GOLDEN RATIO OF LAW AND SOCIAL POLICY REVIEW
VOLUME 5, ISSUE. 2 (2026)
Website: https://goldenratio.id/index.php/grlspr

GOLDEN RATIO
ISSN [Online]: 2808-2923

LAW & SOCIAL POLICY | RESEARCH ARTICLE

# Reconstructing Criminal Liability Models for the Dissemination of False Information in the Indonesian Criminal Justice System (An Analysis of the ITE Law After the 2024 Amendment)

Nabil Librian Pratama[1], R Arif Sulaiman[2]

[1,2] Universitas KH. Bahaudin Mudhary Madura, Sumenep, Indonesia.
Email: Nabil.librian@yahoo.com[1], arafisulaiman@gmail.com[2]

**ARTICLE HISTORY**

Received: March 1, 2026
Revised: April 28, 2026
Accepted: April 28, 2026

**DOI**
https://doi.org/10.52970/grlspr.v5i2.2135

**ABSTRACT**
This study analyzes and reconstructs the model of criminal liability for the dissemination of false information in the Indonesian criminal law system, particularly based on the provisions of the Electronic Information and Transactions Law after the 2024 amendment. Despite the increasing regulation of false information under the ITE Law, there remains a lack of clarity regarding the conceptual boundaries and application of criminal liability, as well as limited scholarly discussion on how such liability should be reconstructed to balance law enforcement and freedom of expression. This study addresses this research gap by offering a systematic reconstruction model. This study employs a normative legal approach using legislative and conceptual methods, analyzed descriptively and prescriptively through a structured literature review. The findings show that criminal liability for the dissemination of false information requires the fulfillment of the elements of criminal acts (actus reus) and fault (mens rea), which are reflected in the elements of "intentionally" and "without rights" in the ITE Law. However, in practice, there is still uncertainty regarding the definition of "false information," the potential for multiple interpretations, and the risk of excessive criminalization that could conflict with freedom of expression. These issues indicate a gap between normative regulation and its practical implementation. Therefore, the reconstruction model emphasizes (1) clear and restrictive definitions of false information, (2) strict proof of intent, (3) application of proportionality in criminal sanctions, and (4) differentiation of roles between content creators, redistributors, and electronic system operators. This model places criminal law as the ultimum remedium to ensure legal certainty, justice, and effective protection of freedom of expression in the digital space.

**Keywords:** Legal Reconstruction, Criminal Liability, Dissemination of False Information, Indonesian Criminal Law System, ITE Law 2024.

## I. Introduction

The rapid development of information and communication technology has brought significant changes in the way people interact, obtain, and disseminate information. The internet and digital platforms such as social media, blogs, forums, and instant messaging applications allow information to be disseminated instantly large audiences without spatial and temporal limitations to millions of people without space and

ISSN [Online]: 2808-2923

time limitations. This transformation has fundamentally reshaped the flow of information in modern society. On the one hand, this phenomenon has had positive impacts, such as faster access to information, democratization of content, and empowerment of civil society in the digital public sphere (Castells, 2009; Shirky, 2011). However, on the other hand, the ease of information dissemination has also facilitated the widespread distribution opened up vast opportunities for the distribution of negative content, especially false information or hoaxes that have the potential to cause harmful effects on individuals and communities.

In this context, the proliferation of false information has emerged as a critical issue. False information or hoaxes are content that is deliberately designed to be untrue and disseminated to mislead the public for specific purposes, such as political or economic gain, or simply to manipulate public opinion (Allcott, H., & Gentzkow, 2017). The spread of hoaxes has become a global issue that affects various aspects of life, ranging from consumer decisions, social stigma, communal conflicts, to threats to national security (Wardle, C., & Derakhshan, 2017). This global trend is also evident at the national level. In Indonesia, a similar phenomenon has occurred on a massive scale, marked by an increasing number of hoax cases involving individuals and groups. For instance, false information related to public health has triggered panic buying and vaccine hesitancy, while political disinformation during election periods has contributed to social polarization and the spread of hate speech across communities. In addition, economic hoaxes, such as fraudulent online investment schemes, have caused significant financial losses for the public. These conditions have resulted in economic losses, social polarization, and disruptions to democratic processes, including general elections (Muhammad, 2019).

