Strata Law Review, 2025, Vol. 4, No. 1, 22–34
E-ISSN: 2986-8114 | P-ISSN: 2987-3185
doi: 10.59631/slr.v4i1.494
Advance Access publication March 31, 2026

STRATA LAW REVIEW
journals.stratapersada.com/index.php/slr

Criminal Offences of Covert Dissemination of Obscene Content from the Perspective of Equality Before the Law

Irvan Abdillah[a*], Adistia Lulu Apriana[b]

[a*]*Sekolah Tinggi Ilmu Hukum Sultan Adam, Indonesia, irvanabdillah011@gmail.com*
[b]*Sekolah Tinggi Ilmu Hukum Sultan Adam, Indonesia, adistialuluapriana1717@gmail.com*

Article History	Submitted	Revised	Accepted
	2026-01-25	2026-02-23 & 2025-03-02	2025-03-10

Abstract

The rapid expansion of digital technology has transformed personal data into a central object of control and vulnerability, giving rise to data-driven crimes such as the covert dissemination of obscene content. This study examines such conduct within the framework of Indonesia's Personal Data Protection Law (Law No. 27 of 2022) from the perspective of equality before the law. Employing a normative legal research method based on statutory and systematic approaches, this research analyzes primary, secondary, and tertiary legal materials through systematic, historical, and hermeneutical interpretation. The findings demonstrate that non-consensual recording and dissemination of intimate content constitute not merely morality-based offenses but serious violations of personal data protection rights. Although Indonesia's legal framework provides multiple avenues for criminal liability and victim protection, enforcement remains fragmented, with a predominant reliance on morality provisions that marginalizes the data protection dimension of the offense. Structural challenges—including limited legal awareness, technological barriers in digital evidence collection, cross-border dissemination, and inconsistent sanctioning practices—further weaken substantive equality. The study reveals a persistent gap between formal legal guarantees and their practical realization, underscoring the need to integrate personal data protection principles more coherently into the criminal justice system to ensure non-discriminatory and effective legal protection in the digital era.

Keywords: Covert dissemination of obscene content, criminal offence, equality before the law, personal data protection.

Doi: 10.59631/slr.v4i1.494

INTRODUCTION

The development of digital technology and information systems has transformed patterns of social interaction, communication, and information distribution in modern society.[1] Digitalization not only expands access to information but also reshapes power relations concerning the production, control, and dissemination of personal data. Despite its benefits, technological advancement has also generated new forms of digital-based crime,[2] including the covert dissemination of obscene content without the consent of the data subject.[3] This phenomenon reflects a shift in the nature of criminality from conventional forms to data-driven crimes that exploit vulnerabilities in digital systems and deficiencies in privacy literacy. Such conduct not only violates moral norms but also constitutes a serious infringement of the right to personal data protection as an integral component of human rights.

The covert dissemination of obscene content generally involves the recording, possession, storage, and distribution of sensitive personal data, such as images or videos depicting an individual's body or private activities. Within the framework of data protection law, such actions qualify as unlawful processing of personal data in the absence of legitimate grounds and explicit consent from the data subject. Victims are placed in a highly vulnerable position, as control over their personal data is effectively transferred to the perpetrator. The resulting harm is not merely juridical in nature but also social and psychological, including loss of dignity, security, and professional reputation, as well as the risk of prolonged discrimination. Such harm is often irreversible due to the digital environment, which enables rapid reproduction and cross-border dissemination.

Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) was enacted as a legal instrument to guarantee every individual's right to the protection of their personal data.[4] The PDP Law affirms that all data subjects possess equal rights to the protection, control, and security of their personal data, including specific categories of sensitive data.[5] Normatively, the PDP Law incorporates fundamental principles of data protection, such as lawful processing, consent, purpose limitation, and accountability, which constitute the foundation of modern data protection regimes.[6] Nevertheless, in the enforcement of criminal offenses involving the covert dissemination of obscene content, challenges persist in ensuring the fair and consistent application of the PDP Law, particularly where victims belong to vulnerable groups or occupy weaker social positions. This discrepancy between normative guarantees and practical

---

[1] Azzahra Nayla Aqila and Eva Muti'ah, "The Impact Of Social Media On Changes In Social Interaction Patterns In Cities," *Bina Bangsa International Journal of Business and Management* 5, no. 1 (April 30, 2025): 304–16, https://doi.org/10.46306/bbijbm.v5i1.127.

[2] Ujang Hibar, Enjum Jumhana, and Suherman Arifin, "Cybercrime Digital Crime How Technology Is Utilized for Crime," *Journal of Law Science* 7, no. 1 (January 31, 2025): 1–9, https://doi.org/10.35335/jls.v7i1.5848.

