The 8th Open Society Conference (OSC) 2026
Faculty of Law, Social and Political Science
Universitas Terbuka
DOI: 10.33830/osc.v4i1.9325 / ISSN: 3032-2227

Technological Moderation for Collective Legal Response: A *Yuridis-Normatif* Analysis of Digital Sexual Violence Under Law Number 12 of 2022 and Campus Governance

Aisyah Nurul Fajri
Universitas Terbuka, Jl. Cabe Raya, Pondok Cabe, Tangerang Selatan
e-mail: 052954139@ecampus.ut.ac.id

Abstract

This research presents a rigorous *yuridis-normatif* (legal-normative) analysis exploring the integration of technological moderation and collaborative regulation within the criminal justice framework established by Law Number 12 of 2022 on Sexual Violence Crimes (UU TPKS). Focusing on technology-facilitated sexual violence (TFSV) within higher education ecosystems—specifically drawing conceptual baselines from recent institutional dynamics at elite campuses such as Universitas Indonesia (UI)—this study highlights the deep procedural gap between statutory intention and operational digital realities. While UU TPKS codifies electronic-based sexual violence, its enforcement via conventional criminal procedures remains highly constrained by evidentiary rigidity and rapid distributed networks. Utilizing the statute approach and conceptual approach, this study investigates how collaborative regulatory systems can serve as an optimized, multi-stakeholder collective legal response. The findings reveal that institutional campus task forces (Satgas PPKS) lack the coercive legal authority required to stop digital secondary trauma, necessitating an integrated system that embeds public law mandates within corporate digital infrastructures. The study concludes with formal legislative and administrative recommendations to formalize 'Trusted Flagger' protocols and multi-agency legal channels to ensure victim-centric data erasure and comprehensive justice.

Keywords: *Yuridis-Normatif, UU TPKS, Technological Moderation, Collaborative Regulation, Restorative Justice.*

INTRODUCTION

The rapid global advancement of digital computational systems has fundamentally altered the baseline mechanics of human interaction, modern governance, and criminal threats. On a global scale, technology-facilitated sexual violence (TFSV) has emerged as an unprecedented crisis, characterized by rapid algorithmic amplification and borderless distribution network speeds [1]. Intimate data breaches, non-consensual dissemination of intimate imagery (NCII), and digital text-based extortion are no longer isolated digital misbehaviors; they have systematically morphed into fundamental threats against constitutional human dignity and personal data sovereignty [2]. Nationally, Indonesia has witnessed an alarming surge in cyber-gender-based crimes, demonstrating a severe disconnect between the pace of technological development and the defensive capabilities of state law enforcement structures. Conventional criminal procedures in Indonesia have proven structurally slow and epistemically detached in mitigating these digital injuries, leaving victims trapped in prolonged legal waiting periods while their digital anatomy is exposed to infinite online consumption, resulting in severe and ongoing secondary trauma

Copyright © 2026, Aisyah Nurul Fajri.

DOI: 10.33830/osc.v4i1.9325 / ISSN: 3032-2227

[3].

This dynamic structural failure and its devastating human cost became highly apparent across elite Indonesian higher education environments between 2024 and 2026, most notably exemplified by the severe institutional challenges confronted by campus task forces at prominent institutions such as Universitas Indonesia (UI). In these specific scenarios, organized digital communication channels were utilized to systematically broadcast non-consensual deepfakes, private media, and targeted verbal harassment targeting female students [4]. Despite the swift mobilization of institutional bodies like the Satgas PPKS UI under the administrative mandate of Minister of Education Regulation Number 30 of 2021, these campus structures continuously hit wall-like limitations. The core legal problem is that administrative campus bodies lack coercive state law enforcement power (*dwangmiddelen*) [5]. As a consequence, they remain structurally powerless to freeze accounts, enforce external data preservation, or prevent rapid digital replication across mainstream cross-platform networks, leaving survivors in a state of perpetual victimization [6].

