MITSAQAN GHALIZAN
Journal homepage: https://journal.umpr.ac.id/index.php/jmg
E-ISSN: 2964-2191
Vol.6 No. 1 June 2026

A Multifaceted Approach to Doxing Offenses: Assessing Legal Responses Drawing from National, Islamic Criminal, and Human Rights Frameworks

Abdul Syatar[1], Alamsyah Halim[2], Muhammad Fazlurrahman Syarif[3]
[1,2] Universitas Islam Negeri Alauddin Makassar, Indonesia
[3] Hamad bin Khalifa University, Doha, Qatar
* Corresponding Author: abdul.syatar@uin-alauddin.ac.id
DOI: https://doi.org/10.33084/mg.v6i1.12851

Received: 06-05-2026 Revised: 06-06-2026 Accepted: 26-06-2026

Article

Keywords:
Document Tracing; Doxing; National Law; Islamic Criminal Law; Human Rights.

How to cite:
Syatar, A., Halim, A., & Syarif, M. F. (2026). *A Multifaceted Approach to Doxing Offenses: Assessing Legal Responses Drawing from National, Islamic Criminal, and Human Rights Frameworks. Mitsaqan Ghalizan*, 6(1), 53–69. https://doi.org/10.33084/mg.v6i1.12851

Abstract

This study examines the phenomenon of document tracing, commonly referred to as doxing, as a growing legal and ethical challenge in Indonesia. It aims to analyze how national law, Islamic criminal law, and human rights frameworks respond to doxing, particularly in safeguarding privacy and protecting individuals from reputational and security harms. Employing a qualitative–empirical design, the research combines document analysis with case studies through a comparative approach. Data were collected via semi-structured interviews with academics, religious scholars, and activists, complemented by observation and a review of relevant laws, policies, and real-life instances of doxing. Triangulation was used to ensure credibility and comprehensiveness. The findings reveal that Indonesia has addressed doxing primarily through the Information and Electronic Transactions (ITE) Law, the Personal Data Protection Law, and provisions in the Criminal Code. From the perspective of Islamic criminal law, doxing is classified as *al-jarā'im al-maḥẓūrāt* (prohibited acts) that violate privacy, with punishments potentially falling under *ḥudūd* or *ta'zīr*. In both legal systems, doxing is recognized as a violation of fundamental human rights, particularly the right to privacy and dignity. Unlike prior studies that focus narrowly on either legal or technological dimensions, this research integrates national law, Islamic jurisprudence, and human rights principles into a unified analysis. It highlights the role of *maqāṣid al-sharī'a* in developing privacy protections and in bridging classical legal concepts with contemporary digital realities. The study suggests that strengthening legal frameworks through both statutory reform and Islamic jurisprudential interpretation can provide more equitable protection for citizens. These findings contribute to broader debates on digital ethics, privacy, and the harmonization of religious and secular legal systems in addressing emerging cybercrimes.

INTRODUCTION

The digital age has transformed privacy into a vulnerable commodity.[1] The widespread use of social media platforms such as Instagram, Facebook, Twitter, and TikTok has made personal information easily accessible.[2] Individuals often disclose details voluntarily, yet these data points can be exploited for harmful purposes.[3] Reports indicate that over 4.9 billion people worldwide are active on social media, with approximately 60% sharing personal details online.[4] Cybercrime cases linked to identity theft and doxing have surged globally, showing a 151% increase between 2019 and 2021.[5] In Indonesia alone, the Ministry of Communication and Information recorded more than 190 million cyberattacks in 2022, many of which involved breaches of personal data.[6] These alarming statistics illustrate that social media has become both a tool of connectivity and a threat to individual security.

Scholars remain divided over whether doxing is a form of protection or a violation of rights.[7] Some argue that restricting doxing protects privacy,[8] while others emphasize that freedom of expression and the disclosure of harmful conduct are equally important.[9] This tension creates ongoing debates in legal and academic circles.[10] Doxing as a severe privacy violation that can endanger lives, while other studies suggest it may serve democratic functions by exposing corruption or misconduct.[11] The European Union's General Data Protection Regulation (GDPR) strongly prohibits unauthorized disclosure of personal data, yet many jurisdictions

---

[1] Ayah Hamad and Bochen Jia, "How Virtual Reality Technology Has Changed Our Lives: An Overview of the Current and Potential Applications and Limitations," *International Journal of Environmental Research and Public Health* 19, no. 18 (2022), https://doi.org/10.3390/ijerph191811278.

[2] Esteban Ortiz-Ospina, "The Rise of Social Media," *Our World in Data*, 2019, https://ourworldindata.org/rise-of-social-media.

[3] Hamidreza Shahbaznezhad, Rebecca Dolan, and Mona Rashidirad, "The Role of Social Media Content Format and Platform in Users' Engagement Behavior," *Journal of Interactive Marketing* 53 (2021): 47–65, https://doi.org/10.1016/j.intmar.2020.05.001.

[4] Statista, "Social Media," statista.com, 2025, https://www.statista.com/topics/1164/social-networks/.

[5] Mohammad Fadil Imran, "Preventing and Combating Cybercrime in Southeast Asia," *International Journal of Cyber Criminology* 17, no. 1 (2023): 223–33, https://doi.org/10.5281/zenodo.4766614.

[6] Enni Soerjati Priowirjanto Teguh Cahya Yudiana, Sinta Dewi Rosadi, "The Urgency of Doxing on Social Media Regulation and the Implementation of Right to Be Forgotten on Related Content for the Optimization of Data Privacy Protection in Indonesia," *Padjadjaran Jurnal Ilmu Hukum* 9, no. 1 (2022): 24–45, https://doi.org/10.22304/pjih.v9n1.a2.

[7] 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.

[8] Andriana Putri.

[9] Anne Cheung, "Doxing and the Challenge to Legal Regulation: When Personal Data Become a Weapon," *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, 2021, 577–94, https://doi.org/10.1108/978-1-83982-848-520211041.

[10] 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.

