry out psychological manipulation of victims and other parties, for example by representing victims in digital communications.

Thus, doxing can be seen as an initial crime (predicate crime) that triggers advanced cybercrime. This view is in line with the opinion of Abdul Wahid and Mohammad Labib who stated that the crime of doxing is often a chain and interrelated between one criminal act and another.[4] In this context, doxing serves as an initial means of obtaining data that is then used in further crimes. From a criminalistic perspective, doxing through WhatsApp is a criminal event that has special characteristics. Criminalistic views crime as an event that must be proven through evidence and scientific methods. According to Topo Santoso, criminalism plays an important role in uncovering modern crimes by utilizing science and technology, including in proving cybercrimes.[5] Digital traces in the form of conversation screenshots, message metadata, IP addresses, and account activity history can be used as valid electronic evidence as recognized in Article 5 of Law Number 11 of 2008 concerning Electronic Information and Transactions.

However, the main challenge in disclosing doxing cases is the anonymous and cross-border nature of cybercrime. Perpetrators can disguise their identities through fake accounts or virtual networks, making it difficult to identify and enforce the law. Therefore, special technical expertise and cooperation between law enforcement officials, electronic service providers, and other related institutions are needed. In addition to the law enforcement aspect, the low digital literacy of the community also contributes to the rampant practice of doxing. Many WhatsApp users do not understand the importance of maintaining the confidentiality of personal data and the legal risks of indiscriminately disseminating information. According to Soerjono Soekanto, the effectiveness of the law is not only determined by written rules, but also by the legal awareness of the community as a subject of law.[6] This shows that efforts to counter doxing do not only depend on a repressive approach through criminalization, but also require a preventive approach through education, digital literacy, and increasing public legal awareness.

Reference Sources

[1] Edmon Makarim, Introduction to Telematics Law, RajaGrafindo Persada, Jakarta, 2016.
[2] Law of the Republic of Indonesia Number 27 of 2022 concerning Personal Data Protection.
[3] Barda Nawawi Arief, Mayantara Crime, RajaGrafindo Persada, Jakarta, 2014.
[4] Abdul Wahid & Mohammad Labib, Cyber Crime, Refika Aditama, Bandung, 2016.
[5] Topo Santoso, Criminalistics, RajaGrafindo Persada, Jakarta, 2017.
[6] Soerjono Soekanto, Factors Influencing Law Enforcement, RajaGrafindo Persada, Jakarta, 2018.

CONCLUSION

Conclusion

Based on the results of the discussion, it can be concluded that the juridical regulation of cybercrime in Indonesian criminal law has basically been accommodated through the Electronic Information and Transaction Law and the Personal Data Protection Law. However, the regulation regarding doxing has not been specifically formulated as a separate criminal offense, so its application still depends on the interpretation of articles related to personal data protection and privacy rights. This condition poses challenges in law enforcement, especially in providing legal certainty for victims of doxing.

REFERENCES

Andi Hamzah, Criminal Law, 2018
Sudarto, Introduction to Law, 2016
Soerjono Soekanto, Legal Research Methods, 2017
Peter Mahmud Marzuki, Legal Research, 2019
Jimly Asshiddiqie, Indonesian Constitution and Constitutionalism, 2015
Yulius Hamka, Information Technology Law, 2020
Artidjo Alkostar, The Struggle for Law Enforcement, 2019
Barda Nawawi Arief, Bunga Potpourri Criminal Law Policy, 2014
M. Yahya Harahap, Indonesian Criminal Procedure Law, 2015 10. E. Utrecht, Criminalistics: An Introduction, 2017

Benny Riyanto, Personal Data Protection Law, 2022
Djoko Agus Purwanto, Cybersecurity and Cybercrime Law, 2023
Raden M. Drajat, Cybercrime and Digital Criminal Law, 2021
Faisal Basri, Digitalization and Legal Development, 2018
Gunawan Widjaja, Cybercrime and Digital Ethics, 2020
Helmi Hamzah, Indonesian Legal System, 2016
Siti Zuhro, Information Technology Law, 2019
Rachel Laksmi, Ethics and Law in IT, 2021
Agus Rahardjo, Introduction to Criminalistics, 2015
Indira Chusnul Mar'iyah, Cyber Crime Study, 2024
Arief Budi Santoso, Information Protection and Personal Data, 2023
Putri Ayu, The Development of Cybercrime in Indonesia, 2024
Leonardo Nababan, Legal Research Methodology, 2017
Rini Wulandari, Digital Forensics in Criminalistics, 2022
Hendra Gunawan, Social Media and Legal Provisions, 2019
Wahyudi Sutopo, Cyber Law and Consumer Protection Studies, 2023
Fadly Hermansyah, Digital Privacy Protection, 2021
Siwi Widayati, Utilization of IT for Law Enforcement, 2018