Humanities, Society, and Community, Vol. 3 No. 2 (2026) https://doi.org/10.31098/hsc.v3i2.3068

Research Paper

Analysis of Law Enforcement Regarding Fault in Defamation Crimes Through Electronic Media

Diah Pudjiastuti[1]*, Sahat Maruli Tua Situmeang[2]
[1]Internasional Women University, Indonesia
[2]Universitas Komputer Indonesia, Indonesia

Received: February 3, 2025	Revised: January 11, 2026	Accepted: February 4, 2026	Online: May 29, 2026

Abstract

This research investigates the enforcement of defamation laws in electronic media, focusing on the interpretation of "intentional" and "unauthorized" elements under Law No. 1 of 2024, which amends Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law). The urgency of this study arises from legal ambiguities and the rising number of online defamation cases, highlighting inconsistencies in judicial interpretations and enforcement challenges. Using a normative juridical approach, this study analyzes statutory provisions, jurisprudence, and fault theory to assess the practical application of defamation laws. The findings reveal a lack of uniformity in judicial decisions, emphasizing the need for clearer definitions and standardized legal interpretations. This study underscores the necessity of refining existing legal provisions to enhance legal certainty and enforcement effectiveness. Practical implications include increasing public legal awareness of responsible digital communication and implementing preventive measures against cyber defamation. To address legal gaps, this research recommends legislative reforms to clarify legal definitions, promote alternative dispute resolution mechanisms, and strengthen law enforcement training, ensuring a balance between legal protection and freedom of expression in the digital era.

Keywords: *Defamation, Electronic Media, Fault, Mens Rea, Law Enforcement, Digital Evidence, Legal Certainty*

INTRODUCTION

In response to this, the Indonesian government enacted the Electronic Information and Transactions Law (ITE Law) to address emerging challenges in cyberspace, including the rise of online defamation cases. According to Arliman (2017), effective law enforcement is a central element in realizing Indonesia as a state based on law, as mandated by the Constitution. Currently, technological developments are progressing very rapidly.

In Hardinanto's (2019) view, the ITE Law was established as a legal response to these advances in information technology, particularly in the criminal law sphere. Similarly, Putri (2019) emphasizes that the ITE Law reflects the convergence of information and electronic transaction law within the framework of corporate crime regulation under Law No. 11 of 2008 in conjunction with Law No. 19 of 2016.

In line with this, the internet revolution has played a major role in the emergence of social media, which is now widely used to influence and shape public policy and law (Latifah & Najicha, 2022). The Regulation on Information and Electronic Transactions (ITE Law) has been in force since 2008 to regulate activities in cyberspace and, up to 2024, has undergone two amendments: the first through Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 on Electronic Information and Transactions, and the second through Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions.

In Law Number 1 of 2023 concerning the Criminal Code, as well as in the ITE Law, defamation is understood as an attack on a person's honor or good name that targets their sense of self-worth

Corresponding author's email: diahpudjiastuti@iwu.ac.id

or dignity. In Indonesian criminal law, the terms defamation (*pencemaran nama baik*), insult (*penghinaan*), and slander (*fitnah*) refer to related but distinct offenses. Defamation is generally defined as an act that attacks a person's honor or reputation by accusing them of something in a way intended to be known by the public, including through electronic media.

Insult involves offensive or degrading expressions that may not necessarily be false, but are aimed at humiliating or lowering someone's dignity. At the same time, slander more specifically concerns false accusations made with the intent to damage another person's reputation, as reflected in the formulation of fitnah in Article 311 KUHP. Understanding these doctrinal distinctions is essential to ensure accurate legal classification of conduct, consistent application of relevant provisions in the KUHP and ITE Law, and to avoid misinterpretation in court decisions, especially in cases involving criticism and freedom of expression in digital spaces.

Judging from its characteristics, the regulation of defamation in the Criminal Code and in the ITE Law both concern attacks on a person's honor or good name, referring to conduct aimed at degrading or damaging someone's reputation, particularly through defamatory and/or slanderous acts, and which can be committed by anyone against a specific individual. The emergence of these offenses in cyberspace has had a significant impact on the Indonesian criminal justice system, especially in changing the case handling process—from reporting to the police, to evidence collection, which is often constrained by the technical nature of electronic systems and the need for reliable digital forensics (Andria & Saifulloh, 2022).

To the identification of perpetrators, the determination of the locus and tempus delicti in ITE cases (Pakaya & Mahyani, 2022), measures to be taken when electronic evidence has been deleted, the transfer or seizure of electronic devices without systematic procedures, the multiple interpretations of offense formulations in the ITE Law when linked to alleged criminal acts, and non-compliance with the principles governing complaint offenses and ordinary offenses under the ITE Law.

The second amendment to the ITE Law, through Law No. 1 of 2024, was driven by inconsistencies in judicial interpretation and the resulting legal uncertainty, particularly in defamation cases. Prior to this revision, key terms such as "without right" (*tanpa hak*) and the broad wording of defamation provisions were vulnerable to multiple interpretations, which led to disparate court rulings and the use of the law to prosecute social media users merely for expressing opinions, raising concerns about its chilling effect on freedom of expression.