[3] Muhamad Rizal Satrio Nugroho, Muhammad Nurcholis Alhadi, and Ikhwanul Muslim, "The Crime of Spreading Pornographic Content in Digital Media," *TATOHI: Jurnal Ilmu Hukum* 5, no. 1 (March 31, 2025): 1, https://doi.org/10.47268/tatohi.v5i1.2890.

[4] Zaid, *Perlindungan Privasi Dan Data Pribadi: Sebuah Tinjauan Pengantar* (Malang: Setara Press, 2024).

[5] Zaid; Syahreza Fachran, Sinta Dewi Rosadi, and Prita Amalia, "Protection Of Data Subject Rights In The Transfer Of Personal Data Between Data Controllers In Indonesia: A Comparative Analysis Of The PDP Law And The EU GDPR," *Awang Long Law Review* 8, no. 2 (January 16, 2026): 518–29, https://doi.org/10.56301/awl.v8i2.1827.

[6] Zaid, *Perlindungan Privasi Dan Data Pribadi: Sebuah Tinjauan Pengantar*.

implementation raises concerns regarding the effectiveness of legal protection in ensuring equal access to justice.

From the perspective of equality before the law, all individuals are equal before the law and are entitled to legal protection without discrimination.[7] This principle requires the state to ensure equal treatment of all parties within legal proceedings, whether victims or perpetrators, regardless of social background, gender, economic status, or other personal attributes. Theoretically, equality before the law demands not only formal equality but also substantive equality, which takes into account the factual circumstances of the parties in order to prevent structural injustice.[8] In practice, victims of covert dissemination of obscene content frequently encounter victim blaming, challenges to their credibility, and even the risk of counter-criminalization, while perpetrators are not always prosecuted proportionally. This phenomenon indicates the presence of structural bias within law enforcement processes that may undermine the principle of non-discrimination.

Such imbalance in legal treatment reveals a gap between the normative framework guaranteeing personal data protection and its implementation in practice. If the principle of equality before the law is not consistently operationalized, personal data protection risks becoming merely a declarative norm devoid of effective protective force. This situation calls for a critical evaluation of regulatory design, law enforcement mechanisms, and the paradigmatic approach of law enforcement authorities toward victims of digital-based crimes. Accordingly, the issue extends beyond violations of morality and implicates the integrity of the criminal justice system in ensuring equal justice.

From an academic perspective, previous studies generally follow two principal strands. First, research that situates the dissemination of obscene content solely within the domain of cybercrime or morality (pornography) offenses[9] without thoroughly examining the personal data protection regime as a basis for criminal liability. Second, studies that address such conduct under information and electronic transaction laws,[10] without specifically engaging with the newly enacted PDP Law. Consequently, scholarly analysis of the PDP Law remains limited, particularly in its application to the issue of covert dissemination of obscene content through the lens of equality before the law. A significant academic space therefore remains underexplored, especially in assessing the extent to which the principle of equality before the law has been genuinely internalized in the enforcement of the PDP Law in cases involving the non-consensual distribution of intimate content.

---

[7] Malia Dwi Putri et al., "Disability Law and Human Rights: Theory and Policy," *Disability & Society* 40, no. 5 (May 4, 2025): 1435–37, https://doi.org/10.1080/09687599.2024.2411148.

[8] Vibeke Blaker Strand and Ingunn Ikdahl, "Responding to Disadvantage and Inequality through Law," *Oslo Law Review* 4, no. 3 (December 15, 2017): 124–32, https://doi.org/10.18261/issn.2387-3299-2017-03-01.

[9] Harly Clifford J Salmon, Denny Latumaerissa, and Judy Marria Saimima, "Penegakan Hukum Terhadap Pelaku Penyebaran Konten Asusila," *Risalah Hukum* 21, no. 1 (June 30, 2025): 20–31, https://doi.org/10.30872/risalah.v21.i1.1593.

[10] Ibrahim Fikma Edrisy, "Tinjauan Yuridis Terhadap Tindak Pidana Asusila Dalam Undang-Undang ITE (Studi Putusan Nomor 262/Pid.Sus/2021/PN Kbu)," *Jurnal Hukum Legalita* 5, no. 1 (July 31, 2023): 1–13, https://doi.org/10.47637/legalita.v5i1.730; Muhammad Rizki, Irawan Harahap, and Rudi Pardede, "Penerapan Hukum Terhadap Pelaku Penyebaran Konten Pornografi," *Collegium Studiosum Journal* 8, no. 1 (June 30, 2025): 265–76, https://doi.org/10.56301/csj.v8i1.1710.