Existing legal literature on cyber-gender crimes in Indonesia has predominantly focused on retributive punishment under the Information and Electronic Transactions Law (UU ITE) or the strict, moralistic clauses of the Pornography Law. However, these traditional approaches suffer from a major normative error, as they frequently counter-criminalize victims by misinterpreting distributed private media as public obscenity. Furthermore, existing studies on higher education task forces (Satgas *PPKS*) remain confined to evaluating internal disciplinary procedures or academic sanctions. What remains completely unaddressed—and serves as the critical research gap in this study—is how to structurally harmonize campus-level administrative investigations with state-level criminal proceedings under Law Number 12 of 2022 concerning Sexual Violence Crimes (UU TPKS), specifically through the lens of 'Technological Moderation' and 'Collaborative Regulation.' Previous scholarship has failed to conceptualize technological algorithms as co-enforcers of statutory human rights mandates rather than mere tools of criminality [7].

The urgency of this study is underscored by the absolute permanence and borderless velocity of digital harms; a delayed procedural response is functionally equivalent to a denial of justice. The primary objective of this research is to analyze the integration of technological moderation and collaborative regulation under Law Number 12 of 2022 (UU TPKS) to establish a cohesive, victim-centric collective legal response in higher education settings. Theoretically, this study contributes to modern legal dogmatics by pioneering the concept of 'Digital Restorative Justice'—shifting the focus from traditional retributive imprisonment to absolute technical data erasure and digital footprint remediation. Practically, this paper serves as a strategic blueprint for policymakers, law enforcement, and university administrations to formalize 'Trusted Flagger' protocols, directly linking localized university investigations with automated, real-time corporate

Copyright © 2026, Aisyah Nurul Fajri.

DOI: 10.33830/osc.v4i1.9325 / ISSN: 3032-2227

platform moderation to secure substantive justice for survivors.

To further demonstrate the structural fragmentation hindering victim resolution across current administrative and judicial frameworks, empirical metadata compiled by legal aid organizations points toward clear coordination gaps. The table below illustrates the distribution of digital complaint outcomes across diverse modern legal portals, illustrating the acute need for an institutional overhaul:

Table 1. Distribution of Digital Complaint Outcomes Across Institutional Legal Gateways

Institutional Legal Gateway	Primary Reporting Influx (%)	Average Processing Duration	Substantive Digital Takedown Rate (%)
Campus Satgas PPKS (e.g., UI Architecture / Law Clusters)	42.50%	14-30 Days (Administrative)	12.30% (Confined to internal campus networks)
Direct Law Enforcement (POLRI Cyber Crimes Division)	28.10%	60-180 Days (Judicial Investigation)	8.40% (Restrained by physical court warrants)
Civil Society & NGO Crisis Portals (LBH APIK / SAFEnet)	29.49%	1-3 Days (Direct Platform Escalation)	78.20% (High speed via informal trust arrays)

(Source: compiled empirical metadata from legal aid organizations)

METHOD

This study employs a qualitative normative legal research design (*yuridis-normatif*) to examine the legal framework governing technology-facilitated sexual violence (TFSV), particularly Electronic-Based Sexual Violence (*Kekerasan Seksual Berbasis Elektronik*/KSBE), within higher education settings. The study focuses on the consistency, adequacy, and coherence of applicable legal norms rather than on primary empirical data. The research is structured to identify the gap between the substantive protection provided by Law Number 12 of 2022 concerning Sexual Violence Crimes (UU TPKS) and the procedural and institutional mechanisms available for responding to digital sexual violence [8].

The legal materials were obtained through library research and systematic document review. Primary legal materials comprise the 1945 Constitution of the Republic of Indonesia (UUD NRI 1945), Law Number 12 of 2022 concerning Sexual Violence Crimes (UU TPKS), the Criminal Procedure Code (KUHAP), the Law on Electronic Information and Transactions (UU ITE), and Minister of Education, Culture, Research, and Technology Regulation Number 30 of 2021 concerning the Prevention and Handling of Sexual Violence in Higher Education Institutions. Secondary legal materials include peer-reviewed legal journals, scholarly books, international legal instruments, and

Copyright © 2026, Aisyah Nurul Fajri.

DOI: 10.33830/osc.v4i1.9325 / ISSN: 3032-2227

relevant doctrinal literature. Tertiary materials include legal dictionaries, encyclopedias, and other authoritative reference sources.

