



Indonesia Media Law Review, Volume 4 Issue 2 (December 2025), pp. 190-211

ISSN 2829-7628 (Print) 2829-7423 (Online)

<https://doi.org/10.15294/imrev.v4i2.35972>.

Indonesia Media Law Review is Journal for Media, Press Law and Ethics in Journalism

Published biannually by the Faculty of Law, Universitas Negeri Semarang, Indonesia and managed by Law Student Press Community and Press and Journalism Law Studies Center, Faculty of Law Universitas Negeri Semarang, INDONESIA

Protecting Journalists in the Digital Age: A Cross-Jurisdictional Legal Comparison of Indonesia and the Netherlands

Chanidia A.R.*

Faculty of Law, Universitas Negeri Semarang, Indonesia

Cahya Wulandari

Faculty of Law, Universitas Negeri Semarang, Indonesia

Mutmainah Nur Qoiri

Faculty of Law, Universitas Negeri Semarang, Indonesia

Winarsih

Faculty of Law, Universitas Negeri Semarang, Indonesia

Nauli Pinorsinta Pasaribu

Faculty of Law, Universitas Negeri Semarang, Indonesia

Jennifer Margareth Uliana Sianipar

Faculty of Law, Universitas Negeri Semarang, Indonesia

**Corresponding author's email: chanidia@mail.unnes.ac.id*

ABSTRACT: This study examines the legal frameworks of Indonesia and the Netherlands in addressing doxing as an emerging threat to press freedom and the protection of journalists' personal data. Although Indonesia has established several legal instruments, including the Press Law No. 40/1999, the amended Electronic Information and Transactions Law No. 1/2024, and the Personal Data Protection Law No. 27/2022. The existing regulations remain implicit, fragmented, and insufficient in providing legal certainty. Interviews conducted with three journalists from diverse professional backgrounds reveal that legal protection remains predominantly passive, with inadequate

law enforcement against actors who perpetrate digital intimidation and attacks on journalists.

In contrast, the Netherlands has adopted a more comprehensive regulatory approach through its constitutional guarantee of freedom of expression, the direct implementation of the General Data Protection Regulation (GDPR), the establishment of an independent data protection authority (*Autoriteit Persoonsgegevens*), and the enactment of a specific anti-doxing law in 2024 that prescribes clear criminal sanctions. Additionally, the *PersVeilig* protocol demonstrates a more institutionalized mechanism for safeguarding journalists against threats in both physical and digital environments. Employing a normative legal approach triangulated with interview evidence, this study finds a critical institutional paradox: while journalist legal protection remains inadequate due to inconsistent law enforcement, the Press Council's mediation mechanisms function effectively as ethical arbiters yet suffer from systematic non-coordination with criminal justice authorities despite possessing *lex specialist* status.

Comparative analysis highlights the pressing need for Indonesia to strengthen legal protections for journalists through a more integrated model. This study recommends the development of explicit anti-doxing regulation, the establishment of an independent data protection authority, and the creation of cross-institutional collaboration protocols to ensure the safety of journalists and uphold press freedom in the digital democratic ecosystem.

KEYWORDS: Press freedom, doxing, personal data protection.

I. INTRODUCTION

The phenomenon of doxing has evolved into one of the main issues in legal regulation, digital communication, and press freedom. Etymologically, doxing derives from the word “docs” or “documents,” which refers to the act of collecting and then publishing an individual’s personal data in the digital sphere without consent. This term initially emerged within hacker communities in the 1990s, before becoming a widespread practice on the internet for purposes of revenge, social pressure, or simply to disseminate the victim’s personal information¹. In line with the increasing use of social media, doxing has now evolved onto social media platforms and has become a serious threat to anyone, including journalists and media workers conducting their professional duties.

¹ Sal Sabila Khoirotunnisa Utami, “Doxing As A Digital Crime: A Human Rights And Privacy Protection Perspective Under Indonesian Law,” *Domus Legalis Cogitatio* 2, no. 2 (October 2025): 147–64, <https://doi.org/10.24002/dlc.v2i2.9912>.

The principal characteristics of doxing are delineated by the unauthorized disclosure of an individual's personal data; the presence of an underlying intent to inflict harm, public humiliation, intimidation, or punitive consequences upon the targeted party; and the execution and amplification of this conduct within digital environments facilitated by internet-based platforms². The information disclosed in doxing incidents may include personal identifiers, residential addresses, contact details, family-related data, personal background, and other sensitive information that can generate psychological, economic, and even physical harm to the victim. Such risks are particularly pronounced for journalists who frequently face death threats and intimidation following doxing attacks. In the context of journalism, doxing is often closely associated with various forms of online harassment, including cyberbullying, cancel culture, and cyberstalking, with the intent to undermine the exercise of press freedom and to coerce journalists into silence from reporting facts that are perceived as detrimental to certain parties³.

Doxing represents a novel form of threat against press freedom, one that did not previously exist in the era of print media. Journalists who engage in critical reporting on sensitive matters, such as corruption, human rights violations, or governmental policymaking, are increasingly becoming the primary targets of doxing attacks conducted by actors who perceive such journalistic activities as a threat to their interests⁴. The Alliance of Independent Journalists (AJI) has indicated that since 2019, digital attacks including doxing have become an increasingly prevalent tactic used to obstruct journalistic work. AJI recorded 14 such cases in 2020 and five cases in 2021, demonstrating a sustained pattern of digital threats targeting media professionals⁵. Incidents such as the doxing of a CNN Indonesia journalist in February 2025 who reported on the *Indonesia Gelap* demonstrations,

² David M. Douglas, "Doxing: A Conceptual Analysis," *Ethics and Information Technology* 18, no. 3 (2016): 199–210, <https://doi.org/10.1007/s10676-016-9406-0>.