The 2024 amendment seeks to clarify the elements of defamation—now expressly defined as intentionally attacking another person's honor or good name by accusing them of something with the intent that it becomes publicly known through electronic systems—and to promote greater consistency in judicial decision making, while at the same time protecting digital rights and ensuring accountability for genuinely defamatory conduct.

Fault theory plays a crucial role in determining criminal liability in defamation cases. This study adopts fault theory to evaluate how intent (*dolus*) and negligence (*culpa*) affect criminal liability in online defamation, building on the doctrinal understanding of fault developed in Indonesian criminal law scholarship (Marpaung, 2005).

In this framework, punishment is justified only where there is intentional wrongdoing or culpable negligence, so that the offender can fairly be held responsible for the harmful result. Inconsistent application of fault theory in prior court rulings has led to arbitrary enforcement; explicitly integrating fault analysis into judicial interpretation is therefore essential to ensure a more predictable and equitable approach to defamation cases, where the protection of individual rights is balanced against the need for legal accountability.

In this regard, the entire sequence of legal processes against perpetrators of information and electronic transaction crimes lies in the hands of investigators, who receive reports and collect

evidence, followed by law enforcement actions such as arrest, investigation, prosecution, defense, trial, and adjudication as procedural steps to assess whether the elements of the alleged ITE offense are fulfilled.

In Moeljatno's view, criminal liability does not arise merely from the commission of a criminal act; it also requires the presence of fault or a blameworthy mental attitude, encapsulated in the principle "no punishment without fault" (*geen straf zonder schuld, ohne Schuld keine Strafe*) (Moeljatno, 1993). Thus, a criminal act (*strafbaar feit*) cannot be equated with criminal responsibility: the former is grounded in the principle of legality, whereas the latter is based on the principle of fault. Fault (*schuld*) concerns the offender's inner state or mental attitude before or at the time of the act, is inherently attached to the perpetrator, and is therefore a subjective element of criminal responsibility.

The increasing incidence of criminal acts of defamation has led to a rise in cases handled by law enforcement agencies such as the police, prosecutors, and courts, and consequently to growth in the prison population, indicating that the Information and Electronic Transactions Law (UU ITE) has not yet contributed to reducing either the number or frequency of these offenses, as perpetrators are predominantly dealt with through criminal proceedings as the primary—if not sole—response.

Several prior studies have examined defamation through electronic media: Asmadi (2021) analyzes the formulation of offenses and sentencing patterns for defamation on social media and highlights the potential for disparity in the application of Law No. 11 of 2008 on Electronic Information and Transactions (Asmadi, 2021). Alviolita and Arief (2019) discuss policy formulation in defining criminal acts of defamation in the context of Indonesian penal law reform, including comparative insights into how several countries regulate punishable acts and justifying grounds for defamation offenses.

Purnomo (2020) assesses law enforcement of defamation through the media from the perspective of criminal law concepts and emphasizes the alignment among criminalization, societal and cultural values, religious values, and the protection of material and immaterial interests. Muthia and Arifin (2019) examine cybercrime-related defamation cases in Indonesia and conclude that spreading false information that harms a person's reputation may lead to criminal sanctions and fines. Rochman et al. (2021) compare the treatment of defamation through social media in positive criminal law and Islamic criminal law, noting that, outside the Shafi'i school, defamation is generally subject to *ta'zīr* punishment at the discretion of the ruler or judge, while the Shafi'i school analogically prescribes one year of exile.

However, these studies have not specifically analyzed the post-amendment application of fault theory to the elements of "intentionally" and "without right" in cyber defamation provisions, an issue crucial to clarifying judicial reasoning and promoting uniformity in law enforcement (Asmadi, 2021).

Meanwhile, this research focuses on the fulfillment and enforcement of the elements "intentionally" and "without right" in the criminal act of defamation under Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions, examined through the lens of fault theory in order to promote legal certainty. In this respect, the study differs from previous research by specifically addressing, first, how the policy formulation of the elements "intentionally" and "without right" in defamation offenses under Law No. 1 of 2024 can be understood in connection with fault theory, and second, how these elements are applied in practice to defamation through electronic media within the criminal justice process.

Theoretically, the research is expected to strengthen the relevance of fault theory—namely, the requirement that punishment be grounded in culpable intent or negligence—in interpreting cyber defamation and, practically, to offer policy recommendations for more consistent, fair, and

accountable law enforcement practices under the amended ITE Law.

LITERATURE REVIEW

A state based on the rule of law upholds legal principles. It guarantees justice for its citizens, where justice becomes a fundamental condition for creating a harmonious society in which every individual receives fair treatment and can contribute as a responsible member of the community (Kusnardi & Ibrahim, 1988). In this context, Marc Ancel emphasizes that every organized society must possess a legal system comprising criminal law norms and their sanctions, a criminal procedure code, and effective mechanisms for enforcing criminal law (Arief, 2010).

