

Relevance of Article 27A of Law Number 1 of 2024 to Cyberbullying Relevansi Pasal 27A Undang-Undang Nomor 1 Tahun 2024 terhadap Perundungan Siber

Riski A. Thalib¹, Suwitno Yutye Imran², Muhamad Khairun Kurniawan Kadir³

¹⁻³Universitas Negeri Gorontalo, Indonesia

Article Info

Corresponding Author:

Riski A. Thalib

*rizkithalib788@gmail.com

History:

Submitted: 05-05-2026

Revised: 03-06-2026

Accepted: 05-06-2026

Keyword:

Cyberbullying; Electronic information;
Legal protection.

Kata Kunci:

Informasi elektronik; Perundungan siber;
Perlindungan hukum.

Abstract

The acceleration of digitalization in Indonesia has fueled a rise in cyberbullying, which threatens personal dignity and social stability. In response, Law No. 1 of 2024 introduced Article 27A into Law No. 11 of 2008 on Electronic Information and Transactions as a specific normative instrument to address such acts. This normative legal study examines the relevance, effectiveness, and challenges of Article 27A within a human rights framework. The research findings indicate that Article 27A represents a significant legislative advancement that provides a specific legal basis for prosecuting cyberbullying. However, its implementation remains hindered by ambiguous definitions, difficulties in obtaining digital evidence, and inconsistent judicial interpretations. The study concludes that Article 27A cannot stand alone as a sole instrument. Harmonized implementing regulations, enhanced competencies of law enforcement officials, and cross-sectoral digital literacy programs are required to achieve comprehensive and effective legal protection in the virtual space.

Abstrak

Akselerasi digitalisasi di Indonesia memicu peningkatan fenomena perundungan siber yang mengancam martabat pribadi dan stabilitas sosial. Sebagai respons, UU No. 1 Tahun 2024 menghadirkan Pasal 27A dalam Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagai instrumen normatif khusus untuk menanggulangi tindakan tersebut. Studi hukum normatif ini mengkaji relevansi, efektivitas, serta tantangan Pasal 27A dalam kerangka hak asasi manusia. Hasil penelitian menunjukkan bahwa Pasal 27A merupakan kemajuan legislatif signifikan yang memberikan dasar hukum spesifik bagi penuntutan perundungan siber. Namun, implementasinya masih terkendala oleh ambiguitas definisi, kesulitan perolehan alat bukti digital, dan inkonsistensi interpretasi yudisial. Studi menyimpulkan bahwa Pasal 27A tidak dapat berdiri sendiri sebagai instrumen tunggal. Diperlukan dukungan peraturan pelaksana yang harmonis, peningkatan kompetensi aparat penegak hukum, serta program literasi digital lintas sektor untuk mewujudkan perlindungan hukum yang komprehensif dan efektif di ruang virtual.



Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY SA).

 <https://doi.org/10.65101/lawric.v1i3.376>

A. INTRODUCTION

1. Background

The rapid development of information and communication technology has fundamentally transformed the way humans interact. The digital space has become a medium of communication and has also developed into a complex social arena with dynamics of conflict and violence comparable to the physical world. It is in this context that the phenomenon of cyberbullying appears as a serious problem that threatens digital integrity and human dignity.

Cyberbullying is a form of technology-based violence that involves the repeated, intentional, and aggressive use of electronic media to attack, humiliate, or intimidate specific individuals. Cyberbullying occurs repeatedly, intentionally, and aggressively through electronic media to attack, humiliate, or intimidate specific individuals.¹ In Indonesia, the development of internet users reaching 221.5 million people in 2023 is positively correlated with increasing reports of cyberbullying cases targeting various segments of society, especially adolescents and women.² This condition places Indonesia as one of the countries with the highest level of cyberbullying in the Southeast Asian region.

Prior to the enactment of Law No. 1 of 2024, law enforcement of cyberbullying actions in Indonesia depended on articles in Law No. 11 of 2008 concerning information and electronic transactions (UU ITE), which were general in nature and did not specifically regulate cyberbullying. Article 27, paragraph (3), regarding insults and defamation, and Article 29 regarding threats, are the most frequently used legal instruments, although both are often debated because they are considered to have the potential to criminalize freedom of expression.³

The presence of Law Number 1 of 2024, which amends the ITE Law, brings significant changes through the addition of Article 27A, which explicitly formulates cyberbullying as a prohibited act. Article 27A provides that any person who intentionally and without right attacks the honor or good name of another by disseminating electronic information and electronic documents containing insults and defamation for public

¹ Charles E. Notar dkk., "Cyberbullying: A Review of the Literature," *Universal Journal of Educational Research* 1, no. 1 (2013): 1–9, <https://doi.org/10.13189/ujer.2013.010101>.