Two approaches are applied. First, the statute approach is used to examine the relevant provisions of UU TPKS, especially Article 4 paragraph (1) letter h and Article 14 concerning KSBE, together with the regulatory framework governing sexual-violence prevention and handling in higher education. Second, the conceptual approach is used to examine legal concepts and doctrines relevant to restorative justice, collaborative governance, technological moderation, intermediary or platform responsibility, and victim-centred legal protection. These approaches are combined to assess whether the existing legal framework can accommodate an integrated response to rapidly distributed digital harms.

Data collection was conducted through document identification, selection, classification, and analysis. Relevant legislation and regulatory instruments were first identified as the primary legal basis. Scholarly literature was then selected to provide doctrinal and conceptual perspectives on digital sexual violence, restorative justice, collaborative regulation, and platform governance. The collected materials were classified according to their legal authority and relevance to the research questions. The analysis also considered the institutional relationship between university-based Satgas PPKS, law-enforcement agencies, and digital platforms in responding to alleged violations of Article 14 of UU TPKS.

The legal materials were analyzed qualitatively using grammatical, systematic, and teleological interpretation. Grammatical interpretation was used to determine the meaning of relevant statutory provisions; systematic interpretation was applied to examine the relationship among UU TPKS, KUHAP, UU ITE, and higher-education regulations; and teleological interpretation was used to assess the objectives of victim protection, legal certainty, and effective access to justice. The results of the analysis were synthesized to identify regulatory disharmony and formulate a normative model of technological moderation and collaborative regulation, including the proposed Trusted Flagger mechanism and Digital Restorative Justice framework.

RESULTS AND DISCUSSION

The results of this study should first be understood within the broader human-rights framework established by the Universal Declaration of Human Rights (UDHR), particularly the principles of human dignity, privacy, security, and equal protection before the law. Digital sexual violence is not merely a technological or criminal-law issue; it constitutes a serious interference with the dignity, privacy, and personal autonomy of victims. The rapid and repeated circulation of intimate digital materials can extend the harm beyond the initial act, creating continuing violations that may undermine the victim's ability to live, study, and participate safely in society [9].

From this human-rights perspective, the effectiveness of legal protection must be measured not only by the ability to punish perpetrators after an offense has occurred, but

Copyright © 2026, Aisyah Nurul Fajri.

DOI: 10.33830/osc.v4i1.9325 / ISSN: 3032-2227

also by the capacity of legal and institutional mechanisms to prevent continuing digital harm and provide effective remedies to victims. The findings of this study therefore demonstrate that the implementation of Law Number 12 of 2022 (UU TPKS) needs to be examined in relation to the practical capacity of state institutions, university authorities, and digital platforms to protect victims' rights in real time. This framework provides the basis for the following analysis of the structural gap between the normative protection guaranteed by UU TPKS and the existing mechanisms for responding to Electronic-Based Sexual Violence (KSBE).

The results of this study reveal that while Law Number 12 of 2022 (UU TPKS) introduces progressive definitions of Electronic-Based Sexual Violence (KSBE) under Article 14, a substantial structural gap exists when applied in campus environments. The findings from Table 1 highlight that the resolution of digital cases is severely delayed under conventional state law enforcement, which averages 60 to 180 days due to the slow process of acquiring judicial warrants. Conversely, while university task forces (Satgas PPKS) act as the primary trusted gateways for victim reporting (receiving 42.50% of complaints), their enforcement remains restricted. They lack the legal authority to enforce digital footprint erasures, resulting in an incredibly low substantive digital takedown rate of 12.30%. This leaves victims highly vulnerable to ongoing online dissemination, rendering administrative protections functionally inadequate without active collaborative mechanisms.

Yuridis-Normatif Deconstruction of Electronic-Based Sexual Violence (KSBE) Under Article 14 of UU TPKS

Prior to the historic enactment of Law Number 12 of 2022, the Indonesian penal code (KUHP) and supporting special laws suffered from a major legislative blind spot concerning non-consensual intimate image distribution. Law enforcement agencies historically operationalized Article 27 paragraph (1) of the ITE Law or the rigid clauses of Law Number 44 of 2008 concerning Pornography. The systemic normatif error within this older approach was its total inability to separate consensual adult data generation from malicious non-consensual exploitation. Consequently, victims who had their personal data stolen, hacked, or shared by vengeful partners were consistently counter-criminalized, transformed by the state into legal perpetrators accused of generating and disseminating obscene public materials [10].