Building upon this foundation, Gustav Radbruch, as quoted by Roeslan Saleh in *Rechtsphilosophie*, emphasizes that the principle of "no punishment without fault" must be upheld. However, a crime is defined, and punishment cannot be imposed without the offender's subjective involvement, in the form of a blameworthy mental state (Wardana, 2023). This principle ensures that criminal responsibility is not assigned arbitrarily, but is grounded in the individual's intention and awareness at the time the offense is committed.

In the context of defamation, Radbruch's philosophy is particularly relevant for assessing whether a defamatory statement was made with the intent to harm another person's reputation or merely resulted from negligence, and Indonesian criminal law itself draws a clear distinction between intentional and unintentional acts in determining liability (Utoyo et al., 2020). The central challenge in digital defamation cases is therefore to establish whether the accused genuinely intended to damage the victim's good name or whether the expression arose without malice, a distinction that is crucial to achieving fair and proportionate judicial outcomes.

Fault theory is a core principle of criminal law that requires criminal liability to be based on culpability, either intent (*dolus*) or negligence (*culpa*). Moeljatno explains this through the maxim *geen straf zonder schuld* (no punishment without fault), which places fault as a necessary condition for imposing criminal responsibility, distinct from the mere occurrence of a prohibited act. Hart further argues that punishment must be proportionate to the degree of blameworthiness, meaning that the severity of sanctions should correspond to the offender's culpable mental state rather than solely to the external act.

In digital defamation cases, fault theory is crucial for assessing whether the accused acted with malicious intent in disseminating defamatory content or whether the act resulted from negligence, without a deliberate intent to harm. Establishing fault functions as a safeguard for personal rights and legal certainty, because imposing criminal sanctions in the absence of provable intent or negligence would conflict with the fundamental requirement that no one be punished without a blameworthy state of mind.

Expanding this discussion, Barda Nawawi Arief clearly distinguishes between criminal acts and fault, arguing that criminal acts are defined in terms of objective conduct. In contrast, the perpetrator's inner attitude belongs to the domain of *schuld* (fault) and criminal responsibility. This view accords with the position that the concept of a criminal act should focus on behavior prohibited by law. In contrast, questions about the perpetrator's mental state, such as intention or negligence, are treated separately within the framework of culpability and accountability.

This perspective parallels Williams' understanding that an act classified as a crime may, in certain circumstances, be objectively innocent if the requisite culpable state of mind is absent, reinforcing the analytical distinction between the wrongful act and the basis for punishment. Consequently, criminal acts concern the external elements of the offense. In contrast, criminal responsibility is tied to individuals' subjective obligation to act lawfully and is evaluated by their mental state at the time of the act.

In Indonesian law, this distinction is particularly important in enforcing the ITE Law's

defamation provisions, where liability often hinges on whether online expressions are accompanied by an intent to damage someone's honor or reputation. The presence or absence of such subjective intent can determine whether a digital communication is treated as punishable defamation or as conduct that, though perhaps improper, does not meet the threshold of criminal responsibility.

Conceptually, Fletcher distinguishes two types of criminal law norms: first, legal norms that define prohibited or mandated conduct, which systematize the various forms of criminal offenses; and second, legal norms that regulate criminal responsibility, which ensure that punishment is imposed only when fault can be established. This dual structure underscores the separation between the descriptive definition of offenses and the evaluative criteria for attributing liability, thereby reinforcing the idea that not every violation of an offense definition automatically entails criminal responsibility.

Within this framework, unlawfulness (*wederrechtelijkheid*) is central alongside the principle of legality, and two principal perspectives can be identified. The formal perspective maintains that unlawfulness constitutes an element of a criminal act only when the statute explicitly includes it, a position associated with writers such as Pompe, who argue that *wederrechtelijkheid* is generally not presumed as an element unless expressly stated.

By contrast, the material perspective treats unlawfulness as an inherent element of every criminal act, whether or not it is textually mentioned in the provision. Supported by scholars such as Vos and Moeljatno, this view posits that a criminal act requires both an unlawful character and a responsible perpetrator, thereby integrating the act's wrongfulness with the assessment of fault and accountability.

According to the material conception of unlawfulness, Hazewinkel Suringa requires that both the unlawful nature of the act and the offender's responsibility be affirmatively demonstrated by the prosecution before punishment may be imposed. If, in the course of this assessment, the act is found to be lawful, for example, because it falls within the protection of a right or a justification ground, the perpetrator cannot be held criminally accountable and must be acquitted.

In Indonesian practice, this requirement is particularly important in defamation cases under the ITE Law, where establishing unlawful intent behind digital expressions is complicated by competing appeals to freedom of expression and the public interest in information, making it difficult to determine when criticism crosses the line into punishable defamation. The more subjective and value-laden these boundaries become, the greater the need for courts to carefully prove both unlawfulness and fault so that criminal sanctions do not unduly restrict legitimate speech.