³ Jeane Neltje Saly and Tabriz Sulthanah Lubna, "Pelindungan Data Pribadi Dalam Tindakan Doxing Berdasarkan Undang-Undang Nomor 27 Tahun 2022," *Jurnal Kewarganegaraan* 7, no. 2 (2023): 1708–13.

⁴ Satria Adhi N, "Doxing, Bentuk Ancaman Baru Kebebasan Pers," *Universitas Gajah Mada*, May 26, 2021, <https://ugm.ac.id/id/berita/21170-doxing-bentuk-ancaman-baru-kepada-kebebasan-pers/>.

⁵ Adi Marsiela and Luh De Suriyani, "Panduan Keamanan Digital Untuk Jurnalis," *Aliansi Jurnalis Independen*, 2022, <https://aji.or.id/data/panduan-keamanan-digital-untuk-jurnalis>.

further illustrate how digital attacks are strategically deployed to intimidate the press and suppress the dissemination of information that is considered unfavorable to certain stakeholders⁶, Similar digital harassment was also directed at a journalist from Liputan6.com, Cakrayuni Nuralam, in September 2020, following his coverage of politically sensitive issues, further demonstrating how doxing is utilized as a coercive mechanism to pressure journalists and inhibit the fulfillment of their constitutional role in delivering information to the public⁷ and similar incident also affected a journalist from Nusadaily.com in April 2021,⁸ demonstrates that such threat constitutes not merely a theoretical concern, but rather an empirical reality that substantially imperils the physical, psychological, and professional security of journalists.

From human rights perspective, doxing violates various fundamental principles guaranteed within international legal instruments. *Article 12 Universal Declaration of Human Rights* states that:

“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks” which explicitly prohibits arbitrary interference with an individual’s privacy, and Article 19 of the Universal Declaration of Human Rights, which states:

“Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.” which explains the right to freely express information and ideas through any media, regardless of territorial boundaries.

Netherlands has adopted comprehensive anti-doxing regulations that explicitly criminalize the intentional dissemination of personal data with the

⁶ Khumar Mahendra, “Dua Jurnalis CNN Indonesia Kena Doxing Usai Liput Aksi Indonesia Gelap, Apa Sanksi Bagi Pelakunya,” *Tempo*, January 25, 2025, <https://www.tempo.co/hukum/dua-jurnalis-cnn-indonesia-kena-doxing-usai-liput-aksi-indonesia-gelap-apa-sanksi-bagi-pelakunya-1212008>.

⁷ “AJI Jakarta Kecam Doxing Terhadap Jurnalis Liputan6com,” *Aliansi Jurnalis Independen*, December 9, 2020, <https://aji.or.id/berita-aji/aji-jakarta-kecam-doxing-terhadap-jurnalis-liputan6com>.

⁸ “AJI Malang Kecam Doxing Terhadap Dua Jurnalis Nusadaily.Com,” *Aliansi Jurnalis Independen*, September 21, 2021, <https://aji.or.id/berita-aji/aji-malang-kecam-doxing-terhadap-dua-jurnalis-nusadailycom>.

aim of intimidating, obstructing, or impeding the performance of professional duties. On July 11, 2023, the Dutch Senate approved this historic legislation formally criminalizing doxing, with the regulations taking effect on January 1, 2024⁹. In Indonesia, the protection of personal data and press freedom is regulated through several legal instruments, including the Press Law No. 40 of 1999, which guarantees press freedom and protects journalists from intimidation and threats that may hinder journalistic work; the Information and Electronic Transactions Law (ITE Law) No. 1 of 2008, which includes provisions on the illegal dissemination of personal information, defamation, and threats via electronic media; and the Personal Data Protection Law No. 27 of 2022, which safeguards individuals' rights over their personal data and stipulates sanctions for those who misuse such information. Despite the severity and prevalence of journalist doxing in Indonesia, the legal framework provides inadequate and fragmented protection, characterized by four fundamental deficiencies.

Referring to various previous studies, the research to be conducted will be related to earlier investigations. Prior studies include: Syailendra et al., which focused on the phenomenon of doxing in Indonesia, defined as the act of revealing an individual's personal information without consent, particularly in the context of social media. This study analyzed the legal and ethical aspects of doxing, the effectiveness of existing regulations, and its impact on victims. However, the current research team intends to focus more on a comparative legal analysis of doxing between Indonesia and the Netherlands¹⁰.

The next study by Balqis and Monggilo focused on doxing as a threat to online journalists. This research examined the doxing case experienced by Cakrayuni Nuralam, a former journalist at Liputan6.com, after reporting on the PDIP politician Arteria Dahlan. The current research team places

⁹ "Doxing to Become a Criminal Offence Carrying 2-Year Sentence," *Dutch News*, December 7, 2023, <https://www.dutchnews.nl/2023/07/doxing-to-become-a-criminal-offence-carrying-2-year-sentence/>.

¹⁰ Moody Rizqi Syailendra, Et Al., *Studi Kasus Sebuah Ancaman Terhadap Privasi Kasus Doxing Di Indonesia Dalam Perspektif Hukum Dan Etika*, 4, no. 4 (2024): 32–45.

greater emphasis on the legal regulations concerning doxing that pose a threat to press freedom in Indonesia¹¹.

Sari's research concentrated on doxing persecution as a new pattern of victimization against journalists in Indonesia, analyzing how doxing has evolved into a form of digital violence threatening press freedom. This study explored the mechanisms of doxing persecution, its triggering factors, recurring patterns, and its impact on journalists and the media industry¹².