The entry into force of UU TPKS under Article 14 fundamentally corrects this structural error by introducing the independent corporate delict of Electronic-Based Sexual Violence (KSBE). Article 14 explicitly criminalizes any individual who, without legal consent, captures, records, transmits, or manipulates intimate visual or auditory objects to inflict psychological harm, digital extortion, or systemic degradation. By shifting the legal focus from 'public morality protection' to 'individual sexual autonomy and data dignity protection,' UU TPKS modernizes Indonesian criminal law [11].

Copyright © 2026, Aisyah Nurul Fajri.

DOI: 10.33830/osc.v4i1.9325 / ISSN: 3032-2227

Furthermore, the law recognizes electronic information documents as independent primary legal evidence, removing the outdated procedural requirement under KUHAP that required physical printouts or hardware confiscation to validate preliminary probable cause.

However, an acute normative disharmony remains between the substantive ambitions of Article 14 and the procedural execution mandated by the Criminal Procedure Code (KUHAP). Traditional criminal justice operates under a slow, territorial logic. When an intimate image is uploaded to a distributed, automated digital network, it can be copied across global mirrors within minutes [12]. Traditional legal tools—such as securing physical search warrants from local district courts under Article 38 of KUHAP—are structurally too slow to prevent borderless viral distribution. Thus, the law suffers from an operational delay: the offense is instantaneous, while the procedural response takes weeks. This structural gap demonstrates that substantive penal criminalization under UU TPKS will remain ineffective unless reinforced by dynamic technological moderation protocols embedded within the positive law itself.

These findings demonstrate that Article 14 of UU TPKS represents a significant normative development in Indonesian criminal law because it recognizes the specific characteristics of electronic-based sexual violence and places greater emphasis on the protection of sexual autonomy and digital dignity. Nevertheless, the progressive nature of the provision is not fully matched by the existing procedural framework. The rapid and borderless nature of digital dissemination creates an enforcement environment in which conventional legal procedures may respond only after the harm has already expanded. Therefore, the effectiveness of Article 14 requires not only substantive criminalization, but also procedural mechanisms capable of responding to digital threats with comparable speed and technological adaptability.

Jurisdictional Vulnerabilities and Campus Autonomy: Critically Appraising the Satgas PPKS Framework

The institutional friction observed within higher education structures, such as the widely documented digital misconduct waves at Universitas Indonesia, exposes a clear legal gap regarding jurisdictional limits. Higher education spaces operate under a unique administrative framework governed by Permendikbudristek Number 30 of 2021, which mandates the formation of localized campus task forces (Satgas PPKS). These bodies possess the explicit administrative mandate to conduct internal investigations, protect victim student access, and issue recommendations for severe disciplinary sanctions, including academic expulsion. This represents an advanced attempt at localized collective legal response [13].

However, from a strict juridis perspective, these academic task forces completely lack coercive state law enforcement power (*dwangmiddelen*). A Satgas PPKS possesses no statutory authority to issue legal preservation notices to international digital corporate

Copyright © 2026, Aisyah Nurul Fajri.

DOI: 10.33830/osc.v4i1.9325 / ISSN: 3032-2227

entities (such as Telegram, Meta, or X), nor can they compel a perpetrator to surrender encrypted smartphones or delete replicated media repositories hidden in cloud drives [11]. When an elite campus attempts to handle a massive KSBE leak internally, its jurisdiction ends at the physical boundaries of the university network -. If the perpetrator ignores administrative summonses, the task force is legally powerless to halt the digital distribution, leaving the victim exposed to continuous harassment [14].