Within the broader framework of criminal policy, criminalization and decriminalization form key instruments through which legislators respond to changing social conditions and perceptions of harm. Criminalization denotes the process of designating previously lawful conduct as a criminal offense, typically to address new or escalating threats. In contrast, decriminalization removes or relaxes criminal penalties for certain behavior in light of evolving social norms and cost-benefit considerations regarding penal intervention. Legislators are therefore expected to evaluate carefully which societal values, such as personal honor, public order, or economic security, justify the use of criminal law, consistent with its role as *ultimum remedium*.

The Information and Electronic Transactions (ITE) Law serves as the legal framework for regulating electronic transactions, data protection, cybersecurity, and digital intellectual property. It emphasizes that individual rights must be protected from unjustified interference, thereby supporting peace and security in society. In practice, judges have developed guidelines through case law to balance the protection of individual rights with the effective enforcement of the law. Within the judicial process, evidence plays a central role in establishing the truth of disputed claims, and

procedural rules must be strictly followed to ensure that court decisions are final and legally binding (Situmeang, 2022).

According to Rahardjo (2001), the judicial system should function as a last resort for resolving legal disputes because court proceedings tend to be lengthy, formalistic, and rigid; thus, non-penal approaches ought to be prioritized to achieve justice and broader social benefit (Setiyono, 2016). In the context of online defamation, this implies that alternative dispute resolution mechanisms such as mediation or restorative settlements can offer more responsive and constructive outcomes than relying immediately on criminal prosecution (Raharjo, 2001).

The implementation of criminal law policy through penal measures generally proceeds in three stages: a formulation stage in which legislators define and refine legal provisions, an application stage in which law enforcement agencies apply those provisions in concrete cases, and an execution stage in which sanctions are carried out based on final judicial decisions (Arief, 2007). The Information and Electronic Transactions (ITE) Law provides the legal framework for regulating electronic transactions, data protection, cybersecurity, and aspects of digital intellectual property, while also requiring that individual rights be protected from unjustified interference to preserve social order and security (Arief, 2007).

Judges have progressively developed guidelines in case law to balance individual rights with effective enforcement. Within the judicial process, evidence, particularly electronic evidence, plays a central role in establishing the truth of disputed claims, so that only decisions reached through proper procedures can be regarded as final and legally binding (Saad, 2023).

In academic discourse, cybercrime is widely recognized as a complex and evolving concept with no single universally accepted definition. However, many classifications broadly describe it as any crime facilitated or committed using computers, networks, or digital devices. Most contemporary definitions emphasize the central role of information and communication technologies in enabling such offenses, and this evolving conceptualization helps provide greater legal clarity for judges when interpreting and applying cybercrime provisions amid rapid technological change (Sarkar & Shukla, 2024).

One of the major challenges in digital defamation cases concerns evidence collection, because, unlike traditional defamation, where physical documents or oral testimony may predominate, online defamation often relies on electronic records, screenshots, and metadata that are technically easy to alter. These characteristics create significant hurdles for law enforcement and courts in proving both the authenticity of digital evidence and the intent behind online statements, especially when forensic tools are limited or not used systematically (Abdillah, 2023).

Consequently, Indonesia's legal framework needs to continue adapting by incorporating more advanced digital forensic techniques and strengthening cross-border cooperation in cyber investigations to address the transnational and technologically sophisticated nature of such offenses (Sarkar & Shukla, 2024).

Awareness of human dignity should guide the judiciary when addressing privacy violations, especially where digital technologies are involved. Some UK decisions have been criticized for implying that privacy protection alone is sufficient. Whereas a more comprehensive approach places human dignity at the center and treats privacy, reputation, and expression as interests that must all be evaluated through that lens in defamation and privacy cases (Koltay & Wragg, 2020). This perspective is particularly relevant in digital defamation disputes, where courts must carefully balance privacy rights, freedom of expression, and public interest in a way that is sensitive to context rather than mechanically favoring one right over another.

Legal enforcement is not a purely logical or deductive exercise but involves weighing rational arguments against concrete social and situational realities. In this regard, Rizky Ariestandi Irmansyah emphasizes that the function of law is not only to secure legal certainty but also to

uphold human rights and democratic values, so that law remains responsive to societal needs (Irmansyah, 2013). Building on this, Sunarso underscores the importance of a corrective approach that develops legal principles and rules to create fair relationships, enhance justice for victims, and improve the legal system so it evolves in line with changing patterns of victimization and social expectations (Sunarso, 2015).

German legal scholar Hans Joachim Schneider characterizes computer crime as offenses that either use electronic data processing equipment as an instrument of crime or target such equipment and data as the object of the offense. By contrast, legal definitions of defamation focus on the intentional dissemination of false or misleading statements that damage another's reputation, with liability typically requiring demonstrable harm that goes beyond mere insult or subjective offense (Li & Qin, 2018). Although the scope of sanctions and available remedies varies between legal systems, a shared principle is that legal consequences should attach only where reputational harm can be substantiated and causally linked to the defamatory communication (Khalil, 2024).