[11] Thania Christy Corne, "Legal Protection of Privacy Data Through Encryption Technology," *Lampung Journal of International Law* 1, no. 2 (2020): 63–70, https://doi.org/10.25041/lajil.v1i2.2027.

still lack explicit laws on doxing.[12] Furthermore, classification of doxing into malicious, political, and self-regulatory categories reveals its multifaceted nature.[13] These contrasting views demonstrate that doxing lies at the intersection of privacy rights, public interest, and legal ambiguity.

Despite the rising prevalence of doxing, comprehensive academic studies remain scarce. Existing research often highlights its dangers but rarely offers detailed legal analysis or comparative perspectives. Addressing this gap requires contextualized examination across national and religious legal frameworks. Previous studies largely focus on Western legal contexts, leaving a limited understanding of doxing in Islamic criminal law.[14] Indonesian research, while acknowledging cybercrime, often treats doxing as a subset of identity theft without addressing its independent legal implications.[15] Consequently, there remains an urgent need to evaluate how national and Islamic legal systems conceptualize and respond to doxing.[16] This study therefore seeks to investigate the legal treatment of doxing, particularly within the framework of Islamic criminal law and national legislation.

Understanding doxing through the lens of Islamic law provides unique insights into balancing rights and protections. Islamic criminal law considers doxing not only a violation of privacy but also a transgression against fundamental human dignity. Such a perspective enriches global legal debates by offering moral and ethical considerations alongside legal reasoning. The Qur'an explicitly prohibits *tajassus* (spying) and public exposure of faults (Q.S. al-Hujurat: 12), aligning with the principle of protecting individuals from harm. Scholars such as Al-Buthy classify privacy violations as offenses undermining social harmony,[17] while contemporary jurists argue that online doxing constitutes a modern form of *hirābah* (cyber-aggression). Comparative studies show that integrating Islamic legal principles could strengthen protective measures against doxing in Muslim-majority societies.

---

[12] Batuhan Kukul, "Personal Data and Personal Safety: Re-Examining the Limits of Public Data in the Context of Doxing," *International Data Privacy Law* 13, no. 3 (2023): 182–93, https://doi.org/10.1093/idpl/ipad011.

[13] Teguh Cahya Yudiana, Sinta Dewi Rosadi, "The Urgency of Doxing on Social Media Regulation and the Implementation of Right to Be Forgotten on Related Content for the Optimization of Data Privacy Protection in Indonesia."

[14] Hannah C Mery, "The Dangers of Doxing and Swatting: Why Texas Should Criminalize These Malicious Forms of Cyberharassment," *St. Mary's Law Journal* 52, no. 3 (2021): 1–40, https://commons.stmarytx.edu/thestmaryslawjournal/vol52/iss3/8.

[15] Titis Anindyajati, "Limitation of the Right To Freedom of Speech on the Indonesian Constitutional Court Consideration," *Indonesian Law Journal* 14, no. 1 (2021): 19–36, https://doi.org/10.33331/ilj.v14i1.45.

[16] M. Lutfi Chakim, "Freedom of Speech and the Role of Constitutional Courts: The Cases of Indonesia and South Korea," *Indonesia Law Review* 10, no. 2 (2020): 191–205, https://doi.org/10.15742/ilrev.v10n2.605.

[17] Supardin Supardin and Abdul Syatar, "Adultery Criminalization Spirit in Islamic Criminal Law: Alternatives in Indonesia's Positive Legal System Reform," *Samarah: Jurnal Hukum Keluarga Dan Hukum Islam* 5, no. 2 (2021): 913–27, https://doi.org/10.22373/sjhk.v5i2.9353.

Incorporating Islamic legal perspectives can offer a holistic framework to address doxing, safeguarding both privacy and public welfare.

METHOD

Investigating doxing requires a design that captures both its legal complexity and human impact. This study adopts a literature approach using a comparative legal framework to examine doxing in national and Islamic contexts. Data were collected through non-participant observation, semi-structured interviews with academics, religious authorities, and activists, as well as analysis of laws, policies, and real-life cases. Qualitative approaches are effective for exploring context-bound legal phenomena. Purposeful sampling ensured access to informants with expertise, while snowballing extended the reach to hidden actors. Triangulating observation, interviews, and documents enhances credibility and completeness of findings. This design and collection strategy generated a robust dataset capable of reflecting both doctrinal debates and lived experiences of doxing.

The study employed data reduction, display, and conclusion drawing while coding themes across empirical patterns and legal categories. Simultaneously, ethical safeguards, confidentiality, anonymization, and compliance with data protection law-were embedded in every stage. The reduction–display–conclusion cycle is a validated analytic framework for qualitative studies.[18] Analytic memoing, coding cycles, and member checks improved reliability, while comparative matrices aligned findings with legal principles. Ethical protocols followed the Belmont Report (1979), the Association of Internet Researchers (2019), and Indonesia's PDP Law No. 27/2022 to minimize harm and protect identities. Through rigorous analysis and strong ethical protections, the study ensures findings are both trustworthy and socially responsible.

RESULTS AND DISCUSSION

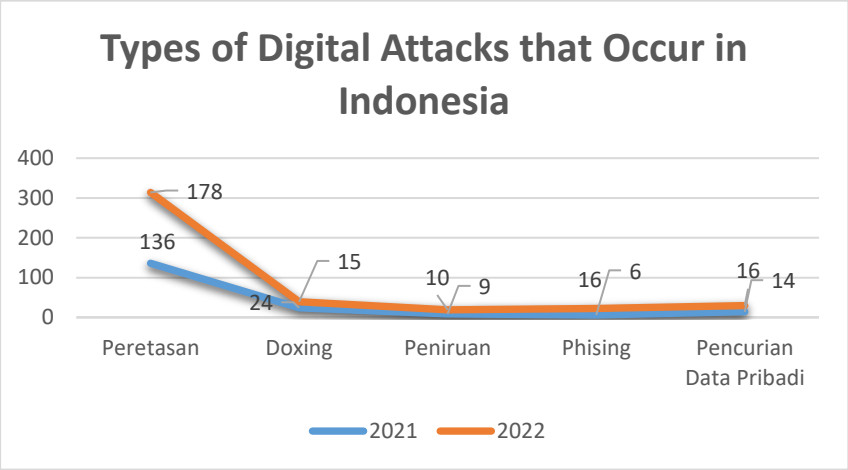
National Legal Regulations for Doxing Cases

The practice and phenomena of doxing are becoming increasingly uncomfortable in Indonesia due to the rise in digital activities in the modern era.[19] Despite being acknowledged Not yet have a clear strategy to overcome the act of doxing on my own. Regulations that can serve as a minimum standard for addressing doxing. Several regulations govern this matter, including the Information and

[18] Miles, M.B., Huberman, A.M., Saldana, J, *Qualitative Data Analysis; A Methods Sourcebook*, 3rd ed. (Los Angeles: SAGE Publications, 2014).