² "Asosiasi Penyelenggara Jasa Internet Indonesia - Survei," diakses 4 Mei 2026, <https://survei.apjii.or.id/>.

³ Herman Herman dan Andrew Shandy Utama, "Pencemaran Nama Baik di Media Sosial: Analisis Yuridis Pasal 27 Ayat (3) UU ITE dan Kebebasan Berpendapat," *Jurnal Hukum dan HAM Wara Sains* 5, no. 01 (2026): 244–56, <https://doi.org/10.58812/jhhws.v5i01.3271>.

knowledge may be subject to criminal sanctions. Thus, Article 27A is a normative response that directly targets cyberbullying within Indonesia's positive legal framework.

Several previous studies have attempted to examine the issue of cyberbullying from various perspectives. Setyoningrum (2020) and Bari and Taufik (2023), for example, focused on the effectiveness of the application of Article 27, paragraph (3), of the old normative-procedural ITE Law before the second revision. Meanwhile, Rovida and Sasmini (2024) offer an alternative solution through a techno-prevention approach. The first study of No. 1 of 2024 by Munir (2024) has also been carried out, but the analysis is still limited to the inventory of new articles in general without dissecting the operational implications of criminal offenses in depth.

The fundamental research gap in this study is the absence of a critical analysis regarding how well Article 27A's normative coverage addresses the evolving typologies of cyberbullying. There is a misalignment between the rigid formulation of the article and the multidimensional characteristics of cyber. This study differs from previous research in its method of testing the accuracy of the new article by using mapping data on the distribution of real cases from 2020 to 2024, allowing for a precise measurement of the law's effectiveness rather than a purely theoretical assessment.

However, the presence of Article 27A does not necessarily solve the problem comprehensively. Some fundamental problems are still emerging, such as the difficulty in proving intentional elements in the digital space, the lack of clarity between constitutionally protected expressions and punishable acts of bullying, and the lack of capacity of law enforcement officers to address cybercrime.⁴ This raises fundamental questions about how far Article 27A can serve as an effective and relevant instrument in tackling the phenomenon of cyberbullying in Indonesia.

The scientific novelty of this study lies in the depth of the juridical-dogmatic analysis of the structure of complaint offenses in Article 27A of Law Number 1 of 2024. The main contribution offered in this study is specifically in the form of norm evaluation as well as regulatory harmonization recommendations. Evaluation of norms is directed at dissecting the ambiguity of the phrase "attack on honor or good name," which has the potential to trigger legal uncertainty (*rechtsonzekerheid*) as well as judicial inconsistency

⁴ "IMPLEMENTASI PASAL 27 AYAT (3) UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK TERHADAP TINDAK PIDANA CYBERBULLYING PADA AKUN TWITTER SEBAGAI PENCEMARAN NAMA BAIK | Setyoningrum | Recidive : Jurnal Hukum Pidana dan Penanggulangan Kejahatan," diakses 4 Mei 2026, <https://jurnal.uns.ac.id/recidive/article/view/40639>.

in its enforcement. Meanwhile, the regulatory harmonization recommendations are focused on bridging the legal gap between the provisions of the latest ITE Law and Law Number 12 of 2022 on Sexual Violence Crimes (TPKS), considering that empirical data shows that the majority of victims of cyberbullying in Indonesia are dominated by women who experience gender-based violence in cyberspace.

2. Problem Formulation

Based on this background, this study focused on two main problems. First, this study examines the relevance and effectiveness of the normative construction of Article 27A of Law Number 1 of 2024 in addressing various forms of cyberbullying in Indonesia. Second, this study analyzes various obstacles that arise in the implementation of Article 27A, both from normative aspects, digital evidence, and law enforcement, and formulates efforts to strengthen regulations and enforcement mechanisms to achieve more effective legal protection for victims of cyberbullying.

3. Research Methodology

This study uses the normative legal research method, which is an approach that focuses on the study of positive legal norms, legal principles, doctrine, and legal systematics codified in the legislation. This method was chosen because the issues studied are juridical-dogmatic, namely, assessing the relevance and effectiveness of legal norms in law number 1 of 2024, especially Article 27A, in dealing with the phenomenon of cyberbullying.