Law enforcement is an active, dynamic process through which legal norms are translated from abstract rules into concrete decisions and practices, rather than a simple exercise in deductive logic. Within this process, the ITE Law provides a framework for addressing digital misconduct. However, it must be continuously developed to maintain a proper balance between legal certainty, justice, and social utility in an environment of rapidly changing technologies (Li & Qin, 2018). Responding to evidentiary difficulties in digital defamation cases and ensuring that sanctions remain proportionate to the gravity and impact of online speech are therefore central challenges for the future evolution of Indonesian cyber law (Khalil, 2024).

RESEARCH METHOD

This research employs a normative juridical approach, focusing on the analysis of legal norms and judicial reasoning relevant to the fulfillment of the elements "intentionally" and "without rights" in defamation provisions under the ITE Law, and examining how these elements are interpreted and applied in decisions of the Indonesian criminal courts. The research adopts an analytical descriptive design using doctrinal and interpretative methods: the doctrinal method is used to examine statutory provisions such as Law Number 11 of 2008 on Electronic Information and Transactions and its amendments, the Indonesian Criminal Code (KUHP), and procedural regulations governing defamation while the interpretative method explores how judges construe elements of fault in digital defamation cases, guided by fault theory as the primary analytical framework.

A purposive sampling strategy is applied to select court decisions that (1) have significant legal relevance for the development of cyber defamation law, (2) possess precedent-setting value in terms of judicial reasoning or interpretation, and (3) clearly illustrate enforcement challenges or inconsistencies in practice (Juridical Study of Customary Law in the Indonesian National Law System, 2023).

The research employs structured legal analysis comprising: (a) textual analysis of statutory provisions and legislative documents; (b) doctrinal analysis of fault theory and its implications for criminal liability; (c) case law analysis using coding of judicial reasoning, particularly regarding how courts define and apply "intentionally" and "without rights" in their verdicts; and (d) identification of enforcement challenges arising in court practice and prosecutorial discretion (Indonesian Journal of Law and Justice, 2024).

FINDINGS AND DISCUSSION

Policy Formulation of the Implementation of Elements Deliberately and Without Rights in the Crime of Defamation in Law No. 1 of 2024 concerning the Second Amendment to Law

Number 11 of 2008 concerning Information and Electronic Transactions Linked to the Theory of Error

The elements "intentionally" and "without rights" are fundamental to the evidentiary process in ITE crimes because both must be proven to establish criminal liability under the ITE Law. In doctrinal criminal law, intention is treated as a subjective element that reflects the perpetrator's fault. Hence, an ITE offense occurs when a person deliberately commits the prohibited act with awareness of its consequences, consistent with the assumption that users of digital platforms are legally capable subjects possessing cognitive awareness (Hamzah, 2012).

By contrast, the element "without rights" is an objective element that expresses the unlawful character of the conduct, meaning that a person lacks the right or authority to act when the law prohibits the behavior or when it contravenes generally accepted legal principles and societal notions of justice (Hamzah, 2012). In the context of Article 27(3) of the ITE Law, scholarly and judicial interpretations link "without rights" to actions that are unlawful, despicable, or inappropriate, indicating that the actor realizes they are not entitled to distribute, transmit, or make certain electronic information or documents accessible.

Court interpretations of "without rights" have varied significantly, producing inconsistencies in defamation rulings under the ITE Law. In some cases, defendants have been convicted under Article 27(3) despite invoking journalistic freedom or the public's right to know, while in other cases courts have acquitted defendants in similar factual settings on the basis that the statements served the public interest or fell within legitimate criticism, revealing the judiciary's ongoing struggle to balance digital rights such as freedom of expression and press freedom with demands for legal accountability in online defamation cases.

According to the explanatory memorandum (*memorie van toelichting*), deliberate action is understood as a conscious will directed at the commission of a particular offense, so that *opzet* essentially means both knowing and wanting the realization of the act and its consequences. In this context, Pompe distinguishes between "intention," as a specifically directed purpose, and "intentional," as a broader state of awareness. This distinction can create ambiguity in legal analysis when courts must decide which level of mental involvement satisfies the statutory requirement of intent (Hamzah, 2012).

The formulation of "without rights" in the ITE Law is inconsistent. Some provisions use the phrase "without rights," while others use "without rights or against the law," creating room for divergent interpretations in practice. Drawing on Dutch doctrine, Andi Hamzah explains that "against the law" (*wederrechtelijk*) may mean acting "without one's own right" (*zonder eigen recht*), "contrary to the rights of others" (*tegen eens anders recht*), or "contrary to objective law" (*tegen het objectieve recht*), and following Pompe he supports a material rather than purely formal understanding of *wederrechtelijkheid*, in which unlawfulness is assessed against broader legal principles and societal notions of justice, not only against the literal wording of statutes (Hamzah, 2012).

