

**JUSTICE BEYOND THE VERDICT: CRIMINAL LAW ENFORCEMENT GAPS IN
PROTECTING CYBERBULLYING VICTIMS IN MAKASSAR CITY**

Ibrahim¹, Andi Risma², La Ode Husen³

¹²³Program Studi Magister Hukum, Pascasarjana, Universitas Muslim Indonesia, Makassar,
Indonesia

Correspondence Email: im733134@gmail.com

ABSTRACT

This study critically examines the criminal law enforcement gaps in protecting cyberbullying victims in Makassar City, Indonesia. Adopting a normative-legal research methodology with a socio-legal orientation, this research integrates statutory, conceptual, and case approaches, supplemented by qualitative interviews with law enforcement officers. The findings reveal three interconnected gaps: (1) a substantive gap, where the absence of a lex specialis for cyberbullying forces reliance on general defamation provisions in the UU ITE and KUHP; (2) a structural gap, characterized by limited digital forensic capacity, inadequate human resources, and evidentiary difficulties in proving mens rea in digital environments; and (3) a cultural and procedural gap, where the justice system prioritizes retributive verdicts (pro justitia) over restorative justice, neglecting victim rehabilitation and psychological recovery. These gaps form a self-perpetuating cycle of dysfunction that undermines victim protection. The study concludes that achieving "Justice Beyond the Verdict" requires comprehensive legal reform, enhanced institutional capacity, and a paradigm shift toward victim-centered restorative justice in Indonesia's cyberbullying enforcement framework

Keywords: cyberbullying, criminal law enforcement, victim protection, legal gaps, Makassar City, restorative justice.

Submitted: 09 August 2026	Accepted: 07 September 2026	Published: 26 September 2026
----------------------------------	------------------------------------	-------------------------------------

INTRODUCTION

The rapid proliferation of information and communication technologies has fundamentally transformed human interaction, erasing geographical boundaries and enabling instantaneous global connectivity. In Indonesia, this digital revolution has been particularly pronounced. Based on reports from the Indonesian Internet Service Providers Association (APJII) and global digital insights platforms such as Hootsuite and IPSOS, internet penetration has surged exponentially over the past decade, with a significant majority of the population actively engaging in social media ecosystems. Platforms like Instagram, TikTok, Twitter, and Facebook have become integrated into daily life, serving as primary conduits for socialization, commerce, and self-expression (Kowalski et al., 2012; Wall, 2007).

However, this unprecedented connectivity harbors a darker consequence: the rise of cyberbullying. Defined as an aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly and over time against a victim who cannot easily defend him or herself, cyberbullying represents a distinct evolution from conventional bullying (Olweus, 1993; Slonje & Smith, 2008; Willard, 2007). Unlike traditional physical or verbal harassment, digital aggression transcends the limitations of physical space and time. As Tokunaga (2010) synthesizes, cyberbullying victimization follows victims "home from school," creating a persistent, inescapable digital environment of fear. Vandebosch and Van Cleemput (2008) and Menesini and Nocentini (2009) further emphasize that the defining features of this phenomenon anonymity, rapid dissemination, and the permanence of digital footprints make it qualitatively more damaging than its offline counterpart. The digital disinhibition effect (Suler, 2004) lowers psychological barriers for perpetrators, enabling cruelty that would rarely occur in face-to-face interactions.

The urgency of this issue is not merely a theoretical construct; it manifests starkly in the local context of Makassar City, South Sulawesi. The region has become a poignant epicenter of the crisis, where the offline and online worlds collide with devastating consequences. The city has witnessed a series of highly viral, traumatic incidents that underscore the fragility of child protection in the digital age. In one seminal case, a video circulating widely on social media showed an adult mother physically assaulting an elementary school student inside a classroom, acting on a misguided assumption of misbehavior. This act of *eigenrichting* (vigilante justice) was not only a physical crime but quickly morphed into a mass cyberbullying spectacle, amplifying the trauma for the child. Another harrowing case involved the viral spread of a video depicting an adult man, Firdaus, physically bullying a 12-year-old boy selling *jalangkote* in Pangkep, an incident that rapidly spread through Facebook groups and Makassar-based information accounts. Most recently, a viral video captured the shocking physical abuse of a disabled junior high school student in Makassar, where the perpetrators kicked the victim in the head. This case, which was immediately reported to the Makassar Police (Report No. 1091/VI/2024/POLDA SULSEL/Restabes Mks), highlighted how offline violence is quickly repackaged and spread online, causing systemic humiliation and mental anguish. These cases collectively illustrate that Makassar is a litmus test for Indonesia's capacity to protect its citizens, particularly its youth, from the intertwined threats of physical violence and digital pervasiveness.

In response to the growing threat of digital crime, Indonesia has constructed a normative legal framework. The primary instruments include the Electronic Information and Transactions Law (UU ITE, Law No. 11 of 2008, as amended by Law No. 19 of 2016), the Criminal Code (KUHP), and the Child Protection Law (Law No. 23 of 2002, revised by Law No. 35 of 2014). These regulations theoretically provide a basis for criminalizing harmful online behaviors, ranging from defamation and hate speech to threats and the distribution of immoral content (Wahid & Labib, 2004; Gillespie, 2019).

Despite this legal architecture, a profound paradox persists. The existing laws are fundamentally general in nature. They criminalize specific acts such as defamation (Pasal 310 KUHP) or distribution of offensive content (Pasal 27 ayat (3) UU ITE) but they fail to recognize cyberbullying as a distinct, autonomous criminal offense. This lack of a *lex specialis* creates a legal vacuum, violating the strict legality principle (*nullum crimen, nulla poena sine lege*) which demands precise and unambiguous legal definitions (Aiman El & Samara, 2016; Kasidin & Wiragama, 2022). Consequently, law enforcement relies heavily on judicial interpretation, leading to inconsistent application and potential misuse of "multitafsir" (multiple interpretations) articles, particularly concerning defamation and hate speech (Marpaung & Sazali, 2025; Aprilianti, 2025).