Based on the foregoing, an in-depth examination of the criminal offense of covert dissemination of obscene content within the framework of the Personal Data Protection Law, analyzed through the perspective of equality before the law, is imperative. This study seeks to assess the extent to which the principle of equality before the law is internalized in both normative provisions and enforcement practices concerning crimes involving sensitive personal data. It is expected that this research will provide both conceptual and normative contributions toward strengthening the fair and non-discriminatory implementation of the PDP Law, while promoting equal legal protection for all citizens in the context of digital crime.

METHOD

This research employs a normative method. The normative method aligns with library research, involving the collection of data from relevant literature. The approach used in normative legal research encompasses several approaches, including the statutory approach and the legal systematic approach. The data utilized will be sourced from primary, secondary, and tertiary legal materials, as defined by experts. Data collection techniques will be carried out through library research, focusing on relevant literature to address the research questions. Data analysis will employ systematic and historical interpretation, as well as hermeneutical methods to understand the legal context. The stages of this research will not be discussed separately, considering its focus on library research. This research is planned to be written with a clear and systematic structure.

RESULT AND DISCUSSION

Implementation of Personal Data Protection in Cases of the Covert Dissemination of Obscene Content under the Personal Data Protection Law

The covert dissemination of obscene content constitutes a severe violation that harms victims not only by undermining their dignity and reputation but also by inflicting profound social and psychological consequences. This criminal act typically involves the unauthorized recording, possession, control, and distribution of personal data in the form of images or videos, directly infringing upon the fundamental right to privacy. In this context, the protection of victims' personal data becomes legally and constitutionally significant, particularly following the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), which aims to guarantee the protection of personal data as an integral component of individual rights in Indonesia.[11]

Under the PDP Law, personal data is defined as any information capable of identifying an individual,[12] including data relating to personal aspects such as photographs, videos, audio

[11] Zaid, *Perlindungan Privasi Dan Data Pribadi: Sebuah Tinjauan Pengantar*; Awaluddin, "The Existence of Law Number 27 Of 2022 Concerning Personal Data Protection in Protecting Citizens' Privacy Rights," *Indonesian Research Journal in Legal Studies* 4, no. 2 (September 30, 2025): 54–60, https://doi.org/10.31934/irjils.v4i2.8717.

[12] Nadezhda Purtova, "The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law," *Law, Innovation and Technology* 10, no. 1 (January 2, 2018): 40–81, https://doi.org/10.1080/17579961.2018.1452176.

recordings, and other identifying information.[13] In cases involving the covert dissemination of obscene content, the unauthorized use and unlawful distribution of intimate images or videos clearly violate the principles set forth in the PDP Law, which mandates that personal data processing must be conducted lawfully, transparently, for legitimate purposes, and based on the explicit consent of the data subject. Consequently, non-consensual dissemination of intimate content should not merely be viewed as a morality offense but as a specific violation of personal data protection rights.

Criminal Sanctions in Cases of the Covert Dissemination of Obscene Content

From the perspective of substantive criminal law, the act of recording and distributing sexual content without consent is prohibited under multiple statutory regimes.[14] Article 4 paragraph (1) of the Pornography Law prohibits any person from producing, reproducing, duplicating, distributing, broadcasting, importing, exporting, offering, trading, renting, or providing pornography that explicitly contains sexual intercourse (including deviant intercourse), sexual violence, masturbation, nudity or depictions suggestive of nudity, genitalia, or child pornography. Consent plays a pivotal role in determining whether an act constitutes a violation under this provision, as the absence of consent transforms private documentation into unlawful production and dissemination of pornographic material.

Pursuant to Article 29 of the Pornography Law, individuals who commit such acts are subject to imprisonment ranging from six months to twelve years and/or fines ranging from IDR 250,000,000 to IDR 6,000,000,000.

Furthermore, where the dissemination occurs through electronic media or the internet, perpetrators may also be prosecuted under Article 27 paragraph (1) of the Electronic Information and Transactions Law (as amended by Law No. 19 of 2016), which criminalizes the intentional and unauthorized distribution or transmission of electronic information containing content that violates decency. The maximum penalty under this provision is six years of imprisonment and/or a fine of up to IDR 1,000,000,000.

In addition, Law Number 12 of 2022 on Sexual Violence Crimes (TPKS Law) strengthens victim protection by explicitly criminalizing the covert recording of sexual activities. Article 14 paragraph (1)(a) provides for a maximum penalty of four years' imprisonment and/or a fine of up to IDR 200,000,000. This provision demonstrates legislative recognition that non-consensual recording itself constitutes a distinct form of sexual violence.