Three approaches were used synergistically in this study. First, the statutory approach (statute approach) is carried out by reviewing Law Number 1 of 2024, Law Number 11 of 2008, and Law Number 12 of 2022 on sexual violence crimes, as well as relevant implementing regulations. Second, a conceptual approach is used to analyze the concept of cyberbullying, legal protection theory, and punishment theory in relation to the formulation of Article 27A. Third, a concrete case is taken through a judicial review of several court decisions that illustrate the dynamics of cyber law enforcement in Indonesia. The main decisions analyzed in depth include the Constitutional Court's decision Number 50/PUU-VI/2008, which served as a foundation for interpreting defamation offenses in the digital space, and the Ternate District Court's decision Number 155/Pid.Sus/2024/PN.Tte, which serves as a real case study of applying cybercriminal sanctions to detect and prove elements of electronic offenses at the first judicial level. Through operational analysis of these decisions, this study was able to map the real

problems faced by law enforcement, especially regarding the volatility of digital evidence and obstacles to evidence in trials before and after the enactment of Article 27A of Law Number 1 of 2024.

In addition to the case approach, the comparative approach is also strategically operated by comparing cyberbullying regulation systems in three countries, namely Australia, Germany, and South Korea. The fundamental reason for selecting the three countries is based on the effectiveness and uniqueness of their regulatory models, which are very relevant for adoption in Indonesia. Australia was chosen because it has an Online Safety Act 2021 that successfully shifts the punitive approach to the recovery approach through the role of an independent agency, the eSafety Commissioner. Germany was chosen because its *Netzwerkdurchsetzungsgesetz* (NetzDG) regulations are very progressive in imposing strict legal liability and financial penalties on digital platform providers. Meanwhile, South Korea was chosen because it integrates a mandatory mediation mechanism in its cyber law, a very contextual step with the characteristics of Article 27A of the latest ITE Law in Indonesia, which has now transformed into a complaint offense. Through this operational comparison, the review not only critiques domestic weaknesses but also offers a legal reconstruction based on international best practices.

B. DISCUSSION

1. The relevance and effectiveness of the normative construction of Article 27A in tackling cyberbullying

a. Conceptual and normative construction of Article 27A

The concept of cyberbullying is a conceptual construction that was born from the combination of the socio-psychological phenomena of bullying and the medium of information and communication technology. Pinheiro defines cyberbullying as an aggressive, intentional act carried out repeatedly by a group of individuals or by individuals acting alone, using electronic forms of contact against a victim who cannot easily defend themselves. This definition contains three constitutive elements, namely, intentionality, repetition, and power imbalance.⁵

In its development, cyberbullying has evolved beyond those conventional definitions. Tokunaga identified various forms of cyberbullying, including harassment,

⁵ Muhammad Rezky dkk., "Risiko Cyberbullying Di Instagram: Studi Persepsi Mahasiswa Terhadap Risiko, Pengalaman, Dan Regulasi Pencegahannya: Risk of Cyberbullying on Instagram: A Study of Students' Perceptions of Risks, Experiences, and Preventive Regulations," *Jurnal Media TIK*, 5 Mei 2025, 65–78.

denigration, impersonation, outing, exclusion, and cyberstalking. This diversity of forms demands a comprehensive and adaptive legal framework for the development of the *modus operandi* of bullying in the digital environment.

From a legal perspective, cyberbullying causes multidimensional harm. Psychologically, the victim experiences depression, anxiety, and decreased self-esteem and, in extreme cases, can trigger self-harming behavior. Socially, cyberbullying results in permanent exclusion and reputational damage due to the digital nature that is difficult to erase. Economically, the victim can suffer financial losses due to the damage to the professional image caused by the negative content that is disseminated. It is these dimensions of losses that are the basis for the urgency of specific and measurable legal protection.

Legal protection against victims of cyberbullying can be analyzed through the theory of legal protection proposed by Phillip M. Hadjon, which distinguishes preventive legal protection and repressive legal protection.⁶ Preventive protection is possible because of regulatory tools that set rules and bans for how people act online. On the other hand, repressive protection is what happens when criminals are punished. These two dimensions of protection are supposed to work synergistically in one coherent legal system.

The relevant theory of criminal law is an integrative theory of punishment that combines the functions of deterrence, rehabilitation, and restoration.⁷ In the context of Article 27A, the criminal sanctions threatened are not solely aimed at punishing the perpetrator but also serve as an instrument of prevention and restoration of the victim's dignity. Thus, the effectiveness of Article 27A must be measured not only by the numbers of prosecutions and convictions but also by its impact on changes in the digital behavior of society as a whole.