Based on these prior studies, the current research offers novelty by examining the impact of doxing on journalists by adopts a comparative legal approach between Indonesia and the Netherlands, because Netherlands has developed explicit anti-doxing legislation and specialized journalist protection mechanisms that directly address gaps in Indonesian regulation.

II. METHODS

This study is normative legal research employing both statutory and comparative approaches. The statutory approach is conducted through an analysis of various positive legal provisions relevant to the legal issues under examination. Additionally, this research adopts a comparative approach by examining and contrasting the legal systems or statutes of one country with those of one or more other countries on the same matter¹³. The comparative study aims to analyze the differences and similarities in the legal frameworks applied in the Netherlands and Indonesia concerning doxing against journalists. Both Indonesia and the Netherlands operate within civil law systems derived from Continental European legal tradition, sharing fundamental characteristics including codified statutory law as primary legal source, systematic organization of legal rules, and emphasis on legislative positivism. Indonesia's legal system evolved from Dutch colonial law, with the original Criminal Code (*Wetboek van Strafrecht voor Indonesië*) directly

¹¹ Darin Rania Balqis and Zainuddin Muda Z. Monggilo, "Doxing Sebagai Ancaman Baru Jurnalis Online: Menelisik Kasus Doxing Jurnalis Liputan6.Com," *Jurnal Komunikasi* 14, no. 2 (2024): 133–44, <https://doi.org/10.31294/jkom.v14i2.15651>.

¹² Rintan Puspita Sari, "Persekusi Doxing Sebagai Pola Baru Viktimisasi Terhadap Jurnalis Di Indonesia," *Deviance Jurnal Kriminologi* 5, no. 1 (2021): 68, <https://doi.org/10.36080/djk.1139>.

¹³ Peter Mahmud Marzuki, *Penelitian hukum* (Kencana, 2005).

transplanted from the 1886 Dutch Criminal Code, creating path dependencies and conceptual continuities that persist despite post-independence legal reforms. This shared legal DNA means that Dutch statutory approaches, definitional frameworks, and institutional designs can be adapted to Indonesian legal architecture with greater conceptual compatibility than models from common law jurisdictions like the United States or United Kingdom, where fundamentally different approaches to precedent, statutory interpretation, and judicial review create transplantation barriers. By understanding the approach of each jurisdiction, this research can provide insights into the effectiveness of existing regulations and offer recommendations to enhance protection for journalists in Indonesia. Normative legal research, or doctrinal research, is a method that focuses on analyzing primary and secondary legal materials, such as statutes, regulations, and legal doctrines, to understand the concepts and principles of law in force¹⁴.

This approach is often used to examine how written law regulates a specific issue. In the context of doxing, defined as the dissemination of an individual's personal information without consent via the internet. Normative legal research can be applied to analyze how the laws in Indonesia and the Netherlands regulate and respond to this phenomenon.

The primary legal materials used in this study include the Press Law No. 40 of 1999, the Personal Data Protection Law No. 27 of 2022, and the Information and Electronic Transactions Law (ITE Law) No. 1 of 2024, which will be compared with the General Data Protection Regulation (GDPR) and the Dutch Criminal Code. This research is also supported by secondary legal materials, including textbooks, scholarly journals, interviews with journalists, and other materials that provide explanations and context for the primary legal sources used in the study.

¹⁴ Soerjono Soekanto, *Penelitian Hukum Normatif*(2006).

III. RESULT AND DISCUSSION

A. Doxing as a Cyber Threat to Press Freedom in Indonesia

Doxing represents a form of digital attack that has become increasingly prevalent on social media. Douglas categorizes doxing into three types: first, deanonymizing doxing, which involves revealing the real identity of an individual who previously used an alias or remained anonymous on social media accounts; second, targeting doxing, which entails disclosing specific personal information such as home addresses, phone numbers, or social media details that allow others to locate or contact the individual; and third, delegitimizing doxing, which consists of exposing sensitive or private information such as medical records, court documents, or previously unreleased photos and videos with the intent to damage a person's credibility or reputation¹⁵.

Cases of doxing against journalists demonstrate a consistent pattern: journalists engaged in investigative reporting or critical commentary on sensitive issues, such as corruption, human rights violations, or government policy, are the primary targets. The impact of doxing and digital threats on press freedom in Indonesia is profound, posing significant risks to the foundations of democracy. Herlambang P. Wiratraman (2023), in the article *Kebebasan Pers, Hukum, dan Politik Otoritarianisme Digital* published in *Undang: Jurnal Hukum*, emphasizes that the erosion of press freedom in the digital realm occurs alongside the consolidation of authoritarian political power.

First, these attacks undermine journalistic independence. Research indicates that digital harassment fosters widespread self-censorship among journalists and media organizations. This chilling effect directly weakens the press's role as a watchdog and governmental overseer, as individuals must constantly remain vigilant against surveillance and potential legal repercussions¹⁶.

Second, there is a detrimental impact on public access to information. When independent media are silenced, society loses access to accurate, verified, and

¹⁵ Douglas, "op.cit"

¹⁶ Andreas Ufen, "The Rise of Digital Repression in Indonesia under Joko Widodo," *GIGA Focus Asia* 1 (2024), <https://doi.org/10.57671/GFAS-24012>.

balanced information, creating opportunities for disinformation and the manipulation of public narratives to benefit certain actors. Cass Sunstein highlights that without a healthy information ecosystem, citizens are deprived of the ability to distinguish truth from falsehood, thereby threatening the very foundations of democracy¹⁷.

Third, sustained digital attacks on independent and critical media concentrate informational and political power in the hands of pro-government outlets or oligarch-controlled media. This diminishes diversity of perspective and constrains democratic space¹⁸.