Furthermore, this normative structure cultivates a culture of "Partial Enforcement". As Wall and Williams (2007) argue, policing cybercrime often struggles to move beyond reactive measures. In the Indonesian context, the justice system tends to hyper-focus on the procedural outcome: the apprehension and sentencing of the perpetrator (the Verdict). While this satisfies the formal requirements of criminal justice, it systematically neglects the substantive needs of the victim namely, psychological recovery, social rehabilitation, and financial restitution (the Justice) (Citron, 2014). This narrow focus on retribution rather than restoration leaves victims of cyberbullying in Makassar doubly victimized: first by the perpetrator, and second by a legal system that processes the crime but offers little to heal the scars left by relentless digital harassment.

The existing body of literature on cyberbullying in Indonesia has predominantly examined the phenomenon through national or psychological lenses. Studies such as those by Noviana (2024) and Palallo and Jannah (2024) offer valuable kriminologis insights into the behavioral patterns and social causes of cyberbullying among adolescents in Makassar. Similarly, Asrum, Thalib, and Jannah (2024) explore the general criminological contours of the phenomenon. While these works are foundational, they do not specifically dissect the operational, structural, and cultural barriers that impede effective law enforcement in practice at the local level. Other relevant research, such as that by Qarolina, Zainuddin, and Hambali (2025) on data breaches, Nur, Said, and Mursyid (2025) on revenge porn, and Safitri, Arif, and Hambali (2025) on defamation during elections, addresses adjacent issues but does not holistically analyze the specific systemic dysfunction that prevents victim protection in cyberbullying cases within a defined locality like Makassar.

Thus, the novelty of this research lies in its focused, localized systemic analysis. This study moves beyond simply describing cyberbullying as a social ill. It applies Lawrence M. Friedman's theory of the legal system dissecting the interplay between legal structure (institutions), legal substance (norms), and legal culture (values) to pinpoint the precise "gaps" that undermine victim protection in Makassar. By integrating this with Soerjono Soekanto's five factors of law enforcement, this research provides a comprehensive diagnostic of why the promise of legal protection often fails to translate into tangible justice for victims.

In line with the preceding analysis, this article aims to answer the following research questions:

1. How are the normative frameworks for cyberbullying implemented in Makassar City?
2. What are the structural, substantive, and cultural gaps that hinder the effective protection of cyberbullying victims in Makassar City?

Thus, the objective of this study is to critically examine the implementation of cyberbullying laws in Makassar and to formulate a comprehensive understanding of the systemic obstacles that perpetuate the gap between legal verdicts and actual justice for victims.

To effectively analyze the legal gaps in Makassar, it is imperative to establish a precise conceptual distinction between traditional bullying and its digital variant, cyberbullying. Olweus (1993) initially codified bullying as a form of aggressive behavior characterized by intentionality, repetition, and an imbalance of power. However, the transition to digital spaces fundamentally alters these dynamics. As articulated by Kowalski, Giumetti, Schroeder, and Lattanner (2014) in their critical meta-analysis, cyberbullying introduces unique parameters: the anonymity of the perpetrator, the rapid and massive scale of dissemination, and the permanence of digital content. Unlike a punch or a verbal insult, which occurs and then stops, a defamatory post, a humiliating video, or a private image shared without consent can exist in perpetuity on the internet, continuing to victimize the individual indefinitely. The online disinhibition effect (Suler, 2004) further complicates the issue, as the lack of physical cues and empathy in digital interactions emboldens perpetrators to engage in behaviors they would typically restrain in offline social settings.

The consequences of cyberbullying are profoundly multidimensional and significantly more severe than commonly recognized. Nixon (2014) provides compelling evidence that victims exhibit higher rates of depression, anxiety, loneliness, and suicidal ideation. This psychological toll is not merely abstract; Hinduja and Patchin (2010) have established a direct and alarming correlation between cyberbullying and increased suicide risk among adolescents. The subjective experience of social exclusion and digital humiliation engages neural pathways associated with physical pain, as demonstrated by Eisenberger, Lieberman, and Williams (2003) in their foundational fMRI study. Beyond internal psychological states, the impact cascades into social isolation (Patchin & Hinduja, 2018) and reputational destruction, particularly as children and adolescents are the most vulnerable demographic (Livingstone & Smith, 2014; Agustin & Budi Kumala, 2020).

This understanding compels a paradigm shift in legal discourse. The harm inflicted by cyberbullying extends beyond the formal criminal act of "defamation" or "insult." It strikes at the core of a person's dignity, social identity, and mental health. Therefore, victim protection cannot be satisfied merely by convicting and punishing the offender. Effective protection must encompass restitution (compensation for financial and moral losses), psychological rehabilitation, and the restoration of the victim's social standing. As Citron (2014) observes, cyberspace can be a weaponized environment, and the legal remedies must be robust enough to address the totality of the harm suffered.

To dissect why the legal system in Makassar fails to deliver this comprehensive justice, this study adopts the "Gap" approach, utilizing two complementary and robust theoretical frameworks.

First, Lawrence M. Friedman's (2001) Theory of the Legal System provides the primary analytical lens. Friedman posits that a legal system is an interconnected organism composed of three vital components:

1. Legal Structure: The institutional framework of law the "machinery" that includes police, prosecutors, courts, and their respective organizational hierarchies.
2. Legal Substance: The actual norms, rules, and doctrines the legal content that governs behavior. This includes statutory laws (such as the UU ITE and KUHP) and judicial decisions.
3. Legal Culture: The attitudes, values, and expectations of the public and legal professionals towards the law. This includes the level of trust in the system, awareness of legal rights, and the prevailing professional ethics among law enforcers.