[19] Sayid Muhammad and Rifqi Noval, "Doxing Phenomenon in Indonesia: Amid Waiting for Privacy Settings," *Budapest International Research and Critics Institute (BIRCI-Journal): Humanities and Social Sciences* 4, no. 3 (2021): 3636–44, https://doi.org/10.33258/birci.v4i3.2132 3636.

Transactions Electronics (ITE Law),[20] Personal Data Protection Law, Criminal Code (KUHP),[21] and digital platform policies.



Source: Processed from dataindonesia.id

The ITE Law is one of the regulations. The primary governing body responsible for regulating policies in the realm of cyberspace in Indonesia.[22] In the context of doxing, the ITE Law forbids the unauthorized dissemination of personal information.[23] Prohibition can result in criminal offenses and carry penalties. Articles 26 and 27 of the ITE Law address the issue of doxing.[24] However, the implementation and enforcement of ITE Law statutes often become a subject of discussion and criticism due to the ambiguity of key clauses.

The violation of Article 27, paragraphs (1), (2), and (4) of the ITE Law is punishable by a potential prison sentence of 6 years and/or a maximum fine of IDR 1 billion. Temporarily, violating Article 27 paragraph (3) of the ITE Law can result in a maximum prison sentence of 4 years and/or a maximum fine of IDR 750 million.[25]

---

[20] Teguh Cahya Yudiana, Sinta Dewi Rosadi, "The Urgency of Doxing on Social Media Regulation and the Implementation of Right to Be Forgotten on Related Content for the Optimization of Data Privacy Protection in Indonesia."

[21] Thomas Paterson, "Indonesian Cyberspace Expansion: A Double-Edged Sword," *Journal of Cyber Policy* 4, no. 2 (2019): 216–34, https://doi.org/10.1080/23738871.2019.1627476.

[22] Halif Halif, Ainul Azizah, and Prisma Diyah Ratrini, "Regulating Doxing and Personal Data Dissemination in Indonesia," *Jurnal Kajian Pembaruan Hukum* 3, no. 1 (2023): 61, https://doi.org/10.19184/jkph.v3i1.33938.

[23] Ni Nyoman et al., "Uploading Private Chat Screenshots on Social Media : How the Law Respond It ?," *Udayana Master Law Journal* 1, no. 1 (2023): 1–8, https://doi.org/10.24843/JMHU.2023.v12.i0.

[24] Intan Uweng Saripa, Hadibah Zachra Wadjo, and Judy Marria Saimima, "Perlindungan Hukum Pidana Terhadap Doxing Menurut Undang-Undang Informasi Dan Transaksi Elektronik," *Pattimura Law Study Review* 1 (2023): 168–79, https://doi.org/10.47268/palasrev.v1i1.10897.

[25] Pemerintah Republik Indonesia, "Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," *Pemerintah Republik Indonesia* (Jakarta, 2016), https://web.kominfo.go.id/sites/default/files/users/4761/UU 19 Tahun 2016.pdf.

Article 27, paragraph (3) of the ITE Law includes components of "defamation" and "dissemination of harmful content. It is a reference to Article 310 of the Criminal Code, which was established a long time ago. This has been published. The provisions of Article 433 of Law 1/2023, pertaining to the new Criminal Code, remain in effect for a period of three years from the date of promulgation, specifically until 2026.

Indonesia is adequately prepared. Constitution Personal Data Protection involves the specific arrangement for the collecting, processing, and storage of personal data.[26] Rules or guidelines that are set by an authority to control or govern certain activities or behaviors.[27] This can provide extensive and comprehensive protection to individuals and prevent the practice of doxing. Despite being acknowledged, it is not yet fully implemented. The good step of development is the establishment of a constitution for Personal Data Protection to address privacy concerns in the digital age.

Dissemination of information pertaining to arrangements Furthermore, the Criminal Code encompasses anyone who inflict injury upon others. Articles pertaining to pollution include those addressing defamation and insult, as well as article of the Criminal Code, which can be invoked in cases of doxing, particularly where the actions cause injury to someone's honor and reputation such as the criminal offense of defamation against Joko Widodo.[28]

Various digital platforms, including social media and online forums, have distinct policies on privacy violations and doxing.[29] Doxers (doxing perpetrators) have the ability to either forbid or delete their account in accordance with the platform's internal standards.

Dealing with doxing instances in Indonesia requires the involvement of law enforcement agencies, authorized parties, and the general public.[30] Being aware of the hazards and bad repercussions of doxing, as well as prioritizing education on digital security, has become critical and important for mitigating the problem of doxing.[31]

---

[26] Tiurma Mangihut Pitta Adhiwisaksana, Muhammad Faqih; Allagan, "Competent Forum and Applicable Law in Personal Data Protection with a Foreign Element," *Indonesian Journal of International Law* 20, no. 3 (2023): 442, https://scholarhub.ui.ac.id/ijil/vol20/iss3/2/.

[27] Diana Setiawati, Hary Abdul Hakim, and Fahmi Adam Hasby Yoga, "Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore," *Indonesian Comparative Law Review* 2, no. 2 (2020): 2–9, https://doi.org/10.18196/iclr.2219.

[28] Fara Dina Zein, "Analisa Hukum Tindak Pidana Pencemaran Nama Baik Terhadap Joko Widodo Melalui Tabloid Obor Rakyat," *Jurnal Pembaharu Hukum* 1, no. 1 (2020): 61–75.

[29] Suci Marini Novianty, Sri Wijayanti, and Jihad Muamar, "Ethical Discourse of Doxing in Indonesian Twitter Users," *Jurnal InterAct* 12, no. 1 (2023): 1–13, https://doi.org/10.25170/interact.v12i1.4134.