The coexistence of these legal regimes indicates that the covert dissemination of obscene content may trigger cumulative or alternative criminal liability.[15] However, the application of

[13] Ibrahim Muhammad Isya and Susilo Wardani, "Analisis Yuridis Perlindungan Privasi Terhadap Pengambilan Foto Tanpa Izin Di Era Digital," *Jurnal Penelitian Serambi Hukum* 18, no. 02 (June 25, 2025): 228–38, https://doi.org/10.59582/SH.V18I02.1332.

[14] Ratu Indra Kasih Pratiwi, "Understanding Criminal Liability for Pornography in Cyberspace Based on the Pattern of Distribution," *Damhil Law Journal* 4, no. 1 (May 30, 2024): 82, https://doi.org/10.56591/dlj.v4i1.2511.

[15] Azizul Hakiki et al., "Digital Content Crimes In Criminal Liability," *Journal of Multidisciplinary Research*, November 15, 2024, 36–44, https://doi.org/10.56943/jmr.v3i3.651.

these provisions in practice often prioritizes morality-based offenses over personal data protection violations, thereby marginalizing the data protection dimension of the offense.

Measures for Implementing Personal Data Protection in Cases of Criminal Offenses Involving the Dissemination of Obscene Content

1. Recognition and Protection of the Right to Privacy

The PDP Law recognizes privacy as a fundamental right encompassing the protection of sensitive personal information.[16] Intimate images and videos fall within the category of highly sensitive personal data due to their direct connection to bodily autonomy and personal dignity. Accordingly, any non-consensual dissemination constitutes a serious breach of privacy and must be treated as such within criminal proceedings. Effective implementation requires formal acknowledgment that the core harm lies not only in moral transgression but in the unlawful violation of personal data rights.

2. Lawful and Ethical Processing of Personal Data

The PDP Law establishes that personal data may only be processed upon explicit and lawful consent from the data subject.[17] In cases of covert dissemination, both the recording and subsequent distribution lack legal basis and therefore contravene fundamental data protection principles, including lawfulness, purpose limitation, and accountability. The state bears the obligation to ensure that individuals and digital intermediaries engaging in data processing are held legally accountable for violations.

3. Strengthening Victim Protection in Criminal Proceedings

Victims of non-consensual dissemination of intimate content frequently occupy a vulnerable position, often facing stigma, secondary victimization, and social exclusion.[18] The PDP Law provides mechanisms to safeguard the confidentiality of victims' identities and prevent further exposure. In criminal proceedings, this protection must extend to investigative stages, court hearings, and media reporting. Ensuring anonymity and preventing re-victimization are essential components of substantive equality before the law.

4. Responsibility of Digital Platforms and Electronic System Providers

---

[16] Fachran, Rosadi, and Amalia, "PROTECTION OF DATA SUBJECT RIGHTS IN THE TRANSFER OF PERSONAL DATA BETWEEN DATA CONTROLLERS IN INDONESIA: A COMPARATIVE ANALYSIS OF THE PDP LAW AND THE EU GDPR"; Vicky Ibrahim, Yeti Hasan, and Parmin Ishak, "Personal Data Protection Policies and Their Impact on Victims of Cybercrime," *Jurnal Ilmu Hukum Kyadiren* 6, no. 2 (December 10, 2024): 13–25, https://doi.org/10.46924/jihk.v6i2.225.

[17] Dody Novizar Mardyansyah et al., "Harmonization of Personal Data Protection Principles With Electronic Justice Systems In Indonesia," *Yuridika* 40, no. 3 (September 30, 2025): 343–68, https://doi.org/10.20473/ydk.v40i3.74179.

[18] Yulia Martha Prayudati, Wessy Trisna, and Yati Sharfina Desiandri, "Analysis Of The Threat Of The Spread Of Intimate Content Non Consensual In Violence Gender Based Online," *SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan* 4, no. 8 (July 5, 2025): 1911–24, https://doi.org/10.54443/sibatik.v4i8.2833.

The PDP Law imposes obligations on electronic system operators and digital platforms that process personal data.[19] Social media platforms and content-sharing applications must implement adequate security measures to prevent unauthorized dissemination of personal data. Where platforms fail to act upon reports or negligently allow the circulation of intimate content, administrative and potentially criminal sanctions may be imposed. This regulatory framework underscores the shared responsibility between individual perpetrators and digital intermediaries.

5. Dispute Resolution and Victim Remedies

The PDP Law provides avenues for victims to seek remedies, including claims for compensation and requests for content removal or access blocking. Victims may initiate civil proceedings against electronic system operators or other responsible parties and demand the erasure of unlawfully disseminated content. The availability of compensation mechanisms reinforces restorative justice principles within the broader framework of criminal accountability.