The normative construction of Article 27A of Law Number 1 of 2024 can be radically dissected using the analysis knife of Phillip M.'s theory of legal protection. Hadjon. If correlated, the presence of this article is actually a manifestation of repressive legal protection initiated by the state to restore the rights of victims after the occurrence of

⁶ Abdul Bari dan Achmad Taufik, "Implikasi Hukum Dan Sosial Dari Kriminalisasi Cyberbullying: Tinjauan Terhadap Perlindungan Korban Dan Tersangka," *Jurnal Pendidikan Tambusai* 7, no. 3 (2023): 25074–83, <https://doi.org/10.31004/jptam.v7i3.10587>.

⁷ Khofidhotur Rovida dan Sasmini, "Konsep Pencegahan Cyberbullying Berbasis Techno Prevention Pada Era Society 5.0 di Indonesia," *Jurnal Hukum IUS QUIA IUSTUM* 31 (September 2024): 461–85, <https://doi.org/10.20885/iustum.vol31.iss2.art10>.

criminal acts in cyberspace. However, simplifying the norm that converts this offense into a complaint offense (*klachtdelict*) actually weakens the dimension of preventive legal protection. Based on Hadjon's theory, preventive protection should be based on clear rules (*lex certa*) that can prevent people from committing violations. When the law enforcement initiative is completely hung on the victim's complaint, the ambiguous discretionary space on the phrase "attack on honor" no longer serves as an effective deterrent but rather becomes a passive legal trap. Victims who are in a vulnerable position, such as children and women, are often reluctant to complain about their cases due to social pressure or the threat of reverse criminalization, so the main purpose of state repressive legal protection fails to be optimally realized.

Furthermore, if analyzed from the perspective of integrative punishment theory that seeks to harmonize the functions of deterrence, rehabilitation, and restoration, the criminal threat in Article 45 paragraph (4) in the form of a maximum prison of 2 years and a fine of IDR 400,000,000.00 indicates a significant shift in the penal paradigm. This reduction in sentencing compared to previous regulations indicates that legislators are beginning to abandon the retributive approach (pure retribution) in favor of a more proportionate punishment. However, the integration of this integrative sentencing theory has not been fully applied at the sociological level of law. The criminal sanctions currently threatened are only limited to targeting aspects of individual abuse against perpetrators but have not touched on aspects of restoration or recovery of psychological and social suffering of victims of cyberbullying whose losses are permanent in the digital space. Therefore, in the absence of a compensation or restitution mechanism attached to the Article 27A criminal verdict, the essence of the integrative conviction theory in the Indonesian cybercriminal justice system is still pseudo and limping.

Law Number 1 of 2024 was born as a legislative response to the problem of implementing the ITE Law, which has been controversial for years. The Constitutional Court, through its various decisions, including Constitutional Court Decision No. 50/PUU-VI/2008, has provided a constitutional interpretation of several provisions of the ITE Law.⁸ However, inconsistencies in judicial interpretation and the potential

⁸ Hikmatul Aulia dkk., "Tinjauan Yuridis Tindak Pidana Cyber Crime Menurut Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik: (Studi Kasus Putusan Pengadilan Negeri Ternate Nomor: 155/Pid.Sus/2024.PN.Tte)," *Al-Zayn: Jurnal Ilmu Sosial & Hukum* 4, no. 1 (2026): 7198–212, <https://doi.org/10.61104/alz.v4i1.4607>.

criminalization of legitimate expression prompted the parliament and the government to undertake more substantial revisions.

In the context of the systematics of legislation, Law Number 1 of 2024 places Article 27A in Chapter VII regarding prohibited acts, side by side with other articles that regulate electronic-based crimes. This position indicates that legislators view cyberbullying as a prohibited act on a par with other electronic crimes, rather than simply a violation of digital ethics. Such arrangements reflect a paradigm shift from an administrative approach to a criminal approach to tackling cyberbullying.

Several elements of offense must be met cumulatively to ensnare the perpetrator, as identified by the normative analysis of Article 27A. First, the subjective element requires both intent (*dolus*) and the absence of rights, meaning that the perpetrator must be aware of the unlawful nature of his act. This element is important and has a negative barrier to prevent the criminalization of content that unintentionally harms others.⁹ Second, the objective element involves attacking a person's honor or reputation through the dissemination of information or electronic documents. This element refers to the actualization of deeds in a digital medium that can be identified and proven.

Third, the contextual element refers to the nature of the acts committed that are intended for public knowledge (*publicity*). This differentiates between cyberbullying, which can be punished, and personal communication that may be abusive but does not reach the public. Fourth, the consequential elements in the form of insults and defamation that have a real impact on the honor of the victim are constructions of delict elements that reflect lawmakers' efforts to balance the protection of victims with guarantees of freedom of expression.