Fourth, these attacks negatively affect democratic participation. When journalists and activists are targeted by doxing and intimidation, public engagement in political discourse and oversight of public policy decreases significantly. SAFEnet notes that digital assaults instill pervasive fear, which undermines the essence of a democratic state¹⁹.

B. Legal Framework in Indonesia Governing the Handling of Doxing Cases Targeting Journalists

1. Law No. 40 of 1999 on the Press

Law Number 40 of 1999 on the Press (Press Law) constitutes the primary legal foundation for the protection of journalists in Indonesia. Article 4 of the Press Law affirms that journalistic activities in Indonesia are safeguarded by the principle of press freedom. The state guarantees the right of every member of the press to obtain, manage, and disseminate information without censorship, obstruction, or interference from any party²⁰. This provision also ensures that the public has access to information as part of the fulfillment of their constitutional rights. Article 8 of the Press Law explicitly

¹⁷ Cass R. Sunstein, "Lies and Falsehoods," in *Liars*, 1st ed., by Cass R. Sunstein (Oxford University Press New York, 2021), <https://doi.org/10.1093/oso/9780197545119.003.0001>.

¹⁸ Aris Sarjito, "Hoaks, Disinformasi, Dan Ketahanan Nasional: Ancaman Teknologi Informasi Dalam Masyarakat Digital Indonesia," *Journal of Governance and Local Politics (JGLP)* 6, no. 2 (2024): 175–86, <https://doi.org/10.47650/jglp.v6i2.1547>.

¹⁹ "Statement on Digital Repression During the August 2025 Indonesian Protests," *SAFEnet* (Denpasar), August 31, 2025, <https://safenet.or.id/2025/08/statement-on-digital-repression-during-the-august-2025-indonesian-protests/>.

²⁰ Ridwan Ridwan and Muhammad Anshar, "Analisis Regulasi Jurnalistik Pada Undang-Undang Pers No. 40 Tahun 1999," *LITERA: Jurnal Ilmiah Mutidisiplin* 2, no. 1 (2024): 42–61, <https://litera-academica.com/ojs/litera/article/view/77>.

states that “journalists shall receive legal protection in the performance of their profession.” The explanation of Article 8 further clarifies that legal protection constitutes a guarantee by the government and/or society to journalists in exercising their functions, rights, obligations, and roles in accordance with the prevailing statutory provisions.

Based on interviews conducted with three informants from different journalistic backgrounds, including: an international journalist, a journalist working within a municipal government public relations structure, and a local journalist, it can be concluded that the current Press Law remains largely relevant in supporting the execution of journalistic functions. The informants assessed that the provisions of the Press Law continue to provide the necessary legal basis to safeguard freedom of expression, ensure the protection of journalistic work, and uphold the role of the press as a pillar of democracy amid the evolving dynamics of information and communication technology.

However, with regard to Article 8, which emphasizes that journalists must receive legal protection in performing their professional duties, the informants expressed concern that the provision does not yet provide fully active and comprehensive protection for journalists. They highlighted the persisting weaknesses in legal support, particularly regarding the lack of robust law enforcement against perpetrators of intimidation, violence, or other threats directed at journalists.

The interconnection between Law Number 40 of 1999 on Press (Press Law), Law Number 19 of 2016 on Amendment to ITE Law, Law Number 27 of 2022 on Personal Data Protection (PDP Law), and Law Number 1 of 2023 on Criminal Code creates a complex network of regulations with significant normative conflicts that threaten press freedom in Indonesia. The primary conflict lies in the tension between Article 15 paragraph (2) letter d of the Press Law, which grants the Press Council authority to resolve press disputes through mediation, and Article 27 paragraph (3) of the ITE Law, which directly criminalizes defamation through electronic media without requiring prior review by the Press Council, creating legal uncertainty for digital journalists who lack equivalent protections afforded to conventional

journalists. Research demonstrates that the ITE Law has caused a dramatic increase in the criminalization of journalists, with 233 cases during the first term of President Widodo (2014–2019) compared to 74 cases in the previous period, with 82 of 241 individuals charged for insulting the government or public officials, showing that digital regulation has become a repressive instrument that silences press freedom. Article 27 paragraph (3) of the ITE Law references Article 310 of the Criminal Code for the definition of defamation based on Constitutional Court Decision Number 50/PUU-VI/2008, yet the disparity in sanctions is extreme, with the ITE Law threatening imprisonment of up to 4 years and a fine of Rp750 million, while the New Criminal Code Article 433 imposes only a maximum of 1.5 years imprisonment and a Rp50 million fine for essentially identical conduct, creating injustice particularly for digital journalists. The PDP Law exacerbates this situation by not providing explicit exceptions for journalistic work in Articles 15 paragraph (1) and 50, diverging from GDPR Article 85, which requires European Union member states to provide journalistic exemptions, thereby exposing Indonesian journalists who disclose personal data during investigations into corruption or human rights violations to criminal liability under Article 67 paragraph (2) of the PDP Law with threats of 4 years imprisonment and Rp4 billion fine. The Press Council stated that the PDP Law could become a "new instrument of repression" against journalists, with concrete consequences including government ministries refusing to release public documents under the guise of personal data protection and the emergence of self-censorship among investigative journalists.

2. Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions

Law Number 1 of 2024, as the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (ITE Law), introduces significant changes to Indonesia's legal framework, particularly in addressing digital attacks. While the ITE Law serves various important functions and objectives, its substance still presents several challenges. Numerous critiques indicate that, in certain aspects, the law has yet to provide full legal certainty.