[30] 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."

[31] Halif, Azizah, and Ratrini, "Regulating Doxing and Personal Data Dissemination in Indonesia."

The coordination and cooperation between party authorities and society aim to establish a safe and secure internet environment.

Several countries have implemented Constitutions that align with the General Data Protection Regulations (GDPR) to ensure consistent safeguarding of personal data.[32] Since the European Union implemented the General Data Protection Regulation (GDPR) in May 2018, several other countries and areas worldwide have either adopted or updated their laws on personal data protection to align with comparable concepts.[33] Some countries have directly taken inspiration from GDPR to independently construct their own framework laws. The General Data Protection Regulation (GDPR) applies not only to enterprises within the European Union, but also to all organizations worldwide that store and process personal data, including businesses in Indonesia. This issue is evident in the technology practices of firms like Google and Facebook, who send emails to inform users of updates to their privacy policies.[34] These emails clarify the specific data that the company collects and how it is used. The impact of GDPR on firms in the digital industry, particularly startups, can be observed in Indonesia. Entrepreneurs can modify their Terms and Conditions and privacy policies to align with the GDPR and relevant Indonesian regulations to comply with GDPR requirements and improve their personal data operations. If an entrepreneur violates GDPR, they may face more severe consequences.

Islamic Criminal Law and Doxing as Violation Privacy

Islamic criminal law does not explicitly regulate the modern concepts of privacy and doxing.[35] Despite this absence, the law emphasizes principles that safeguard dignity and interpersonal ethics. To interpret these principles for contemporary issues, the guidance of academic experts and legal authorities becomes essential. Scholars note that while Sharīʿah texts rarely mention modern technological violations, their spirit is broad enough to cover emerging issues.[36] Legal principles

[32] Syed Khurrum Husain Naqvi and Komal Batool, "A Comparative Analysis between General Data Protection Regulations and California Consumer Privacy Act," *Journal of Computer Science, Information Technology and Telecommunication Engineering* 4, no. 1 (2023): 326–32, https://doi.org/10.30596/jcositte.v4i1.13330.

[33] Arturo J. Carrillo and Matías Jackson, "Follow the Leader? A Comparative Law Study of the EU's General Data Protection Regulation's Impact in Latin America," *ICL Journal* 16, no. 2 (2022): 177–262, https://doi.org/10.1515/icl-2021-0037.

[34] Yohanes Hermanto Sirait, "General Data Protection Regulation (Gdpr) Dan Kedaulatan Negara Non-Uni Eropa," *Gorontalo Law Review* 2, no. 2 (2019): 60, https://doi.org/10.32662/golrev.v2i2.704.

[35] Ita Musarrofa and Holilur Rohman, "'Urf of Cyberspace: Solutions to the Problems of Islamic Law in the Digital Age," *Al-Ahkam* 33, no. 1 (2023): 63–88, https://doi.org/10.21580/ahkam.2023.33.1.13236.

[36] Wahyuddin Naro et al., "Shariah Assessment Toward the Prosecution of Cybercrime in Indonesia," *International Journal of Criminology and Sociology* 9 (2020): 572–86, https://doi.org/https://doi.org/10.6000/1929-4409.2020.09.5.

such as *hifẓ al-'ird* (protection of honor) and *hifẓ al-māl* (protection of property) extend naturally to the digital sphere.[37] Comparative studies show that many Muslim jurists classify new cybercrimes under classical ethical and legal categories.[38] Although the term "doxing" is modern, its underlying prohibition is firmly grounded in Islamic principles.

Privacy protection is deeply woven into the ethical structure of Islamic law. Islam stresses respectful interactions, condemning unjust interference in others' personal lives. These principles are intended not only for theoretical discourse but also for practical application in daily life. The Qur'an commands believers to "enter not houses other than your own without first announcing your presence" (Q.S. al-Nur: 27),[39] reflecting the sanctity of private space. Classical jurists emphasized the principle of *satr al-'awrah* (covering vulnerabilities), which extends to informational privacy.[40] Contemporary fatwas have reiterated that modern intrusions like digital spying violate these same timeless principles.[41] Accordingly, Islamic law offers enduring guidance for protecting privacy, even amid new technological contexts.

The maqāṣid al-sharī'ah framework situates privacy as a fundamental value worth protecting. Within Islamic criminal law, the principle of *hifẓ al-māl* (protection of property) and *hifẓ al-'ird* (protection of honor) serve as barriers against unauthorized intrusions. These aims of the law extend beyond material security to cover informational and reputational safety. Auda argues that maqāṣid provide a dynamic tool to interpret Sharī'ah in light of modern challenges.[42] For instance, protecting human dignity ranks alongside preserving religion, life, intellect, and wealth. Studies have shown that courts in Muslim countries often rely on maqāṣid reasoning when confronting new crimes not mentioned in classical texts.[43] Maqāṣid-based reasoning offers a solid foundation for prohibiting doxing as an unlawful act.

Spreading harmful private information resembles the classical prohibition of *ghibah* (backbiting). Both practices involve exposing faults and damaging reputations without justification. When carried out intentionally, doxing aligns with *al-jarā'im al-*

---

[37] 'Abdul Qadir 'Audah, *Al-Tasyri' Al-Jinā'i Al-Islāmī; Muqāranan Bi Al-Qanūn Al-Wadh'I*, II (Cairo: Maktabah al-Taufiqiyah, 2013).

[38] Arskal Salim, "Contemporary Islamic Law in Indonesia : Sharia and Legal Pluralism," vol. 6, 2015, 232, https://ecommons.aku.edu/cgi/viewcontent.cgi?article=1007&context=uk_ismc_series_emc.

[39] Dapit Amril, "Etika Informasi Dalam Perspektif Al-Qur'an," *Alfuad: Jurnal Sosial Keagamaan* 1, no. 1 (2018): 54, https://doi.org/10.31958/jsk.v1i1.1157.

[40] 'Audah, *Al-Tasyri' Al-Jinā'i Al-Islāmī; Muqāranan Bi Al-Qanūn Al-Wadh'I*., pp. 12.