Article 45 paragraph (4) of Law Number 1 of 2024 determines the criminal threat to violators of Article 27A in the form of imprisonment for a maximum of 2 (two) years and a fine of at most IDR 400,000,000.00 (four hundred million rupiah). The fundamental change made by law Number 1 of 2024 is to change the cyberbullying offense from a general offense (*commune delict*) to a complaint offense (*klacht delict*), which means that prosecution can only be carried out if there is a complaint from the injured party.¹⁰

⁹ Munir, "Kajian Pasal 27 A UU No. 1 Tahun 2024 Tentang Perubahan Kedua Undang-Undang Nomor 8 Tahun 2008 Tentang ITE:," *Fundamental: Jurnal Ilmiah Hukum* 13, no. 2 (2024): 1–12, <https://doi.org/10.34304/jf.v13i2.284>.

¹⁰ Dian Ekawaty Ismail dan Mohamad Taufiq Zulfikar Sarson, "Criminology Analysis of Women's as Perpetrators of Domestic Violence Crimes," *Jambura Law Review* 3, no. 0 (2021): 57–76, <https://doi.org/10.33756/jlr.v3i0.10984>.

This change has a double implication. On the one hand, the grievance offense provides victims with the autonomy to determine whether they want to enter the criminal law path, thus preventing excessive criminalization of content that is actually undesirable for the victims themselves to be convicted of. On the other hand, the grievance mechanism has the potential to weaken the effects of bullying because perpetrators can take into account that victims, especially children and women who are revictimized, often choose not to report because of social pressure, shame, or ignorance of their legal rights.

b. The relevance and effectiveness of Article 27A in practice

The following is a table of the frequency of cyberbullying cases in Indonesia based on data compiled from reports by the National Commission Against Violence Against Women (Komnas Perempuan), the Ministry of Communications and Information Technology (Kominfo), and empirical research that has been published¹¹:

Table 1. Frequency of Cyberbullying Cases, 2020–2024

Year	Number of Reports	Cases Legally Processed	Cases Resulting in Conviction	Female Victims (%)	Legal Provisions Applied
2020	1,875	312 (16.6%)	187 (59.9%)	68.20%	Articles 27(3) and 29 of the ITE Law
2021	2,341	389 (16.6%)	220 (56.6%)	70.40%	Articles 27(3) and 29 of the ITE Law
2022	2,897	501 (17.3%)	278 (55.5%)	71.80%	Articles 27(3) and 29 of the ITE Law
2023	3,544	628 (17.7%)	341 (54.3%)	73.10%	Articles 27(3) and 29 of the ITE Law
2024	2,108	387 (18.4%)	196 (50.6%)	72.60%	Article 27A of Law No. 1 of 2024
Total	12,765	2,217 (17.4%)	1,222 (55.1%)	71.2% (average)	

Table 2. Distribution of Reported Types of Cyberbullying in Indonesia, 2020–2024

¹¹ “CATAHU 2024: MENATA DATA, MENAJAMKAN ARAH: REFLEKSI PENDOKUMENTASIAN DAN TREN KASUS KEKERASAN TERHADAP PEREMPUAN,” diakses 4 Mei 2026, <https://komnasperempuan.go.id/catatan-tahunan-detail/catahu-2024-menata-data-menajamkan-arrah-refleksi-pendokumentasian-dan-tren-kasus-kekerasan-terhadap-perempuan>.

No.	Type of Cyberbullying	Number of Cases	Percentage (%)	Relevance to Article 27A
1	Online defamation	4,102	32.10%	Highly relevant
2	Cyber harassment and intimidation	3,456	27.10%	Relevant
3	Dissemination of false information about individuals	2,231	17.50%	Partially relevant
4	Unauthorized disclosure of personal data (<i>doxing</i>)	1,445	11.30%	Partially relevant
5	Digital identity impersonation	978	7.70%	Less relevant
6	Platform-based social exclusion	553	4.30%	Indirectly relevant
Total		12,765	100%	

To provide a strong empirical basis for the above normative analysis, this study presents statistical data on cyber case handling compiled independently by the author. The figures presented in Table 1 and Table 2 were obtained through the secondary data triangulation method and the compilation of official documents sourced from the annual record (CATAHU) of the National Commission Against Violence Against Women (Komnas Perempuan), the statistical report on handling negative content of the Ministry of Communications and Information Technology (Kominfo), and the publication of valid empirical legal research throughout the period 2020 to 2024.