Challenges in the Implementation of Personal Data Protection in Cases of Covert Dissemination of Obscene Content

The findings of this study indicate that the implementation of personal data protection in cases involving the covert dissemination of obscene content continues to face substantial structural and normative challenges. One of the primary obstacles lies in the limited level of legal awareness among victims regarding their rights as data subjects under the Personal Data Protection Law (PDP Law).[20] Many victims remain unaware that non-consensual recording, possession, and distribution of intimate content constitute violations of their legally protected personal data rights. As a consequence, a significant number of cases go unreported, and victims often fail to exercise available legal remedies, including the right to file complaints, request content removal, or seek restitution. This lack of awareness not only weakens access to justice but also perpetuates a culture of silence that indirectly benefits perpetrators.

In addition to the issue of legal awareness, law enforcement mechanisms encounter considerable evidentiary and technical difficulties. The digital nature of the offense allows content to be disseminated rapidly across multiple platforms, frequently involving anonymous accounts, encrypted communications, and cross-border data flows. These factors complicate the identification of perpetrators and the collection of admissible digital evidence. Moreover, the process of requesting data disclosure from digital platforms and securing the removal of unlawful content is often procedurally complex and time-sensitive. Delays in response may result in irreversible harm to victims, given the replicable and persistent character of digital content.

[19] Valentina Ancillia Simbolon and Vishnu Juwono, "Comparative Review of Personal Data Protection Policy in Indonesia and The European Union General Data Protection Regulation," *Publik (Jurnal Ilmu Administrasi)* 11, no. 2 (December 30, 2022): 178–90, https://doi.org/10.31314/pjia.11.2.178-190.2022.

[20] Friska Yulanda Pratiwi and Fajar Rachmad Dwi Miarsa, "Urgensi Edukasi Publik Dalam Menangkal Penyalahgunaan Data Pribadi," *RIGGS: Journal of Artificial Intelligence and Digital Business* 4, no. 2 (May 25, 2025): 1342–49, https://doi.org/10.31004/riggs.v4i2.672.

Doi: 10.59631/slr.v4i1.494

Consequently, enforcement challenges are not merely procedural but are inherently linked to the technological architecture of digital platforms.

Another significant concern relates to the proportionality and consistency of sanctions imposed on perpetrators. Although the PDP Law provides criminal sanctions for unlawful processing and dissemination of personal data, in practice, penalties imposed in cases of covert dissemination of obscene content do not always reflect the gravity of the harm inflicted upon victims. In some instances, prosecutorial strategies prioritize morality-based offenses without fully integrating the dimension of personal data violations, thereby narrowing the scope of accountability. This approach risks producing lenient sentencing outcomes that fail to generate adequate deterrent effects. The absence of consistent sanctioning standards undermines both the preventive and retributive functions of criminal law in the context of data-driven offenses.

From the perspective of equality before the law, these implementation challenges reveal a deeper structural issue. Victims—particularly those from socially vulnerable groups—may encounter secondary victimization during investigative and judicial processes, including skepticism toward their testimony, exposure of their private information, or implicit moral judgment. Such treatment creates a disparity between the formal guarantee of equal protection and its substantive realization in practice. Equality before the law requires not only uniform application of statutory provisions but also sensitivity to power imbalances that may impede victims' effective participation in the justice system. Therefore, the enforcement of the PDP Law must be assessed not solely in terms of procedural compliance but also in terms of its capacity to ensure substantive equality.

The effective implementation of personal data protection in cases of covert dissemination of obscene content thus demands a multidimensional approach.[21] Strengthening legal awareness through public education is essential to empower victims to assert their rights. Simultaneously, institutional capacity-building for law enforcement authorities in digital forensic investigation and cross-border cooperation is necessary to address technical barriers. Furthermore, structured collaboration between law enforcement agencies and digital platform providers should be institutionalized to facilitate rapid content removal, evidence preservation, and perpetrator identification. Without coordinated regulatory, institutional, and societal efforts, the promise of personal data protection under the PDP Law risks remaining largely declaratory rather than operational.

Ultimately, ensuring optimal protection for victims requires improvements not only in enforcement mechanisms but also in guaranteeing equal access to justice and non-discriminatory treatment throughout the criminal process. The integration of personal data protection principles into the broader criminal justice framework represents a crucial step toward aligning normative guarantees with practical outcomes. In this regard, the realization of equality before the law in digital crime cases becomes a measurable indicator of the maturity and integrity of the legal system in responding to contemporary technological challenges.