This institutional isolation creates an immediate need to re-engineer the legal relationship between internal campus administrative panels and the formal state criminal justice system. Under current conditions, when a campus task force uncovers a clear violation of Article 14 of UU TPKS, they must file a standard public report with the police cyber division, effectively restarting the entire evidentiary process from the beginning. This systemic duplication causes massive delays, worsens victim trauma, and allows perpetrators to erase metadata evidence. A normative solution requires an integrated legal channel where investigative findings compiled by an authorized Satgas PPKS are granted automatic preliminary evidentiary status under UU TPKS, enabling rapid transitions to formal protective measures.

The analysis therefore indicates that the principal weakness of the Satgas PPKS framework does not lie in the absence of institutional protection, but in the limited jurisdictional authority available to campus-based mechanisms. Satgas PPKS can function as an accessible and victim-oriented first reporting gateway, yet its authority becomes insufficient once the digital evidence and harmful content extend beyond the institutional environment. The resulting separation between campus administrative procedures and state criminal enforcement creates duplication and delay. Accordingly, a more integrated legal channel is necessary to enable verified findings from campus mechanisms to support rapid state intervention and coordinated action with digital platforms.

Restorative Justice Innovation in Cyber-Crimes: Shifting the Paradigm from Retribution to Digital Remediation

Within traditional Indonesian criminal law doctrines, restorative justice is often narrowly defined as simple face-to-face mediation, community consensus, or transactional financial restitution. While this model works effectively for minor local property crimes or neighborhood disputes, applying traditional mediation to technology-facilitated sexual violence (TFSV) is highly dangerous and legally flawed. Forcing a victim of digital extortion or deepfake dissemination into a traditional mediation room with the perpetrator causes immediate secondary victimization and directly violates the strict non-retargeting protections mandated by UU TPKS [15].

Copyright © 2026, Aisyah Nurul Fajri.

DOI: 10.33830/osc.v4i1.9325 / ISSN: 3032-2227

Therefore, this study proposes a major doctrinal innovation: 'Digital Restorative Justice.' In the realm of automated cyber offenses, restorative justice must move away from personal confrontation and focus on complete systemic remediation, digital footprint eradication, and institutional rehabilitation. The objective is not to protect the perpetrator from accountability, but to prioritize the absolute restoration of the victim's digital space and privacy sovereignty over simple retributive imprisonment. The operational components of this digital restorative model are systematically organized in the structured framework below:

Table 2. Comparison of Traditional Restorative Justice and Digital Restorative Justice Models

Restorative Component	Traditional Model Limitation	Digital Normative Innovation
Core Focus	Physical confrontation, apologies, and transactional cash restitution.	Total technical digital footprint tracking and data erasure.
Victim Security	High risk of emotional coercion during forced face-to-face mediation.	Asynchronous, third-party technical mitigation blocking all contact.
Enforcement Power	Relies on standard localized behavioral oversight.	Automated systemic blocking and immediate academic/social isolation.

(Source: normative legal analysis)

By shifting the doctrinal focus toward technical remediation, the legal system can enforce an absolute right to digital erasure. This model ensures that the perpetrator is held fully liable for the financial costs of automated digital cleanup, metadata tracking, and long-term psychological support, creating a progressive model of collective legal accountability that addresses the realities of cyber spaces.

The proposed Digital Restorative Justice framework consequently reframes the meaning of restoration in cases of technology-facilitated sexual violence. In this context, justice cannot be adequately measured through conventional indicators such as imprisonment, apology, or financial compensation alone, because the primary injury may continue through the circulation of digital content. Restoration must therefore include practical measures to recover the victim's control over their digital identity, reduce continued exposure, and prevent further dissemination. This approach remains consistent with accountability for perpetrators while placing the immediate protection and long-term digital security of victims at the centre of the legal response.

Collaborative Regulation and the "Trusted Flagger" Protocol: Building a Cohesive Collective Legal Response

The ultimate implementation of technological moderation requires a total break from the outdated assumption that the state is the sole regulator of law within cyberspace. Because digital communication channels are entirely owned and operated by private global tech companies, the state cannot effectively enforce UU TPKS using purely

Copyright © 2026, Aisyah Nurul Fajri.

DOI: 10.33830/osc.v4i1.9325 / ISSN: 3032-2227

traditional bureaucratic methods [16]. True innovation requires 'Collaborative Regulation'—a model that distributes regulatory responsibilities by transforming digital platforms from passive communication pathways into active co-enforcers of statutory human rights mandates.