Some normative provisions remain ambiguous or overly flexible (so-called “*pasal karet*”) such as Article 27A:

“Setiap Orang dengan sengaja menyerang kehormatan atau nama baik orang lain dengan cara menuduhkan suatu hal, dengan maksud supaya hal tersebut diketahui umum dalam bentuk Informasi Elektronik dan/ atau Dokumen Elektronik yang dilakukan melalui Sistem Elektronik.” Could potentially restricting freedom of expression, including the delivery of opinions and criticism within the digital democratic space²¹.

Interviews with the three informants revealed that although the ITE Law is intended to hold perpetrators of digital attacks against journalists accountable, in practice it can sometimes be applied against journalists themselves when reporting on sensitive issues involving particular individuals or organizations.

3. Law No. 27 of 2022 on Personal Data Protection

Law Number 27 of 2022 on Personal Data Protection (PDP Law) represents a significant advancement in Indonesia’s legal system for safeguarding the personal data of its citizens, including journalists. Article 1(1) of the PDP Law defines personal data as “data concerning an individual who is identified or can be identified either directly or in combination with other information, whether through electronic or non-electronic systems.” Article 4 of the PDP Law further distinguishes between types of personal data, differentiating specific personal data (such as health, biometric, genetic, criminal records, and children’s data) and general personal data (such as name, gender, and nationality).

Article 16(1) stipulates that all forms of personal data processing must be based on the consent of the data subject, except in circumstances explicitly regulated otherwise by law. This provision underscores the fundamental principle of personal data protection: the collection, utilization, and dissemination of personal data cannot occur without legitimate consent from the data owner. In the context of doxing, the disclosure or distribution of

²¹ Bonnibel Rambatan, *On the State of Digital Authoritarianism in Indonesia and Its Contradictions*, n.d., <https://newnaratif.com/on-the-state-of-digital-authoritarianism-in-indonesia/>.

personal information without clear consent constitutes a violation of these provisions.

Article 65 of the PDP Law regulates the prohibition on the misuse of personal data. Article 65(1) states that “Any person is prohibited from unlawfully obtaining or collecting personal data that does not belong to them, with the intent to benefit themselves or others, in a manner that may cause harm to the data subject.” Furthermore, Article 65(2) provides that “Any person is prohibited from unlawfully disclosing personal data that does not belong to them”. Article 67 of the PDP Law establishes the sanctions for violations of personal data protection principles. Specifically, Article 67(1) stipulates that “Any person who intentionally and unlawfully obtains or collects personal data to benefit themselves or others, in a manner that may cause harm to the data subject as referred to in Article 65(1), may be subject to imprisonment of up to five years and/or a fine of up to IDR 5,000,000,000 (five billion rupiah).” Article 67(2) further asserts that “Any person who intentionally and unlawfully discloses personal data that does not belong to them, as referred to in Article 65(2), may be subject to imprisonment of up to four years and/or a fine of up to IDR 4,000,000,000 (four billion rupiah).”

These provisions demonstrate that doxing, as the unauthorized disclosure of personal data, constitutes a serious violation under the PDP Law, subject to substantial legal sanctions²².

UU PDP provides general prohibitions on unlawful collection (Article 65 paragraph 2) and disclosure (Article 67 paragraph 2) of personal data but lacks explicit definitions and classifications of specific violation types such as doxing, data breaches, unauthorized profiling, or surveillance. Research by Putri (2023) demonstrates that the PDP Law generalizes that the activity of disclosing personal data or doxing is prohibited and can be criminalized without distinguishing between doxing for purely malicious purposes and

²² Muhammad Kamarulzaman Satria and Hadi Yusuf, “Analisis Yuridis Tindakan Kriminal Doxing Ditinjau Berdasarkan Undang Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi,” *Jurnal Intelek Dan Cendekiawan Nusantara* 1, no. 2 (2024): 2442–56, <https://jicnusantara.com/index.php/jicn/article/view/266>.

doxing for legitimate public interest purposes²³. This lack of classification creates several problems: law enforcement cannot prioritize cases based on harm severity, prosecutors struggle to determine appropriate charges, and judges lack guidance on proportional sentencing.

C. Press Freedom and Data Protection in Netherlands

Press freedom in the Netherlands constitutes a foundational element of the country's democratic system, recognized both constitutionally and internationally. Article 7 of the Dutch Constitution (*Grondwet*) guarantees freedom of expression, stipulating that “no prior censorship may be imposed, but responsibility may be incurred afterward in cases determined by law”²⁴. This principle is reinforced by Article 10 of the European Convention on Human Rights (ECHR), which protects freedom of expression as a fundamental right in a democratic society²⁵. In practice, Dutch law upholds the principle that individuals may speak or write freely, provided they do not violate existing legal provisions, such as those addressing defamation, incitement to hatred, or, in a contemporary context, digital harassment and doxing.

As a member of the European Union, the Netherlands has directly implemented the General Data Protection Regulation (GDPR) since May 25, 2018. The GDPR is among the most comprehensive and stringent personal data protection regulations globally, encompassing a broad definition of personal data, principles for lawful data processing, and robust individual rights. Article 4 of the GDPR defines personal data as “any information relating to an identified or identifiable natural person,” with a

²³ Nafila Andriana Putri, “Doxing Untuk Malicious Purposes vs Doxing Untuk Political Purposes: Urgensi Pengklasifikasian Ancaman Hukuman Bagi Para Pelaku Doxing Dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi,” *Padjadjaran Law Review* 11, no. 1 (2023): 105–15, <https://doi.org/10.56895/plr.v11i1.1286>.

²⁴ “Constitution for the Kingdom of the Netherlands, after the Amendment of 2018,” Ministry of the Interior and Kingdom Relations, February 28, 2019, <https://www.rijksoverheid.nl/documenten/rapporten/2019/02/28/grondwet-voor-het-koninkrijk-der-nederlanden-2018>.