Using this framework, we identify "gaps" by examining the disconnections between these components. For instance, is there a gap between the substance (laws) and the structure (police capacity to investigate digital evidence)? Is there a gap between the legal culture (community willingness to report) and the structure (accessible victim support mechanisms)? This tripartite model allows for a nuanced forensic analysis of why the legal machinery stalls.

Second, to operationalize these gaps on the ground, the research integrates Soerjono Soekanto's (1983) Five Factors of Law Enforcement. Soekanto argues that effective legal enforcement is contingent upon the interplay of:

1. The Legal Substance itself (the quality of the regulations).
2. The Law Enforcement Apparatus (the competence and integrity of officials).
3. Facilities and Infrastructure (technological tools and budget).
4. The Community (public legal awareness and participation).
5. Culture (the prevailing societal values and traditions).

This framework is particularly adept at mapping the practical obstacles faced by Indonesian police, prosecutors, and courts. It highlights that even with an optimal substance, a lack of digital forensic facilities or a weak legal culture among the populace can render the law impotent.

Finally, these two frameworks are synthesised to operationalize the core concept of this paper: "Justice Beyond the Verdict." Informed by comparative and doctrinal methodologies (Hutchinson, 2015; Zweigert & Kötz, 1998), this concept posits that true justice in cyberbullying cases is not achieved solely by securing a criminal conviction (the Verdict). A verdict is an abstract formal declaration of guilt. True justice is concrete and restorative; it is realized when the victim is effectively rehabilitated, compensated, and empowered to rebuild their digital and social life (Cheng et al., 2020; Citron & Franks, 2019). By analyzing the interactions between Friedman's structures and Soekanto's operational factors, this study will map the exact locations of the breakdowns that prevent Makassar's justice system from delivering this holistic form of justice.

RESEARCH METHODS

Type and Approach

This study employs a normative legal research (doctrinal) methodology, which is the predominant approach in Indonesian legal scholarship for analyzing the congruence between legal norms and their practical implementation. As Hutchinson (2015) articulates, doctrinal legal research provides a systematic exposition of the rules governing a particular legal category, analyses the relationship between rules, explains areas of difficulty, and predicts future developments. However, recognizing the inherent limitations of a purely text-based analysis in capturing the operational realities of law enforcement, this research adopts a socio-legal or normative-empirical orientation. This integrated approach allows the study to move beyond the black-letter law by incorporating empirical data specifically, qualitative insights from law enforcement practitioners to illuminate the

lived realities of legal implementation (Creswell, 2014; Sugiyono, 2017). This methodological choice is particularly apt for examining the “gaps” between *das Sollen* (the law as it ought to be) and *das Sein* (the law as it is practiced), which is the central analytical focus of this paper.

To conduct a comprehensive and multi-faceted analysis, this research employs three distinct yet complementary legal approaches, as is standard in doctrinal research (Zweigert & Kötz, 1998):

1. The Statute Approach (Statute Approach): This involves a systematic and critical examination of all relevant positive laws governing cyberbullying and victim protection. The primary legislative instruments scrutinized include the Electronic Information and Transactions Law (UU ITE), the Indonesian Criminal Code (KUHP), and the Child Protection Law. The analysis focuses on interpreting the literal meaning of the provisions, identifying legal definitions, delineating the elements of each offense, and assessing the coherence and consistency of the normative framework. This approach is essential to determine the substance of the law that law enforcement officers are mandated to apply.
2. The Conceptual Approach (Conceptual Approach): This approach delves into the legal doctrines, principles, and concepts that underpin the positive law. It involves analyzing the theoretical constructs of cyberbullying, victim protection, criminal liability, and the principles of legal enforcement as developed in legal scholarship. By engaging with the works of legal theorists such as Lawrence M. Friedman and Soerjono Soekanto, this approach provides the analytical vocabulary and theoretical lenses such as the “Gap” approach necessary to critique the existing legal framework and propose normative improvements. It ensures that the analysis is not merely descriptive but is grounded in robust jurisprudential reasoning.
3. The Case Approach (Case Approach): This involves the examination of judicial decisions (jurisprudence) that have adjudicated cases related to online defamation, harassment, or other cybercrimes that may serve as proxies for cyberbullying. The focus is on several decisions from the Makassar District Court (Pengadilan Negeri Makassar), particularly Decision No. 515/Pid.Sus/2023/PN.Mks, as well as other relevant decisions from 2025 to 2026. Analyzing these court rulings serves multiple purposes: it reveals how judges interpret and apply the relevant statutes in concreto, illustrates the evidentiary standards applied in practice, and exposes patterns of judicial reasoning that may indicate a gap between legislative intent and judicial outcomes. This approach is vital for understanding how the “Verdict” component of justice is operationalized in local courtrooms.

Data Sources

The validity and reliability of this legal research are anchored in the use of three distinct categories of legal materials, as is standard in doctrinal research (Hutchinson, 2015).