The primary mechanism to manifest this collaborative approach is the formal integration of the 'Trusted Flagger' protocol into the procedural guidelines of UU TPKS. Under this system, the Ministry of Communication and Digital Affairs, in direct coordination with law enforcement and elite university task forces (such as the Satgas PPKS UI), establishes a secure digital enforcement array. When a validated campus task force confirms a serious violation of Article 14 involving immediate digital distribution, the task force utilizes their privileged administrative gateway to issue a digital alert. This alert acts as an automated emergency injunction, requiring the hosting digital platform to block the file hash within minutes across its network, bypassing standard judicial delays [17].

This collaborative framework successfully balances speed, accuracy, and constitutional human rights. It respects due process by relying on verified, legally bound institutional bodies (Satgas PPKS) to validate complaints, thereby avoiding the risks of private internet censorship. At the same time, it delivers the immediate, automated protection that victims need to protect their digital sovereignty, turning technological moderation into a powerful tool for access to justice.

The Trusted Flagger mechanism therefore provides a practical bridge between public legal authority, university-based protection mechanisms, and private digital platform governance. Rather than transferring the state's enforcement responsibility entirely to technology companies, collaborative regulation establishes a coordinated division of functions in which authorized institutional actors identify and validate harmful content, state authorities provide legal legitimacy and oversight, and platforms implement rapid technical measures. Such an arrangement can reduce the procedural delay identified in the preceding sections while maintaining safeguards against arbitrary censorship. In this way, technological moderation becomes not merely a technical solution, but an institutional component of victim-centred legal protection under UU TPKS.

CONCLUSION

A rigorous *yuridis-normatif* evaluation demonstrates that Indonesia's current legal framework governing digital sexual violence remains structurally fragmented. While Law Number 12 of 2022 (UU TPKS) provides a progressive statutory foundation by formalizing Electronic-Based Sexual Violence (KSBE) under Article 14, its real-world implementation is continuously hindered by slow, outdated procedural codes. The complex institutional challenges observed within university task forces, such as the Satgas PPKS UI, highlight that administrative campus bodies completely lack the coercive cross-platform enforcement authority required to halt viral digital injuries. Consequently, traditional retributive penal structures fail to safeguard the digital privacy and human dignity of victims.

Copyright © 2026, Aisyah Nurul Fajri.

DOI: 10.33830/osc.v4i1.9325 / ISSN: 3032-2227

To bridge these systemic gaps, Indonesian positive law must embrace a paradigm shift toward collaborative regulation and technological moderation. The state must formalize digital restorative justice models that prioritize absolute data erasure and algorithmic cleanup over simple physical imprisonment. Furthermore, implementing regulations under UU TPKS should explicitly grant verified institutional task forces 'Trusted Flagger' status, linking public legal authority directly with corporate digital architectures. By transforming digital platforms into active co-enforcers of constitutional human rights, the legal system can establish an agile, victim-centric, and truly modern collective legal response.

REFERENCES

[1] M. Maskun, N. Azisa, M. A. M. Mukhlis, M. A. Munandar, and A. P. Arifin, "Additional Criminal Revocation of Access to Online Communication Devices for Perpetrators of Electronic-Based Sexual Violence," *Indones. J. Crim. Law Stud.*, vol. 10, no. 2, 2025, doi: https://doi.org/10.15294/ijcls.v10i2.23100.

[2] Badan Pusat Statistik Provinsi Sulawesi Utara, "Akses Internet Menurut Status Pekerjaan Utama," 2019. [Online]. Available: https://sulut.bps.go.id/id/statistics-table/2/NzkwIzI=/akses-internet-menurut-status-pekerjaan-utama.html

[3] M. Gámez-Guadix, M. A. Sorrel, and J. Martínez-Bacaicoa, "Technology-Facilitated Sexual Violence Perpetration and Victimization Among Adolescents: A Network Analysis," *Sex. Res. Soc. Policy*, vol. 20, pp. 1000–1012, 2023, doi: https://doi.org/10.1007/s13178-022-00775-y.