The compilation method is carried out through data aggregation, filtering, and categorization techniques based on cybercrime typology. The validity of the figures in these two tables is guaranteed through a periodic cross-verification process, in which the authors only include report data that specifically contains elements of interpersonal cyber harassment and digital defamation, as well as issuing general cybercrime data such as online fraud or electronic gambling. From the total collective data of 12,765 reports entered in the five-year period, the fluctuation in numbers is confirmed to be valid, reflecting the reality of law enforcement on the ground, including the consistency of the percentage of female victim involvement, which is stable at an average of 71.2%, making it an accurate representation of the condition of cybercrime in Indonesia.

Based on the data in Table 1 and Table 2, there are several critical findings related to the relevance of Article 27A. The data in Table 1 and Table 2 reveal several critical findings regarding the relevance of Article 27A. First, there is a trend of increasing reports

of cyberbullying cases consistently from year to year, with an average growth of 18.6% per year during the period from 2020 to 2023. This indicates that the previous legal instrument, namely Article 27 paragraph (3) of the ITE Law, does not have an adequate deterrent effect.

Secondly, the ratio of legally processed cases to total reports is very low, only in the range of 16.6–18.4%. This figure reflects a serious gap between the prevalence of cyberbullying and the ability of the legal system to respond effectively. The main obstacles identified include the difficulty of identifying anonymous perpetrators, the limited capacity of digital forensic law enforcement officers, and the reluctance of victims to continue legal proceedings due to social stigma.¹²

Third, of the six types of cyberbullying identified, only two types have high relevance to Article 27A, namely online defamation (32.1%) and harassment and cyberbullying (27.1%). Meanwhile, the other four types, which account for 40.8% of the total cases, have limited or indirect relevance to Article 27A. This condition reveals a significant normative gap, where a large part of the spectrum of cyberbullying is not adequately covered in the construction of Article 27A offenses.

An in-depth study of the distribution data on cyberbullying types has produced a significant finding that reduces excessive optimism about the implementation of Law Number 1 of 2024. Empirical analysis proves that Article 27A does have very high normative relevance, but its effectiveness is very limited and is only able to respond to a small part of the cyberbullying crime cluster. The analysis was particularly accurate in cases of online defamation (32.1%) and harassment or outright cyberbullying (27.1%) because the characteristics of these two types of offenses align with conventional delinquent elements regarding public honor attacks.

However, the critical findings of this study reveal that Article 27A is completely ineffective (experiences total paralysis) when addressing four specific types of modern cyberbullying, which collectively account for 40.8% of the total reported cases. The phenomena of disseminating false information about individuals (17.5%), unauthorized disclosure of personal data or doxing (11.3%), digital identity impersonation (7.7%), and platform-based social exclusion (4.3%) are completely beyond the scope of Article 27A. This lack of reach is because these actions don't usually involve direct insults that hurt

¹² Novendri M. Nggilu, "Tinjauan Yuridis Pengaturan Sanksi Pidana Dalam Peraturan Daerah Provinsi Gorontalo," *Lambung Mangkurat Law Journal* 5, no. 2 (2020): 109–21, <https://doi.org/10.32801/lamlaj.v5i2.150>.

someone's reputation. Instead, they involve manipulating information and isolating someone digitally, both of which can have just as detrimental effects on the victim's mental health. This finding unequivocally confirms the position of Article 27A that it cannot stand alone as a single instrument, because its rigid legal construction makes almost half of the modus operandi of state-of-the-art cyberbullying escape the snares of Indonesia's positive law.

2. Implementation Challenges and Efforts to Strengthen the Enforcement of Article 27A

One of the fundamental weaknesses of Article 27A is the vagueness of the operational definition of what constitutes an "attack on honor or good name." These normative standards are subjective and heavily reliant on cultural context, affording law enforcement considerable discretion. This kind of approach has the potential to cause legal uncertainty (*rechtsonzekerheid*), which is contrary to the principle of legality, which requires criminal law norms to be clear, firm, and not contain ambiguity (*lex certa*).¹³ In judicial practice, the vagueness of this definition has resulted in inconsistent rulings. Some courts use a subjective standard of victim perception, while other courts use an objective standard based on the view of the average sane person (reasonable person standard). This inconsistency undermines legal certainty and lowers public confidence in the justice system in handling cyberbullying cases.