²⁵ Remco Klöters, “Netherlands Media Law Guide, Defamation and Privacy Law in the Netherlands,” *Carter-Ruck*, n.d., <https://www.carter-ruck.com/law-guides/defamation-and-privacy-law-in-netherlands/>.

low threshold for “identifiable,” meaning that a person can be identified using “all reasonable means likely to be used”²⁶.

Autoriteit Persoonsgegevens (AP), the Netherlands’ independent data protection authority, possesses full authority to investigate complaints regarding GDPR violations, including cases of doxing. The AP can receive reports from doxing victims and conduct investigations into perpetrators or platforms hosting doxing content. In the context of doxing, the AP also plays an educational role, providing guidance on individuals’ rights to remove or modify personal data that has been shared without consent²⁷.

The Dutch response to the increasing incidence of doxing targeting journalists and other professional groups has resulted in a comprehensive and integrated legal framework. On July 11, 2023, the Dutch Senate officially approved legislation criminalizing doxing, which came into effect on January 1, 2024²⁸. This anti-doxing law emerged as a response to the surge in doxing incidents that threatened the safety of emergency responders, police officers, journalists, politicians, scientists, and other public officials²⁹.

Under the Dutch anti-doxing legislation, “obtaining, disseminating, or making available the personal identity data of another person or third party with the intention of instilling fear in others, causing serious disruption to others, or seriously obstructing someone in the performance of their duties or profession shall be punishable by a maximum of two years’ imprisonment or a fine of up to €22,500”³⁰. The penalty is increased by one-third when doxing targets individuals in specific professions, such as mayors, politicians, judges, lawyers, journalists, and police officers, reflecting the Netherlands’ recognition of the professional vulnerability of these groups³¹.

²⁶ “General Data Protection Regulation (GDPR),” <https://gdpr.eu/article-4-definitions/>, n.d., <https://gdpr.eu/article-4-definitions/>.

²⁷ “Data Protection in the Netherlands,” *DLA Piper*, n.d., <https://www.dlapiperdataprotection.com/?t=authority&c=NL>.

²⁸ “The Netherlands,” *Centre For Media Pluralism and Media Freedom*, n.d., <https://cmpf.eui.eu/country/the-netherlands/>.

²⁹ “Use of Personal Data for the Objective of Harassment to Become Criminal Offence,” *Government of the Netherlands*, December 7, 2023, <https://www.government.nl/latest/news/2023/07/12/use-of-personal-data-for-the-objective-of-harassment-to-become-criminal-offence>.

³⁰ *Dutch News*, “Doxing to Become a Criminal Offence Carrying 2-Year Sentence.”

³¹ “Act of 12 July 2023 Amending the Criminal Code, the BES Criminal Code, the Code of Criminal Procedure and the BES Code of Criminal Procedure in Connection with the Criminalization of

The Netherlands has also developed an innovative journalist protection mechanism known as *PersVeilig* (Press Safety), launched in November 2019 as a protocol jointly established by the Dutch Association of Journalists (*Nederlandse Vereniging van Journalisten/NVJ*), the Dutch Society of Editors-in-Chief (*Nederlands Genootschap van Hoofredacteurs*), the national police, and the public prosecution service. *PersVeilig* aims to strengthen the position of journalists when confronted with violence and harassment in public spaces, on social media, and through legal threats.

The *PersVeilig* protocol encompasses a range of preventive protective measures, including a hotline through which journalists can report physical, verbal, sexual, or other forms of threats and receive guidance on appropriate actions. It also provides security plans for media employers and journalists containing practical details on prevention, training, and clear procedures regarding the steps to be taken following an incident.

The police commit to investigating reported cases with urgency, promptly submitting case files to the Public Prosecutor, maintaining a dedicated case registry, and ensuring that the media and journalists are kept informed throughout the investigation process. In situations where journalists experience harassment in their private lives, the police are required to advise employers and journalists regarding appropriate security measures³².

Obtaining, Distributing or Otherwise Making Available Personal Data for Intimidating Purposes (Criminalization of the Use of Personal Data for Intimidating Purposes)," Ministry of Justice and Security Netherlands, July 28, 2023, <https://zoek.officielebekendmakingen.nl/stb-2023-274.html>.

³² "Netherlands: Towards a Safer Haven: Advancing Safety of Journalists amidst Rising Threats in the Netherlands," *Media Freedom Rapid Response*, February 2022, <https://www.ecpmf.eu/wp-content/uploads/2022/04/Towards-a-safer-haven-Advancing-safety-of-journalists-amidst-rising-threats-in-the-Netherlands.pdf>.

The following presents a comparative legal analysis of doxing regulation in Indonesia and the Netherlands:

Aspect	Indonesia	Netherlands
LEGAL AND INSTITUTIONAL FRAMEWORK		
Legal Framework	Law No. 40/1999 on Press; fragmented digital protection (UU ITE, UU PDP); KUHP.	Criminal Code Arts. 261-262 for defamation; Media Act 2008; GDPR Article 85 implementation via UAVG Art. 43; Anti-doxing law (2024).
Press Council Model	Dewan Pers - independent statutory body established 1999 under UU Pers Art. 15; quasi-governmental status.	Raad voor de Journalistiek - independent self-regulatory body established 1948; purely voluntary industry initiative.
Protection Against Doxing	No mechanism to shield journalists' addresses from public registries, UU PDP Arts. 65 & 67 provide general prohibitions only.	Anti-doxing criminal law (2023, effective 2024); journalists can shield personal data from public registries where "serious threat" exists (NVJ-Kadaster Agreement, June 2024)
Sanction Escalation for Crimes Against Journalists	None; journalists receive no elevated protection status; general criminal sanctions apply without differentiation.	Public Prosecution Service commitment under PersVeilig: 200% increased sanctions (doubling base penalty) for all crimes against journalists.
Good Faith Defense Availability	No explicit good faith journalism defense in UU ITE Art. 27(3); KUHP Baru Art. 433(3) adds "public interest" exception but scope unclear; burden on defendant to prove.	Explicit statutory defense in Criminal Code Art. 261(3): no liability if act necessary to defend interests OR journalist believed in good faith allegations were true AND publication necessary for public interest.