Laden Marpaung notes that Indonesian criminal legislation employs both the terms *wederrechtelijk* and *onrechtmatig*, adding another layer of complexity to the analysis of unlawfulness in penal provisions (Marpaung, 1991). Building on this, Indriyanto Seno Adji observes that the concept of an unlawful act, once confined to a formal reading as merely "contrary to written law" (*wederwettelijk*), has shifted toward a material understanding that encompasses broader violations of legal norms and societal notions of propriety and fairness (Adji, 2009).

The inconsistency in interpreting "without rights" is reflected in divergent outcomes in digital defamation cases. In one decision, a social media user was convicted under defamation provisions despite presenting evidence that the statements were substantially true, with the court reasoning that even truthful statements can be defamatory if they unjustifiably damage a person's

reputation. These contrasting rulings underscore the need for a more standardized interpretative approach to online defamation, so that courts consistently distinguish between unlawful attacks on reputation and protected expression in the public interest.

To reduce interpretive discrepancies and strengthen legal certainty, several legislative refinements can be proposed. First, the legislature could consider harmonizing the wording "without rights" with terms such as "intentionally" or "against the law" used in the KUHP, so that the mental and unlawful elements are formulated consistently across statutes (Bisri, 2003). Second, "without rights" should be explicitly defined in the ITE Law by clarifying when an act lacks legal authorization, conflicts with another's rights, or contravenes objective law to guide judges and prevent arbitrary applications (Hamzah, 2012). Third, legal safeguards for digital expression need to be reinforced by clearly differentiating criminal defamation from legitimate criticism, whistleblowing, and public-interest reporting, thereby protecting freedom of speech while still ensuring accountability for genuinely harmful and unjustified attacks on reputation (Sjahdeini, 2009).

Deliberate and Unrighteous Application of the Elements in the Crime of Defamation Through Electronic Media in the Criminal Justice Process

Legal certainty is a core requirement in criminal law enforcement, but realizing it demands legislative refinements that align judicial interpretation with the purposes embodied in statutory provisions. The government bears a central responsibility for ensuring consistency in the criminal justice system so that judges and law enforcement agencies apply uniform legal principles and avoid contradictory constructions of the same norms.

In the enforcement of defamation provisions, a coherent criminal policy is necessary because defamation, as an attack on a person's honor or reputation, requires courts to assess not only the content of a statement but also its context and impact. Under Indonesian law, the ITE Law's defamation provision in Article 27 paragraph (3) is systematically linked to the insult and defamation norms in Article 310 and Article 311 of the Criminal Code, with both regimes treating defamation as a complaint offense (*delik aduan*) that can only be prosecuted following a complaint from the injured party. This construction was reaffirmed in Constitutional Court Decision No. 50/PUU-VI/2008, which held that Article 27 paragraph (3) of the ITE Law must be interpreted consistently with the complaint-based nature of the underlying defamation offenses in the Criminal Code, thereby emphasizing the necessity of a victim-initiated complaint before criminal proceedings may be brought.

The criminal justice process in Indonesia generally follows a sequential flow of investigation, prosecution, and adjudication, leading to sentencing, with each stage involving distinct institutional roles and procedural safeguards. In defamation cases, inconsistencies in outcomes often arise from divergent judicial views on whether particular digital expressions meet the legal threshold of defamatory statements, especially when context, tone, and medium are contested.

Judicial reasoning about law enforcement can be viewed through at least three complementary approaches:

1. Normative approach: positions police, prosecutors, and courts primarily as implementers of statutory norms and legal principles;
2. Administrative approach: treats law enforcement institutions as organizations whose structures, procedures, and coordination affect the effectiveness of criminal justice;
3. Social approach: situates law enforcement within broader social dynamics, in line with progressive and socio-legal perspectives that see law as embedded in community life and power relations.

To ensure fairness in digital defamation cases, courts need to analyze not only the wording

of the statements but also the speaker's intent, the communicative context, and the impact on the alleged victim.

First, statutory definitions in the ITE Law should be clarified so that "without rights" is explicitly defined in the text, for example, by specifying when an act lacks legal authorization, conflicts with another's subjective rights, or violates objective legal norms, thereby giving judges a clear interpretive framework. Second, judicial training programs on digital evidence, forensic techniques, and the specific characteristics of online communication are essential so that judges and law-enforcement officials can correctly assess authenticity, context, and harm in digital defamation cases, in line with a modern, technologically literate criminal justice system (Atmasasmita, 1996).

Third, non-penal solutions such as mediation, penal mediation, or other forms of ADR should be actively encouraged in defamation disputes to avoid unnecessary criminalization where the conflict can be effectively resolved through apology, correction, or compensation rather than imprisonment. By refining the legal formulation of "without rights," improving the capacity of the judiciary, and institutionalizing proportionate, non-penal responses, the ITE Law will be better positioned to balance freedom of expression with legal accountability so that defamation provisions protect reputation without being misused to suppress legitimate public discourse (Marpaung, 1991).