[21] Mary E. Vicks, "An Examination of Internet Filtering and Safety Policy Trends and Issues in South Carolina 's K-12 Public Schools" (Nova Southeastern University, 2013).

The Principle of Equality Before the Law in the Enforcement of Criminal Offenses Involving the Covert Dissemination of Obscene Content, Particularly in the Protection of Victims' Personal Data Rights

The principle of equality before the law constitutes one of the foundational pillars of a constitutional legal order, ensuring that every individual—irrespective of social, economic, political, or other status—is treated equally within the legal process.[22] This principle requires law enforcement authorities to guarantee equal protection of rights and to apply the law impartially and without discrimination. In the context of criminal offenses involving the covert dissemination of obscene content, which frequently entails violations of personal data rights, the operationalization of equality before the law assumes particular urgency. Such offenses not only implicate morality-based criminal provisions but also fundamentally infringe upon the victim's right to privacy and control over sensitive personal data. Accordingly, the enforcement of criminal law in this domain must reflect not merely formal equality, but also substantive equality that effectively safeguards the victim's dignity and personal autonomy.

In cases of covert dissemination of obscene content, the victim's right to privacy—especially in relation to intimate images or videos constituting sensitive personal data—represents the most vulnerable legal interest. The unauthorized recording, possession, and distribution of such content transfer control over personal data from the victim to the perpetrator, thereby producing profound legal, social, and psychological harm. The principle of equality before the law mandates that victims' privacy rights be afforded protection equal to, and not subordinate to, the procedural rights guaranteed to defendants. Throughout the stages of investigation, prosecution, and adjudication, the confidentiality of the victim's personal data must be strictly maintained. Judicial processes must be conducted in a manner that preserves the victim's dignity, prevents secondary victimization, and avoids unnecessary public exposure of sensitive information. In this regard, data protection is not merely a technical administrative safeguard but forms an integral component of substantive justice grounded in equality.

Despite the normative clarity of equality before the law, practical enforcement often reveals disparities between victims and perpetrators, particularly in terms of access to justice. Victims—especially women, children, and members of marginalized communities—frequently encounter social stigma, moral judgment, and psychological pressure even before legal protection is effectively extended to them. This phenomenon may discourage reporting and perpetuate a climate of silence. Consequently, the equality principle requires the state not only to provide identical procedural guarantees in a formal sense but also to adopt measures ensuring effective and meaningful access to justice for victims. Equal protection must therefore encompass non-discriminatory treatment during investigative and judicial proceedings, adequate safeguards for identity protection, access to remedies and compensation, and the availability of legal assistance for individuals lacking sufficient resources. Without such measures, the promise of equality before the law risks remaining declaratory rather than transformative.

[22] Lusiana Jomesti et al., "Reconstructing Justice: The Role of Law No. 8 of 1981 in Upholding Equality Before the Law in Indonesia," *JISRAH: Jurnal Integrasi Ilmu Syariah* 6, no. 1 (April 30, 2025): 35, https://doi.org/10.31958/jisrah.v6i1.15669.

Doi: 10.59631/slr.v4i1.494

The enforcement of equality before the law in cases involving the covert dissemination of obscene content is further complicated by structural and technological challenges. Social stigma surrounding intimate or obscene content frequently results in victim-blaming attitudes that undermine credibility and intensify psychological harm. Simultaneously, digital platforms enable perpetrators to exploit anonymity, encryption, and cross-border dissemination, thereby complicating identification and prosecution. This technological asymmetry often advantages perpetrators while leaving victims with limited capacity to trace digital evidence or initiate effective legal action. Socioeconomic disparities further exacerbate inequality, as individuals from disadvantaged backgrounds may lack financial resources, digital literacy, or institutional support necessary to pursue legal remedies. These structural conditions demonstrate that the realization of equality before the law requires more than normative affirmation; it demands institutional responsiveness capable of addressing social and technological imbalances.

Within this framework, strengthening the implementation of equality before the law necessitates systemic and coordinated measures. Enhancing public awareness of privacy rights and personal data protection can empower victims to assert their legal entitlements and reduce reluctance to report offenses. Simultaneously, law enforcement institutions must internalize a victim-sensitive approach that safeguards dignity and confidentiality while preserving procedural fairness. Regulatory oversight of digital platforms also assumes strategic importance, as service providers play a pivotal role in preventing, detecting, and removing non-consensual intimate content. Clarifying platform responsibilities and ensuring effective cooperation with law enforcement authorities contribute to a more balanced legal environment in which technological infrastructures do not perpetuate inequality.