Journalistic Exception in Data Protection Law	None; UU PDP Arts. 15(1) & 50 exclude only state interests (national defense, law enforcement, public administration, financial supervision, scientific research).	Yes; GDPR Art. 85 mandates reconciliation of data protection with press freedom; Dutch UAVG Art. 43 provides explicit exemption allowing processing personal data for journalistic purposes when publication serves public interest.
---	--	--

Table 1. Comparative legal analysis of doxing regulation in Indonesia and the Netherlands

V. CONCLUSION

A comparative legal analysis of doxing regulations in Indonesia and the Netherlands reveals critical structural divergences across four dimensions: statutory explicitness, institutional capacity, legal culture, and enforcement tools. The Netherlands demonstrates explicit anti-doxing legislation, specialized PersVeilig coordination mechanisms with binding police/prosecutor commitments, rights-protective legal culture, and comprehensive prevention-punishment enforcement tools. Indonesia suffers from statutory ambiguity (doxing lacks explicit criminalization), fragmented institutional authority, authoritarian legal culture (UU ITE prosecutions target "insults to officials"), and exclusively reactive punishment-based tools. However, interview evidence reveals that the Indonesian Press Council's mediation mechanisms are perceived as "sudah cukup bagus" (already quite good), demonstrating that Press Council protections function effectively when properly utilized, the critical deficiency lies not in Press Council design but in systematic law enforcement bypassing of these mechanisms despite Press Council's lex specialist status and the ultimum remedium principle. The fundamental problem is that journalist protection operates as systemic architecture where statutory gaps, fragmented coordination, authoritarian culture, and inadequate enforcement tools collectively undermine even strong Press Council mechanisms. Indonesia must intervene simultaneously across all dimensions while leveraging existing Press Council strengths: (1) enact explicit Article 27C to UU ITE criminalizing doxing; (2) operationalize Personal Data Protection Agency with PersVeilig-equivalent

capacity; (3) establish multi-stakeholder safety protocol integrated with Press Council; (4) undertake legal culture transformation emphasizing journalist protection as state obligation. Only comprehensive systemic reform leveraging existing institutional strengths while addressing coordination failures can shift journalist protection from aspirational norm to operational reality.

ACKNOWLEDGMENTS

This research was financially supported by the *Dana DPA Fakultas Hukum Universitas Negeri Semarang (UNNES) Year 2025*. The author also extends sincere appreciation to the journalists who generously participated as informants and kindly shared their professional experiences and providing valuable insights and perspectives. Their valuable contributions were essential to the successful completion of this research.

REFERENCES

“Act of 12 July 2023 Amending the Criminal Code, the BES Criminal Code, the Code of Criminal Procedure and the BES Code of Criminal Procedure in Connection with the Criminalization of Obtaining, Distributing or Otherwise Making Available Personal Data for Intimidating Purposes (Criminalization of the Use of Personal Data for Intimidating Purposes).” Ministry of Justice and Security Netherlands, July 28, 2023. <https://zoek.officielebekendmakingen.nl/stb-2023-274.html>.

Aliansi Jurnalis Independen. “AJI Jakarta Kecam Doxing Terhadap Jurnalis Liputan6com.” December 9, 2020. <https://aji.or.id/berita-aji/aji-jakarta-kecam-doxing-terhadap-jurnalis-liputan6com>.

Aliansi Jurnalis Independen. “AJI Malang Kecam Doxing Terhadap Dua Jurnalis Nusadaily.Com.” September 21, 2021. <https://aji.or.id/berita-aji/aji-malang-kecam-doxing-terhadap-dua-jurnalis-nusadailycom>.

Andriana Putri, Nafila. “Doxing Untuk Malicious Purposes vs Doxing Untuk Political Purposes: Urgensi Pengklasifikasian Ancaman Hukuman Bagi Para Pelaku Doxing Dalam Undang-Undang Nomor 27 Tahun 2022

Tentang Perlindungan Data Pribadi.” *Padjadjaran Law Review* 11, no. 1 (2023): 105–15. <https://doi.org/10.56895/plr.v11i1.1286>.

Balqis, Darin Rania, and Zainuddin Muda Z. Monggilo. “Doxing Sebagai Ancaman Baru Jurnalis Online: Menelisik Kasus Doxing Jurnalis Liputan6.Com.” *Jurnal Komunikasi* 14, no. 2 (2024): 133–44. <https://doi.org/10.31294/jkom.v14i2.15651>.

“Constitution for the Kingdom of the Netherlands, after the Amendment of 2018.” Ministry of the Interior and Kingdom Relations, February 28, 2019. <https://www.rijksoverheid.nl/documenten/rapporten/2019/02/28/grondwet-voor-het-koninkrijk-der-nederlanden-2018>.

“Data Protection in the Netherlands.” *DLA Piper*, n.d. <https://www.dlapiperdataprotection.com/?t=authority&c=NL>.

Douglas, David M. “Doxing: A Conceptual Analysis.” *Ethics and Information Technology* 18, no. 3 (2016): 199–210. <https://doi.org/10.1007/s10676-016-9406-0>.