CONCLUSIONS

The element of intentionality in defamation cases under the 2024 ITE Law refers to a subjective error, involving the perpetrator's intent and awareness of their actions. Meanwhile, the element of "without rights" indicates the objective nature of an act that is contrary to the law. The revised formulation of defamation offenses in the 2024 ITE Law emphasizes intent as the central criterion. However, the continued use of the phrase "without rights" has led to interpretational inconsistencies, necessitating legal reforms to clarify its meaning and application.

Ambiguities in legal interpretations of "without rights" have led to inconsistent court rulings, raising concerns about selective law enforcement and potential restrictions on freedom of expression. A holistic approach is needed, incorporating both criminal and non-criminal legal policies, along with a thorough understanding of formal law, material law, and legal philosophy. Legal certainty and firm enforcement are essential in ensuring that ITE crimes are addressed fairly and consistently, preventing misuse of legal provisions to suppress digital speech.

The amendment to the ITE Law is necessary to clarify the phrase "without rights." This can be achieved either by explicitly defining its meaning within the legislation or by replacing it with a more precise legal term. Such reforms aim to eliminate multiple interpretations that have led to inconsistencies in judicial decisions and ensure a fairer application of the law. Specialized training programs should be developed and implemented for judges and law enforcement officials handling defamation cases. These programs would enhance their understanding of digital defamation laws, provide guidance on evaluating evidence in online cases, and promote uniformity in legal interpretations.

By equipping judicial authorities with the necessary legal and technological knowledge, more consistent and just rulings can be achieved. To minimize the excessive criminalization of digital defamation, promoting Alternative Dispute Resolution (ADR) mechanisms is essential. Mediation and other non-penal approaches should be encouraged as viable means of settling disputes related to online defamation. These mechanisms provide an opportunity for reconciliation between the involved parties while reducing the burden on the judicial system and preventing unnecessary legal consequences. Strengthening legal protections for digital rights is crucial to maintaining a balanced legal framework. While it is important to hold individuals accountable for defamatory statements,

the law must also safeguard freedom of expression in the digital space.

Legal provisions should be designed to differentiate between harmful defamation and legitimate criticism, ensuring that individuals' rights to express opinions online are not unjustly restricted. Raising public awareness about digital rights and legal responsibilities under the ITE Law is essential in fostering responsible online behavior. Educational campaigns should be conducted to inform citizens about what constitutes defamation, their freedom of speech rights, and the legal implications of online communication. By increasing legal literacy, individuals can better navigate the digital landscape while respecting others' rights.

LIMITATION & FURTHER RESEARCH

The research limitations focus on aspects of criminal law, particularly defamation through electronic media and the application of elements intentionally and without rights in this context. This research is also limited by the scope of Indonesian law, particularly laws governing electronic information and transactions. Further research could examine the implementation of the new law in 2024 and its impact on law enforcement and the justice system.

In addition, further studies can deepen understanding of the legal consequences faced by perpetrators of criminal defamation through electronic media, as well as efforts to raise legal awareness and prevent cybercrime. Further development can also be carried out to identify challenges and obstacles in law enforcement related to ITE crimes, as well as to develop effective and fair alternative dispute resolution. Additionally, future research could explore societal responses to new laws and changes in law enforcement related to cybercrime.

REFERENCES

Abdillah, A. N. (2023). *Kedudukan alat bukti elektronik dalam perkara perceraian di Pengadilan Agama tanpa digital forensik (Studi di Pengadilan Agama Kabupaten Kediri Kelas 1A)* (Skripsi sarjana, IAIN Kediri).

Adji, I. S. (2009). *Korupsi kebijakan aparatur negara & hukum pidana*. Diadit Media.

Alviolita, F. P., & Arief, B. N. (2019). Kebijakan formulasi tentang perumusan tindak pidana pencemaran nama baik dalam pembaharuan hukum pidana di Indonesia. *Law Reform, 15*(1), 130–148. https://doi.org/10.14710/lr.v15i1.23359

Andria, A., & Saifulloh, M. (2022). Forensik metadata foto sebagai alat bukti digital. *Prosiding Seminar Nasional Hasil Penelitian & Pengabdian Masyarakat Bidang Ilmu Komputer*, 8–12.

Arief, B. N. (2007). *Masalah penegakan hukum dan kebijakan hukum pidana dalam penanggulangan kejahatan*. Kencana Prenada Media Group.

Arief, B. N. (2010). *Bunga rampai kebijakan hukum pidana*. PT Citra Aditya Bakti.

Arliman, L. S. (2017). Mewujudkan penegakan hukum yang baik untuk mewujudkan Indonesia sebagai negara hukum. *Jurnal Hukum Doctrinal, 2*(2), 509–532. https://jurnal.um-palembang.ac.id/doktrinal/article/view/2523

Asmadi, E. (2021). Rumusan delik dan pemidanaan bagi tindak pidana pencemaran nama baik di media sosial. *De Lega Lata: Jurnal Ilmu Hukum, 6*(1), 16–33.