[41] Muhammad Alwin Abdillah, Nairazi, and Lina Agustina, "Copyright Infringement Crime in Islamic Criminal Law," *Legalite : Jurnal Perundang Undangan Dan Hukum Pidana Islam* 7, no. 2 (2022): 119–31, https://doi.org/10.32505/legalite.v7i2.5368.

[42] 'Audah, *Al-Tasyri' Al-Jinā'i Al-Islāmī; Muqāranan Bi Al-Qanūn Al-Wadh'I*.

[43] Alfitri Alfitri, "Can the Requirements of Shariah Law Regarding Criminal Punishments Be Interpreted in a Way That Is Compatible With the Iccpr and Cat?," *Indonesian Journal of International Law* 7, no. 1 (2021), https://doi.org/10.17304/ijil.vol7.1.230.

maḥẓūrāt—acts that are strictly forbidden in Islamic law. The Qur'an equates *ghibah* to eating the flesh of one's dead brother (Q.S. al-Hujurat: 12), underscoring its gravity. Scholars like Al-Buthy extend this prohibition to public defamation, including through new media. Modern jurists emphasize that online platforms merely amplify the scale of sin, without altering its essence.[44] Intentional doxing clearly falls under long-standing Islamic prohibitions against defamation and privacy violation.

In Islamic law, the classification of acts depends heavily on intention and harm. Doxing committed to injure is distinct from cases aimed at protecting the public interest or exposing corruption. Judges must therefore consider motives and effects when categorizing such acts. Islamic jurisprudence differentiates between *jarīmah muḥarramah* (prohibited crimes) and actions justified by necessity (*ḍarūrah*).[45] For example, publicizing harmful conduct may fall under *hisbah* (social accountability) rather than *ghibah*. However, malicious disclosure without justification is classified among the gravest offenses against personal dignity. This nuanced framework allows Islamic law to distinguish between legitimate whistleblowing and unlawful doxing.

Islamic criminal law provides punishments rooted in fairness and protection of rights. Where doxing does not fall under fixed penalties (*hudūd*), it is punishable by discretionary sanctions (*ta'zīr*). Judges are expected to evaluate intent, impact, and social consequences in assigning punishment. *Ta'zīr* grants flexibility for emerging crimes, enabling penalties such as fines, imprisonment, or public admonishment. Case studies show that judges often weigh factors like repentance, level of harm, and societal disruption before issuing rulings. Comparative analysis reveals that Muslim countries integrate both Sharī'ah principles and state laws when dealing with digital privacy violations. Judicial discretion ensures punishments for doxing remain proportionate and context-sensitive.

Today, enforcement of doxing-related violations varies across Muslim communities and legal systems. While some countries integrate Islamic criminal law directly into their statutes, others rely more heavily on secular cybercrime frameworks. In practice, victims must often seek redress through courts, police, or legal professionals. In Indonesia, Law No. 27/2022 on Personal Data Protection supplements Islamic principles by criminalizing data misuse. In Saudi Arabia and Qatar, cybercrime laws explicitly prohibit unauthorized disclosure of personal information, reflecting Sharī'ah-inspired protections. Victims of doxing are advised to report cases to law enforcement or consult legal experts for recourse, ensuring their rights are upheld within both state and Islamic frameworks. Ultimately, the integration of Islamic principles with modern legal systems provides victims of doxing with multiple avenues for protection and justice.

---

[44] Mahrus Ali and M. Arif Setiawan, "Penal Proportionality in Environmental Legislation of Indonesia," *Cogent Social Sciences* 8, no. 1 (2022), https://doi.org/10.1080/23311886.2021.2009167.

[45] Hamzah Hasan, "Interview, May" (Makassar, 2023).

Doxing and Human Rights

Doxing, commonly understood as the intentional exposure of someone's private information without consent, has emerged as one of the most pressing human rights challenges in the digital era.[46] The act directly undermines the individual's right to privacy, a principle universally acknowledged as an inherent and inalienable entitlement. Privacy is not simply the ability to shield personal information from public access; rather, it is the autonomy to control how data is collected, stored, shared, and used. When that autonomy is stripped away, individuals are rendered vulnerable to surveillance, exploitation, and humiliation.[47] Unlike casual data sharing, doxing involves a deliberate intent to cause harm by releasing sensitive information such as home addresses, phone numbers, family details, or workplace affiliations. This transforms the breach of privacy into an act of aggression, violating both the dignity and safety of the targeted person. Human rights frameworks emphasize that every individual has the right to live free from arbitrary interference in their private life, and doxing starkly contravenes this standard. By equating exposure with harm, it demonstrates how technological misuse can subvert foundational human rights principles. The recognition of doxing as a violation of privacy is not merely theoretical but an urgent ethical and legal necessity.

The threat posed by doxing becomes particularly severe when personal details are disseminated online, where the reach is virtually limitless and permanence is difficult to undo.[48] Unlike traditional forms of exposure, the internet ensures that once data is published, it can be replicated, shared, and archived beyond the control of both the victim and the authorities. This creates an environment where sensitive details may be weaponized repeatedly, amplifying the victim's sense of insecurity. The risks are not confined to digital harassment alone; leaked information may also enable physical stalking, burglary, identity theft, or financial fraud.[49] Victims frequently report receiving threatening messages, harassing phone calls, or even confrontations at their homes or workplaces after their information is exposed. These tangible consequences highlight how the digital and physical spheres are increasingly intertwined. Infringement of privacy in cyberspace cannot be treated as a

---

[46] Nyoman et al., "Uploading Private Chat Screenshots on Social Media : How the Law Respond It ?"

[47] Mohd Javaid et al., "Unlocking the Opportunities through ChatGPT Tool towards Ameliorating the Education System," *BenchCouncil Transactions on Benchmarks, Standards and Evaluations* 3, no. 2 (2023): 100115, https://doi.org/10.1016/j.tbench.2023.100115.

[48] Virliana Octav, "Keterkaitan Doxing Terhadap Hak Atas Privasi Dalam Hak Asasi Manusia," 2022, https://kawanhukum.id/keterkaitan-doxing-terhadap-hak-atas-privasi-dalam-hak-asasi-manusia/.