Dutch News. “Doxing to Become a Criminal Offence Carrying 2-Year Sentence.” December 7, 2023. <https://www.dutchnews.nl/2023/07/doxing-to-become-a-criminal-offence-carrying-2-year-sentence/>.

“General Data Protection Regulation (GDPR).” <https://gdpr.eu/article-4-definitions/>, n.d. <https://gdpr.eu/article-4-definitions/>.

Government of the Netherlands. “Use of Personal Data for the Objective of Harassment to Become Criminal Offence.” December 7, 2023. <https://www.government.nl/latest/news/2023/07/12/use-of-personal-data-for-the-objective-of-harassment-to-become-criminal-offence>.

Klötters, Remco. “Netherlands Media Law Guide, Defamation and Privacy Law in the Netherlands.” *Carter-Ruck*, n.d. <https://www.carter-ruck.com/law-guides/defamation-and-privacy-law-in-netherlands/>.

Mahendra, Khumar. “Dua Jurnalis CNN Indonesia Kena Doxing Usai Liput Aksi Indonesia Gelap, Apa Sanksi Bagi Pelakunya.” *Tempo*, January 25, 2025. <https://www.tempo.co/hukum/dua-jurnalis-cnn-indonesia-kena-doxing-usai-liput-aksi-indonesia-gelap-apa-sanksi-bagi-pelakunya-1212008>.

Marsiela, Adi, and Luh De Suriyani. "Panduan Keamanan Digital Untuk Jurnalis." Aliansi Jurnalis Independen, 2022. <https://aji.or.id/data/panduan-keamanan-digital-untuk-jurnalis>.

Marzuki, Peter Mahmud. *Penelitian hukum*. Kencana, 2005.

Media Freedom Rapid Response. "Netherlands: Towards a Safer Haven: Advancing Safety of Journalists amidst Rising Threats in the Netherlands." February 2022. <https://www.ecpmf.eu/wp-content/uploads/2022/04/Towards-a-safer-haven-Advancing-safety-of-journalists-amidst-rising-threats-in-the-Netherlands.pdf>.

N, Satria Adhi. "Doxing, Bentuk Ancaman Baru Kebebasan Pers." *Universitas Gajah Mada*, May 26, 2021. <https://ugm.ac.id/id/berita/21170-doxing-bentuk-ancaman-baru-kepada-kebebasan-pers/>.

Rambatan, Bonnibel. *On the State of Digital Authoritarianism in Indonesia and Its Contradictions*. n.d. <https://newnaratif.com/on-the-state-of-digital-authoritarianism-in-indonesia/>.

Ridwan, Ridwan, and Muhammad Anshar. "Analisis Regulasi Jurnalistik Pada Undang-Undang Pers No. 40 Tahun 1999." *LITERA: Jurnal Ilmiah Mutidisiplin* 2, no. 1 (2024): 42–61. <https://litera-academica.com/ojs/litera/article/view/77>.

*SAFE*net (Denpasar). "Statement on Digital Repression During the August 2025 Indonesian Protests." August 31, 2025. <https://safenet.or.id/2025/08/statement-on-digital-repression-during-the-august-2025-indonesian-protests/>.

Saly, Jeane Neltje, and Tabriz Sulthanah Lubna. "Pelindungan Data Pribadi Dalam Tindakan Doxing Berdasarkan Undang-Undang Nomor 27 Tahun 2022." *Jurnal Kewarganegaraan* 7, no. 2 (2023): 1708–13.

Sari, Rintan Puspita. "Persekusi Doxing Sebagai Pola Baru Viktimisasi Terhadap Jurnalis Di Indonesia." *Deviance Jurnal Kriminologi* 5, no. 1 (2021): 68. <https://doi.org/10.36080/djk.1139>.

Sarjito, Aris. "Hoaks, Disinformasi, Dan Ketahanan Nasional: Ancaman Teknologi Informasi Dalam Masyarakat Digital Indonesia." *Journal of Governance and Local Politics (JGLP)* 6, no. 2 (2024): 175–86. <https://doi.org/10.47650/jglp.v6i2.1547>.

Satria, Muhammad Kamarulzaman, and Hadi Yusuf. "Analisis Yuridis Tindakan Kriminal Doxing Ditinjau Berdasarkan Undang Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi." *Jurnal Intelek Dan Cendekiawan Nusantara* 1, no. 2 (2024): 2442–56. <https://jicnusantara.com/index.php/jicn/article/view/266>.

Soerjono Soekanto. *Penelitian Hukum Normatif*. 2006.

Sunstein, Cass R. "Lies and Falsehoods." In *Liars*, 1st ed., by Cass R. Sunstein. Oxford University Press New York, 2021. <https://doi.org/10.1093/oso/9780197545119.003.0001>.

Syailendra, Moody Rizqi, arah Angelina Setiahata Lumban Tobing, Keiko Patricia Liwe, and Hanivah Fitriyani. *STUDI KASUS SEBUAH ANCAMAN TERHADAP PRIVASI KASUS DOXING DI INDONESIA DALAM PERSPEKTIF HUKUM DAN ETIKA*. 4, no. 4 (2024): 32–45.

"The Netherlands." *Centre For Media Pluralism and Media Freedom*, n.d. <https://cmpf.eui.eu/country/the-netherlands/>.

Ufen, Andreas. "The Rise of Digital Repression in Indonesia under Joko Widodo." *GIGA Focus Asia* 1 (2024). <https://doi.org/10.57671/GFAS-24012>.

Utami, Sal Sabila Khoirotunnisa. "Doxing As A Digital Crime: A Human Rights And Privacy Protection Perspective Under Indonesian Law." *Domus Legalis Cogitatio* 2, no. 2 (2025): 147–64. <https://doi.org/10.24002/dlc.v2i2.9912>.