Atmasasmita, R. (1996). *Sistem peradilan pidana perspektif eksistensialisme dan abolisionisme*. Binacipta.

Bisri, I. (2003). *Hukum pidana: Regulasi & implementasi di Indonesia*. Alqaprint.

Hamzah, A. (2012). *Asas-asas hukum pidana di Indonesia dan perkembangannya*. Sofmedia.

Hardinanto, H. (2019). *Akses ilegal dalam perspektif hukum pidana*. Setara Press.

Irmansyah, R. A. (2013). *Hukum hak asasi dan demokrasi*. Graha Ilmu.

Khalil, E. L. (2024). Blasphemy laws contra defamation laws: An anomaly facing rational choice theory. *Social Sciences & Humanities Open, 10*, 101137.

https://doi.org/10.1016/j.ssaho.2024.101137
Koltay, P. A., & Wragg, A. (2020). *Comparative privacy and defamation*. Edward Elgar Publishing.
Kusnardi, M., & Ibrahim, H. (1988). *Hukum tata negara Indonesia*. Sinar Bakti.
Latifah, K. N. & Najicha, F. U. (2022). Implikasi media sosial terhadap formulasi kebijakan publik. *Jurnal Kewarganegaraan, 6*(1), 494–501.
Li, X., & Qin, Y. (2018). Research on computer network defamation crime in China. *Procedia Computer Science, 131*, 1217–1222. https://doi.org/10.1016/j.procs.2018.04.329
Marpaung, L. (1991). *Unsur-unsur perbuatan yang dapat dihukum (delik)*. Sinar Grafika.
Moeljatno. (1993). *Asas-asas hukum pidana*. Rineka Cipta.
Muthia, F. R., & Arifin, R. (2019). Kajian hukum pidana pada kasus kejahatan mayantara (*cybercrime*) dalam perkara pencemaran nama baik di Indonesia. *Resam Jurnal Hukum, 5*(1). https://jurnal.stihmat.ac.id/index.php/resam/article/view/18/22
Pakaya, R. D., & Mahyani, A. (2022). Landasan perumusan *locus delicti* dalam surat dakwaan pada kejahatan siber. *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance, 2*(1), 673–686. https://doi.org/10.53363/bureau.v2i1.160
Purnomo, H. (2020). Penegakan hukum terhadap tindak pidana pencemaran nama baik melalui media berdasarkan konsep hukum pidana. *Soumatera Law Review, 3*(2), 119–136. http://ejournal.lldikti10.id/index.php/soumlaw/article/view/5337/1940
Putri, P. (2019). Konvergensi hukum informasi dan transaksi elektronik dalam kejahatan korporasi (*corporate crime*) menurut Undang-Undang Nomor 11 Tahun 2008 jo Undang-Undang Nomor 19 Tahun 2016. *Lex Et Societatis, 7*(11), 55–63.
Raharjo, S. (2001). *Sisi-sisi lain dari hukum di Indonesia*. PT Gramedia Pustaka Utama.
Rochman, S., Hamdani, F., & Baharuddin. (2021). Pencemaran nama baik melalui media sosial: Perbandingan hukum pidana positif dan Islam. *DIKTUM: Jurnal Syariah dan Hukum, 19*(1), 32–49. https://ejurnal.iainpare.ac.id/index.php/diktum/article/view/2080/886
Saad, H. B. M. (2023). *Defamation (libel) law in Malaysia: An overview*.
Sarkar, G., & Shukla, S. K. (2024). Reconceptualizing online offenses: A framework for distinguishing cybercrime, cyberattacks, and cyberterrorism in the Indian legal context. *Journal of Economic Criminology, 4*, 100063. https://doi.org/10.1016/j.jecrim.2024.100063
Setiyono, S. (2016). Reorientasi kebijakan pemidanaan bagi penyalahguna narkotika. *Jurnal Cakrawala Hukum, 7*(1), 34–44. https://jurnal.unmer.ac.id/index.php/jch/article/view/1782/1146
Situmeang, S. M. T. (2022). Politik hukum pidana terhadap kebijakan kriminalisasi dan dekriminalisasi dalam sistem hukum. *Res Nullius Law Journal, 4*(2), 168–181. https://doi.org/10.34010/rnlj.v4i2.7166
Sjahdeini, S. R. (2009). *Kejahatan dan tindak pidana komputer*. Grafiti.
Sunarso, S. (2015). *Viktimologi dalam sistem peradilan pidana*. Sinar Grafika.
Utoyo, M. H., Afriani, K., Rusmini, R., & Husnaini. (2020). Sengaja dan tidak sengaja dalam hukum pidana Indonesia. *Lex Librum, 7*(1), 75–85. https://lexlibrum.id/index.php/lexlibrum/article/view/298/pdf
Wardana, R. (2023). *Penyelesaian tindak pidana ITE berbasis plea bargaining system*. Jejak Pustaka.