[49] Ananthia Ayu, Titis Anindyajati, and Abdul Ghoffar, "Perlindungan Hak Privasi Atas Data Diri Di Era Ekonomi Digital," *Pusat Penelitian Dan Pengkajian Perkara, Dan Pengelolaan Perpustakaan Kepaniteraan Dan Sekretariat Jenderal Mahkamah Konstitusi* (Mahkamah Agung, 2019), https://www.mkri.id/public/content/infoumum/penelitian/pdf/hasilpenelitian_123_Penelitian Hak Privasi dan Studi Komparasi.pdf.

trivial or abstract issue; rather, it constitutes a direct threat to personal security and bodily integrity. The escalation from digital violation to real-world danger illustrates the unique menace posed by doxing compared to other online misconduct. Thus, doxing should be regarded as a hybrid form of harm, blurring the line between online abuse and offline danger, requiring urgent attention within human rights law.

Beyond individual threats to safety, doxing also carries the potential to exacerbate systemic discrimination and persecution. When targeted at vulnerable populations, doxing becomes a powerful tool of marginalization, enabling attackers to exploit personal data for discriminatory purposes. For instance, individuals may be singled out because of their race, ethnicity, religion, gender identity, sexual orientation, or political beliefs. Once exposed, this information may be used to incite hate speech, encourage mob harassment, or justify acts of persecution. In societies already marked by inequality, doxing can magnify existing vulnerabilities, leaving marginalized individuals further exposed to violence and exclusion. This not only infringes upon the human right to privacy but also undermines the fundamental rights to equality and non-discrimination, which are pillars of international human rights law. The practice resembles a form of digital vigilantism, where perpetrators weaponize information to enforce social or ideological conformity. Victims may be silenced, excluded, or coerced into abandoning their beliefs or identities. This erosion of freedoms illustrates how doxing can have wider societal consequences, undermining the democratic values of pluralism and inclusivity. Thus, the discriminatory potential of doxing should be understood as a grave violation of equality rights, threatening both individual dignity and collective harmony.

Equally significant are the psychological and emotional repercussions that victims of doxing endure. The constant awareness that one's personal details are publicly accessible generates an enduring sense of fear and vulnerability. Victims often describe feeling as though they are under continuous surveillance, which can lead to hypervigilance and severe stress. The anticipation of harassment or retaliation fosters anxiety and may escalate into depressive symptoms or post-traumatic stress disorder (PTSD). For some, the trauma is compounded by the realization that once information is released, it is almost impossible to erase, creating a sense of permanent exposure. This psychological burden is further intensified when harassment spills over into family or professional life, affecting not only the direct victim but also their relatives and colleagues. Human rights frameworks emphasize that dignity and well-being are integral to the right to life, liberty, and security of person. When doxing undermines mental health, it violates not only privacy but also the broader spectrum of human rights associated with psychological integrity. Recognizing the mental health dimension of doxing reframes it from being a mere breach of data protection to a profound ethical crisis. Consequently, addressing

doxing requires integrating mental health safeguards into both legal protections and support systems.

The international community has long recognized the safeguarding of privacy as an essential human right. Landmark documents such as the Universal Declaration of Human Rights (UDHR, Article 12) and the European Convention on Human Rights (ECHR, Article 8) enshrine protection against arbitrary interference in personal and family life. These instruments provide a normative foundation for classifying doxing as a human rights violation. By exposing private data without consent, doxing contravenes the very principles these conventions were designed to uphold. Moreover, these legal frameworks underscore the obligation of states to not only refrain from violating privacy themselves but also to protect individuals from infringements perpetrated by private actors. In the digital era, this responsibility has expanded to include ensuring cybersecurity, regulating data use, and enforcing penalties against online abuse. Treating doxing as a violation under these conventions emphasizes the need for international cooperation, as perpetrators often operate across borders. Thus, embedding doxing within the discourse of international human rights law is not merely symbolic but a necessary step to provide victims with avenues for redress, while also reinforcing global accountability mechanisms that recognize privacy as a non-negotiable element of human dignity.

In response to these international standards, many states have implemented national data protection laws to provide citizens with stronger safeguards against the misuse of personal information. These frameworks typically regulate how personal data is collected, processed, stored, and shared by both public and private entities. They emphasize principles of transparency, informed consent, and proportionality, which are critical in preventing abuses like doxing. Countries such as the United States, Canada, and Singapore have enacted privacy laws tailored to their socio-political contexts, while others draw heavily on international guidelines. Despite variations in implementation, the common goal is to empower individuals with greater control over their personal information while deterring malicious actors through penalties and civil liability. Importantly, national laws often serve as the first line of defense for victims seeking redress, especially in cases where international instruments lack direct enforceability. However, challenges remain in adapting these laws to the evolving digital landscape, where anonymity and transnational activity complicate enforcement. Therefore, while national legislation represents a crucial step forward, it must be continually revised and strengthened to address the ever-changing realities of online harm, particularly those associated with doxing and related forms of digital abuse.

At a regional level, comprehensive frameworks such as the European Union's General Data Protection Regulation (GDPR) provide perhaps the most advanced model for safeguarding personal data in the digital age. The GDPR establishes

uniform standards across member states, ensuring that individuals enjoy consistent protections regardless of jurisdiction. Among its most significant contributions are the rights it grants individuals: the right to access, correct, and delete personal data, as well as the right to object to certain forms of processing. These rights are particularly relevant to the issue of doxing, as they empower victims to demand removal of unlawfully shared information and to seek remedies against violators. Additionally, the GDPR imposes strict obligations on organizations and sets heavy penalties for non-compliance, thereby reinforcing accountability. Its influence extends far beyond Europe, inspiring legislative reforms in countries worldwide that seek to harmonize their data protection standards with global best practices. By framing doxing as a breach of personal data protection, the GDPR not only addresses immediate harms but also contributes to a culture of digital responsibility. Ultimately, such comprehensive approaches illustrate the potential of regional frameworks to shape a more secure and rights-respecting digital environment.