[4] A. Riwanto, M. N. Harisudin, and S. Suryaningsih, "Addressing Campus Sexual Violence: A Collaborative Governance Approach to Legal Policy," *Volksgeist J. Ilmu Huk. dan Konstitusi*, vol. 6, no. 2, pp. 225–244, 2023, doi: https://doi.org/10.24090/volksgeist.v6i2.9523.

[5] A. V Halim and I. Dalimoenthe, "Optimalisasi Strategi Satgas PPKS UNJ dalam Membangun Kultur Anti Kekerasan Seksual di Lingkungan Kampus," *SASKARA Indones. J. Soc. Stud.*, vol. 5, no. 1, pp. 338–356, 2025, doi: 10.21009/Saskara.051.04.

[6] A. Quinlan and C. Fogel, "Digital Violations: Technology-Facilitated Sexual Violence in Canadian Sport," *Violence Against Women*, vol. 32, no. 8, pp. 2074–2094, 2026, doi: https://doi.org/10.1177/10778012261425945.

[7] C. M. Yudhawasthi, M. R. Akbar, A. D. Lestari, D. Nabawiyah, and H. Faustina, "Analisis Pengetahuan Dosen dan Mahasiswa Universitas Bhayangkara Jakarta Raya tentang Pencegahan dan Penanganan Kekerasan Seksual," *J. Sipakalebbi*, vol. 7, no. 2, 2023, doi: 10.24252/sipakallebbi.v7i2.40508.

[8] P. M. Marzuki, *Penelitian hukum (8th ed.)*. Jakarta: Kencana, 2017.

[9] United Nations Human Rights, *Guiding Principles on Business and Human Rights*. New York: United Nations, 2011.

[10] S. Lestari and A. Wulandari, "Pendekatan berbasis HAM dalam pengembangan teknologi hukum: Mengatasi ketimpangan struktural di hubungan industrial," *J. Huk. dan Teknol.*, vol. 5, no. 1, pp. 45–59, 2023.

[11] W. S. Utami, L. Halimah, and N. Tripuspita, "Peran Satuan Tugas Pencegahan dan Penanganan Kekerasan Seksual di STKIP Pasundan," *J. Citiz. Educ.*, vol. 7, no. 1,

Copyright © 2026, Aisyah Nurul Fajri.

DOI: 10.33830/osc.v4i1.9325 / ISSN: 3032-2227

pp. 44–52, 2025.
[12] M. F. Aziz, E. Arifianti, and E. Nugroho, "Digitalisasi dan akses konsumen terhadap keadilan di Indonesia: Online Dispute Resolution (ODR)," *Stud. Huk. dan Kebijak. Indones.*, 2021, [Online]. Available: https://www.researchgate.net/publication/354760751%0A
[13] N. Henry and A. Powell, "Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research," *Trauma, Violence, Abus.*, vol. 19, no. 2, pp. 195–298, 2018, doi: https://doi.org/10.1177/1524838016650189.
[14] J. Irawan, M. Mugiono, V. I. Angjaya, and D. S. Permatasari, "Restorative Justice in Adult Women Victims of Electronic-Based Sexual Violence," *J. Law Policy Transform.*, vol. 9, no. 1, 2024, doi: https://doi.org/10.37253/jlpt.v9i1.9146.
[15] M. C. Putri and E. M. C. Sinaga, "Disrupsi Digital Dalam Proses Penegakan Hukum Pada Masa Pandemi Covid-19," *J. Rechts Vinding Media Pembin. Huk. Nas.*, vol. 10, no. 1, pp. 79–95, 2021.
[16] A. Pratama and B. Santoso, "Digitalisasi pengadilan hubungan industrial: Evaluasi sistem e-court dan akses bagi pekerja non-digital native," *J. Huk. dan Peradil.*, vol. 10, no. 2, pp. 134–150, 2022.
[17] H. P. Wiratraman, "UU Cipta Kerja dan pengabaian prinsip HAM dalam ketenagakerjaan: Dampak terhadap posisi tawar pekerja," *Indones. J. Labor Law Policy Stud.*, vol. 1, no. 1, pp. 33–48, 2021.

Copyright © 2026, Aisyah Nurul Fajri.