1. Primary Legal Materials: These are the authoritative legal sources that are binding and form the core of the normative analysis. They consist of:
 - Law No. 11 of 2008 concerning Electronic Information and Transactions (UU ITE) as the foundational cyber law.
 - Law No. 19 of 2016 concerning the Amendment to Law No. 11 of 2008 on Electronic Information and Transactions, which introduced significant changes to criminal provisions.
 - Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions, representing the most recent legislative response to digital crime.
 - The Indonesian Criminal Code (Kitab Undang-Undang Hukum Pidana / KUHP), specifically provisions concerning defamation (Pasal 310), insult (Pasal 315), and coercion (Pasal 335) which are often used in cyberbullying prosecutions.
 - Law No. 23 of 2002 concerning Child Protection, as amended by Law No. 35 of 2014, which provides a specific legal framework for safeguarding children from all forms of violence, including in digital spaces.
 - Regulation of the Minister of Communication and Informatics No. 5 of 2020 concerning Private Electronic System Providers, which regulates the obligations of digital platforms.
 - These primary sources provide the legal substance (in Friedman's terms) that defines the rights, obligations, and prohibitions relevant to cyberbullying.
2. Secondary Legal Materials: These materials provide explanation, interpretation, and analysis of the primary legal materials. They are essential for understanding the context, application, and doctrinal development of the law. For this research, secondary sources include:

- Academic textbooks and monographs on criminal law, cybercrime, victimology, and law enforcement.
- Peer-reviewed journal articles, both national and international, that discuss cyberbullying, cyber law, victim protection, and the application of the UU ITE and KUHP.
- Previous research, including theses and dissertations, that are relevant to the subject matter.
- Judicial decisions (jurisprudence), particularly those from the Makassar District Court, which serve as a crucial bridge between abstract norms and concrete legal practice.
- Tertiary Legal Materials: These are supporting sources that aid in the interpretation and understanding of the primary and secondary materials. They include:
 - Legal dictionaries and encyclopedias to clarify the meaning of technical legal terms.
 - Academic commentaries and official academic texts (naskah akademik) accompanying the drafting of legislation, which provide insight into legislative intent.
 - Online databases and portals for retrieving legislation and court decisions, such as the official Indonesian state gazette website and the Supreme Court directory of decisions.
- A distinctive and valuable feature of this research, which elevates it from purely doctrinal analysis, is the inclusion of qualitative empirical data collected through semi-structured interviews with a law enforcement officer from the Women and Children Services Unit (Unit PPA) of the Makassar City Police (Polrestabes Makassar). This tertiary data source provides a "ground-level" perspective on the practical challenges faced by investigators in handling cyberbullying cases, including issues of digital evidence, victim cooperation, and inter-agency coordination. The inclusion of this practitioner's voice is critical for identifying the structural and cultural gaps that are often invisible in the text of statutes or judicial opinions.

Analytical Technique

The analytical framework adopted for this research is prescriptive and qualitative, utilizing a deductive reasoning method. This approach is appropriate for normative legal research, which seeks not only to describe the law but also to evaluate it and formulate recommendations for reform.

The analytical process proceeds in a structured, systematic sequence:

- Systematization of Legal Materials: All collected legal materials are systematically organized and categorized based on their relevance to the two research questions: (1) the normative framework for enforcement, and (2) the obstacles faced in practice. This involves grouping primary regulations, secondary literature, court decisions, and interview transcripts into coherent thematic clusters.
- Interpretation and Analysis of Norms: The primary legal materials are subjected to close textual and teleological interpretation. This involves not only reading the literal text of the provisions but also examining their intended purpose, the legal principles they embody, and their relationship with other norms. This step is guided by the Conceptual Approach and supported by doctrinal insights from secondary literature. The aim is to derive a clear picture of the ideal legal framework (das Sollen).
- Application to Practice (The Gap Analysis): The interpreted norms are then set against the empirical realities revealed by the court decisions and the interview data. This is the core of the "Gap" analysis. The study assesses the degree to which the ideal legal framework is reflected in actual practice (das Sein). For example, does the legal procedure for digital evidence collection (as prescribed in law) align with the actual capacity of the police (as revealed in interviews)? Do the judicial decisions consistently apply the doctrinal interpretations of the relevant articles? This step systematically identifies the structural, substantive, and cultural gaps.
- Prescriptive Evaluation and Argumentation: Drawing on the identified gaps, the research formulates critical arguments. This involves evaluating the effectiveness and fairness of the current system, pinpointing the root causes of dysfunction, and arguing for necessary changes. This is where the concept of "Justice Beyond the Verdict" is operationalized, as the analysis moves from a critique of the status quo towards a vision of a more responsive and restorative legal system.
- Conclusion Drawing: Finally, conclusions are drawn deductively, moving from the general principles of the theoretical framework and the established facts of the case to specific answers to the research questions. This ensures that the findings are logically derived from the evidence and contribute to a coherent understanding of the challenges and opportunities for improving cyberbullying law enforcement in Makassar.

RESULTS AND DISCUSSION

The Normative Framework for Cyberbullying Enforcement in Makassar

The foundation of any criminal justice response is the clarity and specificity of the applicable legal norms. In the context of cyberbullying in Makassar, the normative framework is fragmented and relies on general provisions that were not designed to address the unique characteristics of digital harassment. The primary legal instruments utilized by law enforcement agencies in Makassar are the Electronic Information and Transactions Law (UU ITE) and the Indonesian Criminal Code (KUHP). Specifically, Pasal 27 ayat (3) of the UU ITE, which prohibits the intentional and unauthorized distribution or transmission of electronic information containing insult or defamation, serves as the primary statutory basis for prosecuting online harassment (Agustin & Michael, 2022; Zhafira et al., 2023). This is often complemented by provisions in the KUHP, such as Pasal 310 (defamation), Pasal 311 (slander), and Pasal 315 (minor insult), which provide additional, albeit antiquated, frameworks for addressing attacks on honor and reputation (Lingga et al., 2022; Guntik & Yustiawan, 2022).