The analysis above illustrates that the application of equality before the law in cases involving the covert dissemination of obscene content operates at the intersection of criminal law, data protection, and social justice. Although a normative legal framework exists to protect privacy and personal data rights, its effectiveness depends on consistent enforcement practices, equitable access to justice, and the mitigation of structural barriers that disproportionately burden victims. The continued development of a data protection–oriented criminal justice approach remains essential for ensuring that equality before the law functions as a substantive guarantee rather than a purely formal principle within the digital era.

CONCLUSION

This study demonstrates that the covert dissemination of obscene content constitutes not merely a morality-based offense but a serious violation of personal data protection rights that directly implicates the principle of equality before the law. Although Indonesia's legal framework—particularly the Personal Data Protection Law, the Pornography Law, the Electronic Information and Transactions Law, and the Sexual Violence Crimes Law—provides a relatively comprehensive normative basis for criminal liability and victim protection, enforcement practices remain fragmented and insufficiently integrated. In practice, morality-based provisions are often prioritized, while the personal data dimension of the offense is marginalized, thereby narrowing the scope of accountability and weakening deterrence. Structural challenges, including limited legal awareness among victims, technological complexities in digital evidence collection, cross-border dissemination, and inconsistent sanctioning standards, further undermine effective

protection. From the perspective of substantive equality, these conditions reveal a gap between formal legal guarantees and their realization in practice, particularly for victims from vulnerable or marginalized groups who face stigma, secondary victimization, and unequal access to justice.

This research is limited by its doctrinal and normative focus, which relies primarily on statutory analysis and conceptual examination rather than extensive empirical case studies or quantitative enforcement data. Consequently, variations in judicial reasoning, prosecutorial discretion, and regional enforcement practices may not be fully captured. Future research would benefit from empirical investigations, including case law analysis, interviews with law enforcement officials, and victim-centered studies to assess how equality before the law is operationalized in concrete proceedings. Policy-wise, strengthening institutional capacity in digital forensics, enhancing structured cooperation between law enforcement agencies and digital platform providers, and standardizing sentencing guidelines for data-related offenses are essential steps toward improving consistency and proportionality. Equally important is the expansion of public legal education and accessible legal aid mechanisms to ensure that victims can effectively exercise their rights. Through these measures, the integration of personal data protection principles into the broader criminal justice framework can move beyond formal recognition toward substantive realization of equality before the law in the digital era.

REFERENCES

Aqila, Azzahra Nayla, and Eva Muti'ah. "The Impact Of Social Media On Changes In Social Interaction Patterns In Cities." *Bina Bangsa International Journal of Business and Management* 5, no. 1 (April 30, 2025): 304–16. https://doi.org/10.46306/bbijbm.v5i1.127.

Awaluddin. "The Existence of Law Number 27 Of 2022 Concerning Personal Data Protection in Protecting Citizens' Privacy Rights." *Indonesian Research Journal in Legal Studies* 4, no. 2 (September 30, 2025): 54–60. https://doi.org/10.31934/irjils.v4i2.8717.

Edrisy, Ibrahim Fikma. "Tinjauan Yuridis Terhadap Tindak Pidana Asusila Dalam Undang-Undang ITE (Studi Putusan Nomor 262/Pid.Sus/2021/PN Kbu)." *Jurnal Hukum Legalita* 5, no. 1 (July 31, 2023): 1–13. https://doi.org/10.47637/legalita.v5i1.730.

Fachran, Syahreza, Sinta Dewi Rosadi, and Prita Amalia. "Protection Of Data Subject Rights In The Transfer Of Personal Data Between Data Controllers In Indonesia: A Comparative Analysis Of The PDP Law And The EU GDPR." *Awang Long Law Review* 8, no. 2 (January 16, 2026): 518–29. https://doi.org/10.56301/awl.v8i2.1827.

Hakiki, Azizul, Nuruz Zakiyatul Mufidah, Kunarso Kunarso, and Natalia Setyawati. "Digital Content Crimes In Criminal Liability." *Journal of Multidisciplinary Research*, November 15, 2024, 36–44. https://doi.org/10.56943/jmr.v3i3.651.

Hibar, Ujang, Enjum Jumhana, and Suherman Arifin. "Cybercrime Digital Crime How Technology Is Utilized for Crime." *Journal of Law Science* 7, no. 1 (January 31, 2025): 1–9. https://doi.org/10.35335/jls.v7i1.5848.

Ibrahim, Vicky, Yeti Hasan, and Parmin Ishak. "Personal Data Protection Policies and Their Impact on Victims of Cybercrime." *Jurnal Ilmu Hukum Kyadiren* 6, no. 2 (December 10, 2024): 13–25. https://doi.org/10.46924/jihk.v6i2.225.