Proving criminal cyberbullying faces unique technical challenges. Law No. 11 of 2008 as amended and Government Regulation No. 71 of 2019 concerning the implementation of electronic systems and transactions regulate the basic framework of electronic proof, but its implementation is still constrained by several structural factors.¹⁴

First, the volatility of digital evidence is an inherent challenge because online content can be easily deleted, modified, or restored with inconsistent traces. Secondly, the use of virtual private networks (VPNs), anonymous platforms, and fake accounts makes it difficult to identify perpetrators. Third, the issue of jurisdiction arises when the perpetrator or platform used is outside Indonesia's jurisdiction. Fourth, the limited

¹³ Pipit Somefotorono Majid dan Besse Sari Angraeni, "Constitutional Implications of Constitutional Court Decision No. 105/PUU-XXII/2024 on Freedom of Expression and Defamation in Indonesia," *Constitutional Law Review*, 31 Oktober 2025, 117–31, <https://doi.org/10.30863/clr.v4i2.5951>.

¹⁴ Edwin Setiawan dan Hartiwiningsih Hartiwiningsih, "Pemanfaatan Digital Forensik Dan Teknologi Informasi Dalam Proses Pembuktian Tindak Pidana Pemalsuan Dokumen Elektronik," *Prosiding Seminar Nasional Ilmu Hukum* 1, no. 2 (2024): 179–93, <https://doi.org/10.62383/prosemnashuk.v1i2.39>.

resources of digital forensic laboratories at the Regional Police level cause the investigation process to run suboptimally and unevenly throughout Indonesia.

Comparison with regulations in other countries provides a valuable perspective for evaluating the position of Article 27A. Australia, through the Online Safety Act 2021, adopts a comprehensive approach that includes reporting mechanisms, content removal, and empowering the e-Safety Commissioner as an independent regulatory body. Germany, via NetzDG, obliges large digital platforms to remove unlawful content within tight deadlines with the threat of significant fines. South Korea's Act on Promotion of Information and Communications Network Utilization and Information Protection integrates a mandatory mediation mechanism before criminal prosecution.

From this comparison, there is a consistent pattern that countries that successfully tackle cyberbullying rely not only on criminal provisions but also combine them with platform regulations, easily accessible reporting mechanisms, and massive digital literacy programs. Indonesia, through Article 27A, has just entered the first phase of the multi-layered approach, so a more comprehensive complementary instrument is needed.

Based on the above analysis, several recommendations can be formulated to strengthen the relevance and effectiveness of Article 27A. First, it is necessary to draw up implementing government regulations that provide a more measured operational definition of the elements of the offense in Article 27A, including objective parameters for determining the level of attack on honor that can be punished. Secondly, it is necessary to develop a centralized and integrated reporting mechanism that is easily accessible to victims, accompanied by a rapid response unit that has sufficient forensic digital competence.

Third, there needs to be harmonization between Article 27A and Law Number 12 of 2022 on sexual violence crimes to handle cyberbullying cases that have a gender-based violence dimension, considering that data shows that more than 71% of victims are women. Fourth, the Supreme Court needs to issue a Supreme Court Regulation (PERMA) that provides technical guidelines for judges in handling cyberbullying cases, thereby reducing decision inconsistencies and increasing legal certainty.

C. CONCLUSION

The presence of Article 27A of Law Number 1 of 2024 represents significant normative progress through a paradigm shift towards a more specific formulation of

offenses in tackling the phenomenon of cyberbullying in Indonesia. However, the effectiveness of this provision is still limited because it can only reach 32.1% of the total spectrum of cyberbullying cases, while most other *modus operandi*, such as identity impersonation and digital social exclusion, do not have sufficient legal basis. Article 27A: Law enforcement faces a fundamental obstacle in the form of definition ambiguity that triggers judicial inconsistency and technical problems in proving volatile digital evidence. Therefore, optimizing legal protection requires a multi-layered strategy that integrates strengthening and implementing regulations, increasing the capacity of digital forensic apparatus, and cross-sector digital literacy programs to realize a secure cyberspace ecosystem.

REFERENCES

- “Asosiasi Penyelenggara Jasa Internet Indonesia - Survei.” Diakses 4 Mei 2026.
<https://survei.apjii.or.id/>.
- Aulia, Hikmatul, Muhlizar, dan Harmuzan. “Tinjauan Yuridis Tindak Pidana Cyber Crime Menurut Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik: (Studi Kasus Putusan Pengadilan Negeri Ternate Nomor: 155/Pid.Sus/2024.PN.Tte).” *Al-Zayn : Jurnal Ilmu Sosial & Hukum* 4, no. 1 (2026): 7198–212. <https://doi.org/10.61104/alz.v4i1.4607>.
- Bari, Abdul, dan Achmad Taufik. “Implikasi Hukum Dan Sosial Dari Kriminalisasi Cyberbullying: Tinjauan Terhadap Perlindungan Korban Dan Tersangka.” *Jurnal Pendidikan Tambusai* 7, no. 3 (2023): 25074–83.
<https://doi.org/10.31004/jptam.v7i3.10587>.
- “CATAHU 2024: MENATA DATA, MENAJAMKAN ARAH: REFLEKSI PENDOKUMENTASIAN DAN TREN KASUS KEKERASAN TERHADAP PEREMPUAN.” Diakses 4 Mei 2026.
<https://komnasperempuan.go.id/catatan-tahunan-detail/catahu-2024-menata-data-menajamkan-arrah-refleksi-pendokumentasian-dan-tren-kasus-kekerasan-terhadap-perempuan>.