The practical application of these norms is most clearly illustrated through an analysis of judicial decisions from the Makassar District Court (Pengadilan Negeri Makassar). An examination of Decision No. 515/Pid.Sus/2023/PN.Mks, along with subsequent cases from 2025 to 2026 (including Nos. 31/Pid.Sus/2025/PN.Mks, 428/Pid.Sus/2025/PN.Mks, 884/Pid.Sus/2025/PN.Mks, 1336/Pid.Sus/2025/PN.Mks, and 1427/Pid.Sus/2025/PN.Mks), reveals a consistent judicial pattern. In these cases, where the underlying facts involved online harassment, bullying, or the non-consensual distribution of personal content, the judges uniformly convicted the defendants using the generic articles of defamation or insult found in the UU ITE and KUHP. The courts did not reference or create a distinct legal category for cyberbullying as a specific offense.

This judicial practice definitively demonstrates the existence of a Substantive Gap. As Clara, Soponyono, and Astuti (2016) have argued, Indonesian criminal law policy has not yet undergone the necessary reform to specifically address cyberbullying. The *nullum crimen sine lege stricta* principle a cornerstone of criminal law that requires offenses to be precisely defined by law is effectively violated by this reliance on general provisions. While judges technically apply the law, the law itself is inadequate. The current legal substance fails to capture the unique elements of cyberbullying, such as its repetitive nature, the power imbalance facilitated by anonymity, and the severe, long-term psychological harm it causes, which distinguishes it from a singular act of defamation (Clara et al., 2016). This lack of a *lex specialis* forces prosecutors and judges into a position of legal interpretation that stretches the original intent of the provisions, creating legal uncertainty and inconsistency in sentencing. The "Verdict" is delivered, but it is grounded in an ill-fitting legal framework that fails to acknowledge the full gravity and specific nature of the digital crime committed.

The Digital Evidence and Capacity Dilemma

The Substantive Gap is compounded by significant Structural Gaps deficiencies in the institutional machinery responsible for enforcing the law. As Friedman (2001) posited, legal structure includes the police, prosecutors, and courts, as well as their capacity to execute their functions. In Makassar, two critical structural weaknesses have been identified.

The Human Resources and Infrastructure Gap

The first and most frequently articulated challenge by law enforcement officials is the severe limitation of human resources (SDM) and infrastructure. In a qualitative interview, an investigator from the Women and Children Services Unit (Unit PPA) of the Makassar Police explicitly stated:

"Salah satu tantangan terbesar kami adalah kurangnya alat bukti digital yang valid serta minimnya saksi. Kadang pelaku sudah menghapus jejak digital sebelum kasus dilaporkan, bahkan akun media sosialnya sudah hilang." ("One of our biggest challenges is the lack of valid digital evidence and the scarcity of witnesses. Sometimes the perpetrators have already erased digital traces before the case is reported, and their social media accounts are already gone.")

This statement reveals a profound infrastructural deficit. Cyberbullying investigations require specialized skills in digital forensics, the ability to trace IP addresses, and tools to recover deleted data. As the UNODC (2022) and Kominfo (2023) have highlighted, the global rise in cybercrime has placed immense pressure on law enforcement agencies to upgrade their technological capabilities. In Makassar, the absence of such advanced forensic tools and the limited number of trained cyber investigators mean that the police are often unable to secure the primary evidence needed to build a case. The ease with which perpetrators can delete content and create anonymous accounts (Wall, 2007; Gillespie, 2019) renders the investigation process extremely difficult from the outset. This

aligns directly with Soekanto's (1983) factor of "Sarana dan Fasilitas" (Facilities and Infrastructure), confirming that even with a clear legal mandate, the absence of necessary tools critically hampers enforcement. This creates a structural dead end: without sophisticated equipment, the police cannot effectively gather evidence; without evidence, they cannot prosecute; without prosecution, the law remains a paper tiger.

The Evidentiary and Liability Gap

A second structural gap relates to the difficulty of proving the elements of the crime in the digital environment. Criminal liability in Indonesian law hinges on proving two elements: the *actus reus* (the guilty act) and the *mens rea* (the guilty mind or intent/negligence). For cyberbullying, establishing both is exceptionally challenging.

The *actus reus* often consists of a series of digital actions posting, sharing, or commenting which can be easily deleted, altered, or obscured. The *mens rea* the required *kesengajaan* (intent) or *kealpaan* (negligence) requires proving the subjective state of mind of the perpetrator. As discussed in the theoretical framework, proving *dolus* (intent) in the digital realm is complicated by the lack of direct witness testimony and the perpetrator's potential claim of hacking or account misuse (Amri & Fatmawati, 2023). The investigator's statement implicitly confirms this, as the lack of digital evidence makes it impossible to prove beyond a reasonable doubt who was behind the keyboard at the time of the offense.

This evidentiary vacuum directly undermines the application of the Theory of Criminal Liability. The doctrinal requirements for proving *dolus* or *culpa* (negligence) which include establishing the actor's knowledge and will to achieve a prohibited consequence become nearly impossible to satisfy without robust digital forensic evidence. The problem is compounded by the online disinhibition effect (Suler, 2004), where perpetrators may not even consciously consider the legal consequences of their actions, making it harder to establish *mens rea* in the traditional sense. Therefore, the structural lack of digital investigative capacity directly prevents the legal system from accurately applying the principles of criminal responsibility, creating a scenario where perpetrators can act with impunity simply by being technologically savvy enough to cover their tracks.

Cultural and Procedural Gaps: The "Forgotten Victim" Syndrome

The most profound gap exposed by this research is the Cultural and Procedural Gap, which directly implicates the core concept of "Justice Beyond the Verdict." The current system is overwhelmingly oriented towards *pro justitia* the formalistic process of identifying, prosecuting, and punishing the perpetrator. While necessary, this hyper-focus on the "Verdict" often comes at the expense of the "Justice" required by the victim.