Isya, Ibrahim Muhammad, and Susilo Wardani. "Analisis Yuridis Perlindungan Privasi Terhadap

Pengambilan Foto Tanpa Izin Di Era Digital." *Jurnal Penelitian Serambi Hukum* 18, no. 02 (June 25, 2025): 228–38. https://doi.org/10.59582/SH.V18I02.1332.

Jomesti, Lusiana, Emrizal Emrizal, Dian Pertiwi, and Kamaluddin Kamaluddin. "Reconstructing Justice: The Role of Law No. 8 of 1981 in Upholding Equality Before the Law in Indonesia." *JISRAH: Jurnal Integrasi Ilmu Syariah* 6, no. 1 (April 30, 2025): 35. https://doi.org/10.31958/jisrah.v6i1.15669.

Mardyansyah, Dody Novizar, Sukarmi, Adi Kusumaningrum, and Yenny Eta Widyanti. "Harmonization of Personal Data Protection Principles With Electronic Justice Systems In Indonesia." *Yuridika* 40, no. 3 (September 30, 2025): 343–68. https://doi.org/10.20473/ydk.v40i3.74179.

Nugroho, Muhamad Rizal Satrio, Muhammad Nurcholis Alhadi, and Ikhwanul Muslim. "The Crime of Spreading Pornographic Content in Digital Media." *TATOHI: Jurnal Ilmu Hukum* 5, no. 1 (March 31, 2025): 1. https://doi.org/10.47268/tatohi.v5i1.2890.

Pratiwi, Friska Yulanda, and Fajar Rachmad Dwi Miarsa. "Urgensi Edukasi Publik Dalam Menangkal Penyalahgunaan Data Pribadi." *RIGGS: Journal of Artificial Intelligence and Digital Business* 4, no. 2 (May 25, 2025): 1342–49. https://doi.org/10.31004/riggs.v4i2.672.

Pratiwi, Ratu Indra Kasih. "Understanding Criminal Liability for Pornography in Cyberspace Based on the Pattern of Distribution." *Damhil Law Journal* 4, no. 1 (May 30, 2024): 82. https://doi.org/10.56591/dlj.v4i1.2511.

Prayudati, Yulia Martha, Wessy Trisna, and Yati Sharfina Desiandri. "Analysis Of The Threat Of The Spread Of Intimate Content Non Consensual In Violence Gender Based Online." *SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan* 4, no. 8 (July 5, 2025): 1911–24. https://doi.org/10.54443/sibatik.v4i8.2833.

Purtova, Nadezhda. "The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law." *Law, Innovation and Technology* 10, no. 1 (January 2, 2018): 40–81. https://doi.org/10.1080/17579961.2018.1452176.

Putri, Malia Dwi, Eram Maling, Andi Mar'atussholihah, Nurdiana A. Quilo, and Jibria Ratna Yasir. "Disability Law and Human Rights: Theory and Policy." *Disability & Society* 40, no. 5 (May 4, 2025): 1435–37. https://doi.org/10.1080/09687599.2024.2411148.

Rizki, Muhammad, Irawan Harahap, and Rudi Pardede. "Penerapan Hukum Terhadap Pelaku Penyebaran Konten Pornografi." *Collegium Studiosum Journal* 8, no. 1 (June 30, 2025): 265–76. https://doi.org/10.56301/csj.v8i1.1710.

Salmon, Harly Clifford J, Denny Latumaerissa, and Judy Marria Saimima. "Penegakan Hukum Terhadap Pelaku Penyebaran Konten Asusila." *Risalah Hukum* 21, no. 1 (June 30, 2025): 20–31. https://doi.org/10.30872/risalah.v21.i1.1593.

Simbolon, Valentina Ancillia, and Vishnu Juwono. "Comparative Review of Personal Data Protection Policy in Indonesia and The European Union General Data Protection Regulation." *Publik (Jurnal Ilmu Administrasi)* 11, no. 2 (December 30, 2022): 178–90. https://doi.org/10.31314/pjia.11.2.178-190.2022.

Strand, Vibeke Blaker, and Ingunn Ikdahl. "Responding to Disadvantage and Inequality through Law." *Oslo Law Review* 4, no. 3 (December 15, 2017): 124–32.

https://doi.org/10.18261/issn.2387-3299-2017-03-01.

Vicks, Mary E. "An Examination of Internet Filtering and Safety Policy Trends and Issues in South Carolina 's K-12 Public Schools." Nova Southeastern University, 2013.

Zaid. *Perlindungan Privasi Dan Data Pribadi: Sebuah Tinjauan Pengantar*. Malang: Setara Press, 2024.