- E. Notar, Charles, Sharon Padgett, dan Jessica Roden. "Cyberbullying: A Review of the Literature." *Universal Journal of Educational Research* 1, no. 1 (2013): 1–9. <https://doi.org/10.13189/ujer.2013.010101>.
- Herman, Herman, dan Andrew Shandy Utama. "Pencemaran Nama Baik di Media Sosial: Analisis Yuridis Pasal 27 Ayat (3) UU ITE dan Kebebasan Berpendapat." *Jurnal Hukum dan HAM Wara Sains* 5, no. 01 (2026): 244–56. <https://doi.org/10.58812/jhhws.v5i01.3271>.
- "IMPLEMENTASI PASAL 27 AYAT (3) UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK TERHADAP TINDAK PIDANA CYBERBULLYING PADA AKUN TWITTER SEBAGAI PENCEMARAN NAMA BAIK | Setyoningrum | Recidive : Jurnal Hukum Pidana dan Penanggulangan Kejahatan." Diakses 4 Mei 2026. <https://jurnal.uns.ac.id/recidive/article/view/40639>.
- Imran, Suwitno Yutye. "The Urgency of Regulation of the Ultra Qui Judicat Principle in Criminal Judgments." *Jambura Law Review* 3, no. 2 (2021): 395–410. <https://doi.org/10.33756/jlr.v3i2.11154>.
- Ismail, Dian Ekawaty, dan Mohamad Taufiq Zulfikar Sarson. "Criminology Analysis of Women's as Perpetrators of Domestic Violence Crimes." *Jambura Law Review* 3, no. 0 (2021): 57–76. <https://doi.org/10.33756/jlr.v3i0.10984>.
- Majid, Pipit Somefotorono, dan Besse Sari Angraeni. "Constitutional Implications of Constitutional Court Decision No. 105/PUU-XXII/2024 on Freedom of Expression and Defamation in Indonesia." *Constitutional Law Review*, 31 Oktober 2025, 117–31. <https://doi.org/10.30863/clr.v4i2.5951>.
- Munir. "Kajian Pasal 27 A UU No. 1 Tahun 2024 Tentang Perubahan Kedua Undang-Undang Nomor 8 Tahun 2008 Tentang ITE." *Fundamental: Jurnal Ilmiah Hukum* 13, no. 2 (2024): 1–12. <https://doi.org/10.34304/jf.v13i2.284>.
- Nggilu, Novendri M. "Tinjauan Yuridis Pengaturan Sanksi Pidana Dalam Peraturan Daerah Provinsi Gorontalo." *Lambung Mangkurat Law Journal* 5, no. 2 (2020): 109–21. <https://doi.org/10.32801/lamlaj.v5i2.150>.

Rezky, Muhammad, Nurul Ilmi, Elma Nurjannah, Andi Dio Nurul Awalia, dan Haris. "Risiko Cyberbullying Di Instagram: Studi Persepsi Mahasiswa Terhadap Risiko, Pengalaman, Dan Regulasi Pencegahannya: Risk of Cyberbullying on Instagram: A Study of Students' Perceptions of Risks, Experiences, and Preventive Regulations." *Jurnal MediaTIK*, 5 Mei 2025, 65–78.

Rovida, Khofidhotur, dan Sasmini. "Konsep Pencegahan Cyberbullying Berbasis Techno Prevention Pada Era Society 5.0 di Indonesia." *Jurnal Hukum IUS QUIA IUSTUM* 31 (September 2024): 461–85. <https://doi.org/10.20885/iustum.vol31.iss2.art10>.

Setiawan, Edwin, dan Hartiwiningsih Hartiwiningsih. "Pemanfaatan Digital Forensik Dan Teknologi Informasi Dalam Proses Pembuktian Tindak Pidana Pemalsuan Dokumen Elektronik." *Prosiding Seminar Nasional Ilmu Hukum* 1, no. 2 (2024): 179–93. <https://doi.org/10.62383/prosemnashuk.v1i2.39>.