The Neglect of Victim Protection

Data from the interviews and the reviewed literature reveals that victims of cyberbullying in Makassar face a system that is ill-equipped to address their suffering. The investigator's interview revealed a critical insight:

"Saat ini fasilitas yang kami miliki masih terbatas, terutama dalam hal pendampingan psikologis terhadap korban. Kami bekerja sama dengan instansi lain seperti Dinas Sosial, namun idealnya ada unit pendampingan tetap dan ruang khusus untuk korban." ("Currently, our facilities are still limited, especially in terms of psychological support for victims. We cooperate with other agencies like the Social Service, but ideally there should be a permanent support unit and a special room for victims.")

This statement highlights a systemic failure to prioritize victim welfare. The law focuses on punishing the offender but provides no formal mechanism within the criminal justice process for psychological assessment, trauma healing, or long-term social reintegration for the victim (Aradhana & Pangaribuan, 2022; Laena & Riswadi, 2022). Victims are treated as mere witnesses in the prosecution of the state against the perpetrator, rather than as individuals who have suffered a serious violation of their rights and require comprehensive support.

Restorative Justice vs. Retributive Verdict

The prevailing legal culture, as observed in Makassar, is heavily retributive. The primary metric of success is a conviction a "Verdict." However, for the victim of cyberbullying, a verdict does little to heal the psychological scars, restore their social reputation, or compensate for the material and emotional losses suffered (Wahanisa et al., 2021; Anggraini et al., 2024). As Citron (2014) powerfully argues, the harm caused by online hate is not a fleeting event; it is a deeply invasive and lasting injury.

The limited provision of psychological support and the lack of a formalized restorative justice process in such cases mean that victims are left to cope with their trauma alone. The social stigma of being a victim of online harassment, compounded by a community culture that often engages in victim blaming (where the victim is implicitly blamed for the harassment they received), further isolates and harms them. This creates a profound "Justice Gap." The state delivers a verdict on behalf of the people (pro justitia), but it fails to deliver justice to the person who needs it most. This gap is the fundamental tragedy of the current system: it processes the crime but abandons the victim.

Why Enforcement Fails in Makassar

The analysis thus far demonstrates that the failure of the Makassar legal system to effectively respond to cyberbullying is not a product of a single deficiency but of a toxic interplay between the three identified gaps: Substantive, Structural, and Cultural. These gaps do not exist in isolation; they reinforce each other in a self-perpetuating cycle of dysfunction.

Cycle of Dysfunction:

- **Substance Structure:** The Substantive Gap the absence of a specific law for cyberbullying directly causes structural difficulties. The vague and general provisions of the UU ITE and KUHP provide no clear guidance on what constitutes a cyberbullying offense, what evidence is required, or how to weigh digital evidence. This ambiguity forces police and prosecutors into complex interpretive exercises, making it difficult to build a solid, prosecutable case and leaving them reliant on digital evidence. When the police then lack the equipment (Structural Gap) to secure this crucial evidence, the case often collapses.
- **Structure Culture:** The structural failures (lack of evidence, inability to identify perpetrators) lead to a culture of disillusionment. The investigator's lament about disappearing accounts and deleted posts is a symptom of this. When communities in Makassar repeatedly see that reporting cyberbullying often results in no meaningful action due to evidentiary issues, they become disenchanted with the legal system. This fosters a culture (as per Friedman and Soekanto) of low legal awareness and a reluctance to report. Many victims choose to suffer in silence rather than navigate a complex, intimidating process with an uncertain outcome, further exacerbating the problem.
- **Culture Substance & Structure:** This culture of underreporting and low public trust creates a feedback loop that affects both substance and structure. A low number of reported cases gives policymakers the false impression that cyberbullying is not a serious problem in Makassar, reducing the political impetus to reform the substantive law (creating a new *lex specialis*). Simultaneously, the lack of reported cases can reduce the pressure on the government to allocate more funding for police infrastructure and training, perpetuating the structural deficiencies.

This vicious cycle is visualized in the conceptual framework from the original thesis. It demonstrates how the systemic breakdown begins with a generic law that is ill-suited to the crime, which leads to evidentiary and capacity problems for the police, which erodes public confidence, and ultimately enables the rampant growth of cyberbullying without any effective legal deterrent or victim protection.

By failing to address the interplay of these gaps, the system becomes trapped in a state of equilibrium where it can issue verdicts in only the most straightforward, exceptionally well-documented cases but is systemically incapable of providing comprehensive protection and restorative justice for the vast majority of victims. The promise of Justice Beyond the Verdict remains an unfulfilled aspiration.

CONCLUSIONS

This study concludes that criminal law enforcement against cyberbullying in Makassar City remains ineffective due to three interconnected gaps: substantive, structural, and cultural-procedural. The substantive gap arises from the absence of specific criminal provisions addressing cyberbullying, forcing law enforcement authorities to rely on general regulations under the UU ITE and KUHP that inadequately address the repetitive, anonymous, and psychological dimensions of digital harassment. Structural limitations, including insufficient digital forensic facilities, inadequate investigator training, and limited human resources, further complicate evidence collection and prosecution. Meanwhile, the criminal justice system prioritizes offender punishment while neglecting victims' psychological recovery, rehabilitation, and restitution. These interconnected weaknesses undermine public trust, discourage reporting, and perpetuate ineffective enforcement. The findings emphasize

that achieving "Justice Beyond the Verdict" requires clearer legal provisions, stronger institutional capacity, improved digital investigation capabilities, and victim-centered mechanisms that integrate psychological support, rehabilitation, and restorative justice. Ultimately, effective cyberbullying enforcement must extend beyond criminal convictions to ensure comprehensive legal protection, victim recovery, and meaningful access to justice.