CONCLUSION

The rise of doxing in Indonesia each year represents a critical challenge that not only violates personal privacy but also threatens individual dignity and human rights. This study demonstrates that doxing constitutes a deliberate criminal act, prosecutable under the ITE Law, Islamic criminal law, and international human rights conventions. By analyzing these perspectives together, the research underscores that privacy is not merely a legal concern but a universal entitlement tied to ethical, social, and spiritual values. Nationally, the ITE Law provides both civil and criminal pathways to address unauthorized dissemination of personal data. From an Islamic perspective, doxing is categorized as *al-jarā'im al-mahẓūrāt*, prohibited acts infringing *hifẓ al-'irḍ* (protection of honor) and *hifẓ al-māl* (protection of property), reflecting maqāṣid al-sharī'a's commitment to safeguarding individual rights. Globally, instruments such as Article 12 of the Universal Declaration of Human Rights and the General Data Protection Regulation (GDPR) affirm that privacy is a fundamental human right requiring legal protection. The strength of this research lies in its interdisciplinary approach, which bridges doctrinal analysis, religious law, and international frameworks, offering a comprehensive view that is often missing in previous studies. However, limitations remain: the study relies heavily on doctrinal and conceptual analysis without incorporating systematic trend data or empirical accounts from victims and law enforcement. While media reports highlight public concern, they cannot substitute for in-depth fieldwork or statistical analysis, and the rapid evolution of digital technologies risks outpacing current laws. Taken together, the findings affirm that doxing is a multidimensional violation demanding stronger legal frameworks, ethical safeguards, and further empirical research to ensure that privacy and dignity are effectively protected in Indonesia and beyond.

REFERENCES

'Audah, 'Abdul Qadir. *Al-Tasyrī' Al-Jinā'i Al-Islāmī; Muqāranan Bi Al-Qanūn Al-Wadh'Ī*. II. Cairo: Maktabah al-Taufiqiyah, 2013.

Abdillah, Muhammad Alwin, Nairazi, and Lina Agustina. "Copyright Infringement Crime in Islamic Criminal Law." *Legalite : Jurnal Perundang Undangan Dan Hukum Pidana Islam* 7, no. 2 (2022): 119–31. https://doi.org/10.32505/legalite.v7i2.5368.

Adhiwisaksana, Muhammad Faqih; Allagan, Tiurma Mangihut Pitta. "Competent Forum and Applicable Law in Personal Data Protection with a Foreign Element." *Indonesian Journal of International Law* 20, no. 3 (2023): 442. https://scholarhub.ui.ac.id/ijil/vol20/iss3/2/.

Alfitri, Alfitri. "Can the Requirements of Shariah Law Regarding Criminal Punishments Be Interpreted in a Way That Is Compatible With the Iccpr and Cat?" *Indonesian Journal of International Law* 7, no. 1 (2021). https://doi.org/10.17304/ijil.vol7.1.230.

Ali, Mahrus, and M. Arif Setiawan. "Penal Proportionality in Environmental Legislation of Indonesia." *Cogent Social Sciences* 8, no. 1 (2022). https://doi.org/10.1080/23311886.2021.2009167.

Amril, Dapit. "Etika Informasi Dalam Perspektif Al-Qur'an." *Alfuad: Jurnal Sosial Keagamaan* 1, no. 1 (2018): 54. https://doi.org/10.31958/jsk.v1i1.1157.

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.

Anindyajati, Titis. "Limitation of the Right To Freedom of Speech on the Indonesian Constitutional Court Consideration." *Indonesian Law Journal* 14, no. 1 (2021): 19–36. https://doi.org/10.33331/ilj.v14i1.45.

Ayu, Ananthia, Titis Anindyajati, and Abdul Ghoffar. "Perlindungan Hak Privasi Atas Data Diri Di Era Ekonomi Digital." *Pusat Penelitian Dan Pengkajian Perkara, Dan Pengelolaan Perpustakaan Kepaniteraan Dan Sekretariat Jenderal Mahkamah Konstitusi*. Mahkamah Agung, 2019. https://www.mkri.id/public/content/infoumum/penelitian/pdf/hasilpenelitian_123_Penelitian Hak Privasi dan Studi Komparasi.pdf.

Carrillo, Arturo J., and Matías Jackson. "Follow the Leader? A Comparative Law Study of the EU's General Data Protection Regulation's Impact in Latin America." *ICL Journal* 16, no. 2 (2022): 177–262. https://doi.org/10.1515/icl-2021-0037.

Chakim, M. Lutfi. "Freedom of Speech and the Role of Constitutional Courts: The Cases of Indonesia and South Korea." *Indonesia Law Review* 10, no. 2 (2020):

191–205. https://doi.org/10.15742/ilrev.v10n2.605.

Cheung, Anne. "Doxing and the Challenge to Legal Regulation: When Personal Data Become a Weapon." *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, 2021, 577–94. https://doi.org/10.1108/978-1-83982-848-520211041.

Corne, Thania Christy. "Legal Protection of Privacy Data Through Encryption Technology." *Lampung Journal of International Law* 1, no. 2 (2020): 63–70. https://doi.org/10.25041/lajil.v1i2.2027.

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.

Halif, Halif, Ainul Azizah, and Prisma Diyah Ratrini. "Regulating Doxing and Personal Data Dissemination in Indonesia." *Jurnal Kajian Pembaruan Hukum* 3, no. 1 (2023): 61. https://doi.org/10.19184/jkph.v3i1.33938.

Hamad, Ayah, and Bochen Jia. "How Virtual Reality Technology Has Changed Our Lives: An Overview of the Current and Potential Applications and Limitations." *International Journal of Environmental Research and Public Health* 19, no. 18 (2022). https://doi.org/10.3390/ijerph191811278.

Hasan, Hamzah. "Interview, May." Makassar, 2023.

Imran, Mohammad Fadil. "Preventing and Combating Cybercrime in Southeast Asia." *International Journal of Cyber Criminology* 17, no. 1 (2023): 223–33. https://doi.org/10.5281/zenodo.4766614.

Javaid, Mohd, Abid Haleem, Ravi Pratap Singh, Shahbaz Khan, and Ibrahim Haleem Khan. "Unlocking the Opportunities through ChatGPT Tool towards Ameliorating the Education System." *BenchCouncil Transactions on Benchmarks, Standards and Evaluations* 3, no. 2 (2023): 100115. https://doi.org/10.1016/j.tbench.2023.100115.