BIBLIOGRAPHY

- Agustin, I. S. U. N., & Michael, T. (2022). Pencemaran nama baik oleh warganet dalam Pasal 27 Ayat (3) Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. *Court Review*, 2 (4), 26. <https://doi.org/10.69957/cr.v2i04.354>
- Agustin, S., & Budi Kumala, A. P. (2020). Dampak cyberbullying pada remaja di media sosial. *Alauddin Scientific Journal of Nursing*.
- Aiman El, A., & Samara, M. (2016). Cyberbullying and the law: A review of psychological and legal challenges. *Computers in Human Behavior*, 65, 127–141. <https://doi.org/10.1016/j.chb.2016.08.012>
- Amri, A. I., & Fatmawati, N. (2023). Criminal liability of online money lenders. *Journal of Law Theory and Law Enforcement*, 122. <https://doi.org/10.56943/jlte.v2i1.275>
- Anggraini, D. K., H, M. R. F., S, T. S., & D, S. P. (2024). Peran Undang-Undang Perlindungan Anak dalam mengatasi bullying di sekolah. 1 (4), 17. <https://doi.org/10.62383/humif.v1i4.559>
- Aprilianti, A. (2025). Efektivitas dan implementasi Undang-Undang Informasi dan Transaksi Elektronik sebagai hukum siber di Indonesia: Tantangan dan solusi. *Begawan Abioso*, 15 (1), 41. <https://doi.org/10.37893/abioso.v15i1.1002>
- Aradhana, A. A. A., & Pangaribuan, C. S. (2022). Cyberbullying in media social: A mainstreaming the victim protection principles in Indonesian criminal justice system. *Indonesia Media Law Review*, 1 (2). 2829-7628.
- Asrum, M. I., Thalib, H., & Jannah, M. (2024). Criminological review of the phenomenon of cyberbullying. *Horizon Public Legal Studies*, 1 (1), 32–49. <https://doi.org/10.56087/hegels.v1i1.490>
- Cheng, L., Hu, X., Matulewska, A. E., & Wagner, A. (2020). Exploring cyberbullying: A socio-semiotic perspective. *International Journal of Legal Discourse*, 5 (2).
- Chung, Y. (2021). Cyberbullying regulation and social media control in South Korea. *Asian Journal of Comparative Law*, 16 (2), 321–340.
- Citron, D. K. (2014). *Hate crimes in cyberspace*. Harvard University Press.
- Citron, D. K., & Franks, M. A. (2019). The Internet as a speech machine and a weapon. *Fordham Law Review*, 87 (1), 231–260.
- Clara, F., Soponyono, E., & Astuti, E. S. (2016). Kebijakan hukum pidana dalam upaya penanggulangan cyberbullying dalam upaya pembaharuan hukum pidana. *Diponegoro Law Journal*, 5 (3).
- Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). SAGE Publications.
- Eisenberger, N. I., Lieberman, M. D., & Williams, K. D. (2003). Does rejection hurt? An fMRI study of social exclusion. *Science*, 302 (5643), 290–292. <https://doi.org/10.1126/science.1089134>
- Friedman, L. M. (2001). *The legal system: A social science perspective*. Russell Sage Foundation.
- Gillespie, A. A. (2019). *Cybercrime: Key issues and debates* (2nd ed.). Routledge.
- Guntik, D. S., & Yustiaawan, D. G. P. (2022). Corporations as whistleblowers in the crime of defamation based on the electronic and transaction information act. *Policy Law Notary and Regulatory Issues (POLRI)*, 1 (1), 65. <https://doi.org/10.55047/polri.v1i1.43>
- Hinduja, S., & Patchin, J. W. (2010). Bullying, cyberbullying, and suicide. *Archives of Suicide Research*, 14 (3), 206–221. <https://doi.org/10.1080/13811118.2010.494133>
- Hinduja, S., & Patchin, J. W. (2015). *Bullying beyond the schoolyard: Preventing and responding to cyberbullying* (2nd ed.). Corwin Press.
- Hutchinson, T. (2015). The doctrinal method: Incorporating interdisciplinary methods in reforming the law. *Tilburg Law Review*, 20 (2), 130–163.
- Kasidin, S., & Wiragama, R. (2022). Kebijakan UU ITE dalam mengatasi tindak pidana pelaku cyber bullying (perundungan dunia maya) di social media. *Focus Journal of Law*, 2 (2), 118. <https://doi.org/10.47685/focus.v2i2.305>