Kukul, Batuhan. "Personal Data and Personal Safety: Re-Examining the Limits of Public Data in the Context of Doxing." *International Data Privacy Law* 13, no. 3 (2023): 182–93. https://doi.org/10.1093/idpl/ipad011.

Mery, Hannah C. "The Dangers of Doxing and Swatting: Why Texas Should Criminalize These Malicious Forms of Cyberharassment." *St. Mary's Law Journal* 52, no. 3 (2021): 1–40. https://commons.stmarytx.edu/thestmaryslawjournal/vol52/iss3/8.

Miles, M.B., Huberman, A.M., Saldana, J. *Qualitative Data Analysis; A Methods Sourcebook*. 3rd ed. Los Angeles: SAGE Publications, 2014.

Muhammad, Sayid, and Rifqi Noval. "Doxing Phenomenon in Indonesia: Amid Waiting for Privacy Settings." *Budapest International Research and Critics Institute (BIRCI-Journal): Humanities and Social Sciences* 4, no. 3 (2021): 3636–44. https://doi.org/10.33258/birci.v4i3.2132 3636.

Musarrofa, Ita, and Holilur Rohman. "'Urf of Cyberspace: Solutions to the Problems

of Islamic Law in the Digital Age." *Al-Ahkam* 33, no. 1 (2023): 63–88. https://doi.org/10.21580/ahkam.2023.33.1.13236.

Naqvi, Syed Khurrum Husain, and Komal Batool. "A Comparative Analysis between General Data Protection Regulations and California Consumer Privacy Act." *Journal of Computer Science, Information Technology and Telecommunication Engineering* 4, no. 1 (2023): 326–32. https://doi.org/10.30596/jcositte.v4i1.13330.

Naro, Wahyuddin, Abdul Syatar, Muhammad Majdy Amiruddin, Islamul Haq, Achmad Abubakar, and Chaerul Risal. "Shariah Assessment Toward the Prosecution of Cybercrime in Indonesia." *International Journal of Criminology and Sociology* 9 (2020): 572–86. https://doi.org/https://doi.org/10.6000/1929-4409.2020.09.5.

Novianty, Suci Marini, Sri Wijayanti, and Jihad Muamar. "Ethical Discourse of Doxing in Indonesian Twitter Users." *Jurnal InterAct* 12, no. 1 (2023): 1–13. https://doi.org/10.25170/interact.v12i1.4134.

Nyoman, Ni, Juwita Arsawati, Dewi Bunga, Putu Eva, and Ditayani Antari. "Uploading Private Chat Screenshots on Social Media : How the Law Respond It ?" *Udayana Master Law Journal* 1, no. 1 (2023): 1–8. https://doi.org/10.24843/JMHU.2023.v12.i0.

Octav, Virliana. "Keterkaitan Doxing Terhadap Hak Atas Privasi Dalam Hak Asasi Manusia," 2022. https://kawanhukum.id/keterkaitan-doxing-terhadap-hak-atas-privasi-dalam-hak-asasi-manusia/.

Ortiz-Ospina, Esteban. "The Rise of Social Media." *Our World in Data*, 2019. https://ourworldindata.org/rise-of-social-media.

Paterson, Thomas. "Indonesian Cyberspace Expansion: A Double-Edged Sword." *Journal of Cyber Policy* 4, no. 2 (2019): 216–34. https://doi.org/10.1080/23738871.2019.1627476.

Pemerintah Republik Indonesia. "Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik." *Pemerintah Republik Indonesia*. Jakarta, 2016. https://web.kominfo.go.id/sites/default/files/users/4761/UU 19 Tahun 2016.pdf.

Salim, Arskal. "Contemporary Islamic Law in Indonesia : Sharia and Legal Pluralism," 6:232, 2015. https://ecommons.aku.edu/cgi/viewcontent.cgi?article=1007&context=uk_ismc_series_emc.

Setiawati, Diana, Hary Abdul Hakim, and Fahmi Adam Hasby Yoga. "Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore." *Indonesian Comparative Law Review* 2, no. 2 (2020): 2–9. https://doi.org/10.18196/iclr.2219.

Shahbaznezhad, Hamidreza, Rebecca Dolan, and Mona Rashidirad. "The Role of

Social Media Content Format and Platform in Users' Engagement Behavior." *Journal of Interactive Marketing* 53 (2021): 47–65. https://doi.org/10.1016/j.intmar.2020.05.001.

Sirait, Yohanes Hermanto. "General Data Protection Regulation (Gdpr) Dan Kedaulatan Negara Non-Uni Eropa." *Gorontalo Law Review* 2, no. 2 (2019): 60. https://doi.org/10.32662/golrev.v2i2.704.

Statista. "Social Media." statista.com, 2025. https://www.statista.com/topics/1164/social-networks/.

Supardin, Supardin, and Abdul Syatar. "Adultery Criminalization Spirit in Islamic Criminal Law: Alternatives in Indonesia's Positive Legal System Reform." *Samarah: Jurnal Hukum Keluarga Dan Hukum Islam* 5, no. 2 (2021): 913–27. https://doi.org/10.22373/sjhk.v5i2.9353.

Teguh Cahya Yudiana, Sinta Dewi Rosadi, Enni Soerjati Priowirjanto. "The Urgency of Doxing on Social Media Regulation and the Implementation of Right to Be Forgotten on Related Content for the Optimization of Data Privacy Protection in Indonesia." *Padjadjaran Jurnal Ilmu Hukum* 9, no. 1 (2022): 24–45. https://doi.org/10.22304/pjih.v9n1.a2.

Uweng Saripa, Intan, Hadibah Zachra Wadjo, and Judy Marria Saimima. "Perlindungan Hukum Pidana Terhadap Doxing Menurut Undang-Undang Informasi Dan Transaksi Elektronik." *Pattimura Law Study Review* 1 (2023): 168–79. https://doi.org/10.47268/palasrev.v1i1.10897.

Zein, Fara Dina. "Analisa Hukum Tindak Pidana Pencemaran Nama Baik Terhadap Joko Widodo Melalui Tabloid Obor Rakyat." *Jurnal Pembaharu Hukum* 1, no. 1 (2020): 61–75.