- Kitab Undang-Undang Hukum Pidana (KUHP). (Staatsblad Tahun 1915 Nomor 732 sebagaimana telah beberapa kali diubah dan ditambah).
- Kominfo. (2023). National cybersecurity annual report 2023. Ministry of Communication and Information of the Republic of Indonesia.
- Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin*, 140 (4), 1073–1137. <https://doi.org/10.1037/a0035618>
- Kowalski, R. M., Limber, S. P., & Agatston, P. W. (2012). *Cyberbullying: Bullying in the digital age* (2nd ed.). Wiley-Blackwell.
- Laena, M., & Riswadi. (2022). Legal protection for child victims of cyber bullying. *Proceeding of the 2nd International Conference on Law, Social Science, Economics, and Education (ICLSSEE)*. <https://doi.org/10.4108/eai.16-4-2022.2319752>
- Lingga, J., Sastro, M., & Bahreisy, B. (2022). Penerapan keadilan restoratif terhadap tindak pidana pencemaran nama baik. *Suloh Jurnal Fakultas Hukum Universitas Malikussaleh*, 10 (2), 560. <https://doi.org/10.29103/sjp.v10i2.9135>
- Livingstone, S., & Smith, P. K. (2014). Annual research review: Harms experienced by child users of online and mobile technologies. *Journal of Child Psychology and Psychiatry*, 55 (6), 635–654.
- Marpaung, H. W., & Sazali, H. (2025). Multitafsir UU ITE sebagai koridor hukum: Studi pada intensitas user conflicts di media sosial. *Jurnal Indonesia Manajemen Informatika Dan Komunikasi*, 6 (2), 1439. <https://doi.org/10.63447/jimik.v6i2.1438>
- Menesini, E., & Nocentini, A. (2009). Cyberbullying definition and measurement: Some critical considerations. *Journal of Psychology*, 217 (4), 230–232. <https://doi.org/10.1027/0044-3409.217.4.230>
- Nixon, C. L. (2014). Current perspectives: The impact of cyberbullying on adolescent health. *Adolescent Health, Medicine and Therapeutics*, 5 , 143–158. <https://doi.org/10.2147/AHMT.S36456>
- Noviana, N. (2024). Tinjauan kriminologis mengenai cyberbullying di Kota Makassar. *Ranah Research Journal of Multidisciplinary Research and Development*, 6 (6), 2988. <https://doi.org/10.38035/rrij.v6i6.1166>
- Nur, M. R. A., Said, M. F., & Mursyid, M. (2025). Legal analysis of criminal responsibility of revenge porn perpetrators in the protection of victims' personal data. *Horizon Public Legal Studies*, 1 (2). <https://doi.org/10.56087/hegels.v1i2.942>
- Olweus, D. (1993). *Bullying at school: What we know and what we can do*. Blackwell.
- Palallo, P. P., & Jannah, M. (2024). Tinjauan kriminologis terhadap perundungan anak di Kota Makassar. *Qawanin Jurnal Ilmu Hukum*, 4 (2), 79–93. <https://doi.org/10.56087/qawaninjih.v4i2.302>
- Patchin, J. W., & Hinduja, S. (2018). Cyberbullying: Review of an old problem gone viral. *Journal of Adolescent Health*, 63 (4), 1–6.
- Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Privat. (Berita Negara Republik Indonesia Tahun 2020 Nomor 548).
- Qarolina, N. C., Zainuddin, Z., & Hambali, A. R. (2025). Perlindungan hukum bagi korban penyebaran data yang diretas secara ilegal melalui link phishing. *Legal Dialogica*, 1 (1), 11–24. <https://jurnal.fh.umi.ac.id/index.php/legal/article/view/1580>
- Safitri, A. A., Arif, M., & Hambali, A. R. (2025). Tinjauan yuridis terhadap tindak pidana memfitnah dalam tahapan kampanye pemilihan kepala daerah. *Legal Dialogica*, 1 (1), 11–25. <https://jurnal.fh.umi.ac.id/index.php/legal/article/view/1660>
- Slonje, R., & Smith, P. K. (2008). Cyberbullying: Another main type of bullying? *Scandinavian Journal of Psychology*, 49 (2), 147–154.
- Soekanto, S. (1983). Faktor-faktor yang mempengaruhi penegakan hukum. *Rajawali Pers*.
- Sugiyono. (2017). *Metode penelitian kuantitatif, kualitatif, dan R&D*. Alfabeta.
- Suler, J. (2004). The online disinhibition effect. *CyberPsychology & Behavior*, 7 (3), 321–326. <https://doi.org/10.1089/1094931041291295>
- Tokunaga, R. S. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimisation. *Computers in Human Behavior*, 26 (3), 277–287. <https://doi.org/10.1016/j.chb.2009.11.014>

- Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843).
- Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952).
- Undang-Undang Republik Indonesia Nomor 23 Tahun 2002 tentang Perlindungan Anak. (Lembaran Negara Republik Indonesia Tahun 2002 Nomor 109, Tambahan Lembaran Negara Republik Indonesia Nomor 4235).
- Undang-Undang Republik Indonesia Nomor 35 Tahun 2014 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2002 tentang Perlindungan Anak. (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 297, Tambahan Lembaran Negara Republik Indonesia Nomor 5606).
- UNODC. (2022). The global threat of cybercrime: A report on current challenges. United Nations Office on Drugs and Crime.
- Vandebosch, H., & Van Cleemput, K. (2008). Defining cyberbullying: A qualitative research into the perceptions of youngsters. *CyberPsychology & Behavior*, 11 (4), 499–503. <https://doi.org/10.1089/cpb.2007.0042>
- Wahanisa, R., Prihastuty, R., & Noho, M. D. H. (2021). Preventive measures of cyberbullying on adolescents in Indonesia: A legal analysis. *Lentera Hukum*, 8 (2), 267. <https://doi.org/10.19184/ejhlh.v8i2.23503>
- Wahid, A., & Labib, M. (2004). *Cyber crime*. Refika Aditama.
- Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.
- Wall, D. S., & Williams, M. L. (2007). Policing cybercrime: Networked and social control. *Policing and Society*, 17 (3), 305–323.
- Willard, N. E. (2007). *Cyberbullying and cyberthreats: Responding to the challenge of online social aggression, threats, and distress*. Research Press.
- Zhafira, I., Ismansyah, I., & Yoserwan, Y. (2023). Tinjauan yuridis tindak pidana pencemaran nama baik dalam Kitab Undang-undang Hukum Pidana dikaitkan dengan Pasal 27 Ayat (3) Undang-undang Informasi dan Transaksi Elektronik. *UNES Journal of Swara Justisia*, 7 (3), 901. <https://doi.org/10.31933/ujsj.v7i3.408>
- Zweigert, K., & Kötz, H. (1998). *Introduction to comparative law* (3rd ed., T. Weir, Trans.). Oxford University Press.