In response to these developments, the Indonesian government has established a legal framework to regulate digital information. To respond to these challenges, Indonesia regulates the dissemination of information through positive legal instruments, specifically through Law Number 11 of 2008 (Law Number 11 Republic of Indonesia Year 2008 Number 58., 2008). The ITE Law is an important regulation designed to regulate electronic transactions, data protection, and prohibitions on certain content in the digital space. Articles 28 and 45A of the ITE Law specifically prohibit the dissemination of false and misleading news that could harm consumers or create hostility based on ethnicity, religion, race, and intergroup relations (SARA). These provisions were then reinforced through the first amendment in Law Number 19 of 2016 and the second amendment through Law Number 1 of 2024, which adjusted the legal framework in line with the increasingly complex dynamics of digital practices (Law Number 1., 2024). Nevertheless, despite the existence of this regulatory framework, significant challenges remain in its implementation. Although the ITE Law normatively prohibits the dissemination of false information, the application of this norm in law enforcement practice presents conceptual and operational problems. First, there are challenges in interpreting what is meant by "false and misleading news" so that it does not overlap with the right to freedom of expression protected in the national and international legal systems (Anriani, 2020; Nugroho, 2021) Second, proving intent (mens rea) in the digital context is often difficult due to the complex and reflexive nature of cyberspace, where perpetrators can deny their awareness of the information being disseminated (Situmorang, 2022). Third, its generic legal umbrella has led to debates on whether the ITE Law has effectively accommodated modern criminal law demands such as the principle of proportionality and the strict principle of legality.

These challenges have prompted further academic inquiry into the adequacy of existing legal approaches. Furthermore, developments in cyber criminal law practices have encouraged academic studies to not only view the ITE Law as a repressive instrument, but also to examine how criminal liability models are applied fairly, proportionally, and in line with general criminal law principles such as fault liability and no punishment without fault (geen straf zonder schuld) (Moeljatno., 2008; Arief., 2019). In this context, a critical conceptual reconstruction of the criminal liability model is needed, both for individuals and corporations involved in the spread of hoaxes in the digital space, in order to strengthen the quality of criminal law enforcement in an increasingly complex digital era. Importantly, such a reconstruction is not merely theoretical but has direct practical implications for law enforcement and policy-making. A clearer and more structured model of criminal liability can guide judges, prosecutors, and investigators in consistently interpreting legal provisions, particularly in assessing intent, defining false information, and determining proportional sanctions. It can also serve as a reference for policymakers in refining legal norms to reduce ambiguity and prevent overcriminalization.

Based on the foregoing discussion, it becomes evident that the current regulation and application of criminal liability for the dissemination of false information remain unclear and potentially inconsistent in

ISSN [Online]: 2808-2923

practice. Accordingly, this study is directed to address a central question. Therefore, this study seeks to address the following research question: how should the model of criminal liability for the dissemination of false information be reconstructed within the Indonesian criminal justice system, particularly under the amended ITE Law of 2024, in order to ensure legal certainty, proportionality, and the protection of freedom of expression? Accordingly, this study analyzes existing legal provisions and reconstructs an ideal model of criminal liability that is more adaptive, balanced, and responsive to the challenges of the digital era.

## II. Literature Review and Hypothesis Development

### 2.1. Legal Reconstruction

Legal reconstruction is an approach to updating or reformulating legal norms to better suit societal developments and the need for justice. According to Rahardjo (2009), legal reconstruction is progressive in nature in the sense that it prioritizes the adaptation of legal norms to evolving social realities, emphasizes substantive justice over rigid formalism, and allows the law to function as a dynamic instrument for social change and must be responsive to social dynamics, so that the law is not only formal but also substantive (Rahardjo, 2009). Arief (2011) emphasizes that criminal law reconstruction needs to consider effectiveness, justice, and community protection, especially when dealing with new phenomena such as the spread of digital information.

To ensure analytical coherence, the concept of legal reconstruction in this study is specifically directed toward reformulating the model of criminal liability, particularly in addressing the dissemination of false information in digital contexts. Thus, legal reconstruction becomes the basis for developing a model of criminal responsibility that is adaptive to cases of spreading false information. In this regard, the reconstruction of legal norms cannot be separated from the fundamental principles of criminal liability, since any reformulation of the law must ultimately determine how responsibility is assigned to individuals who commit unlawful acts. Therefore, a clear understanding of criminal liability is essential to ensure that the reconstructed legal framework operates effectively and justly.

### 2.2. Criminal Liability

Criminal liability is a key concept in criminal law that determines when a person can be punished for their actions. Structurally, criminal liability consists of two main elements:

a. Objective elements (actus reus) – the unlawful act committed, which refers to the existence of a concrete action or conduct that violates legal norms.
b. Subjective elements (mens rea) – the mental state of the perpetrator, which concerns the intention, awareness, or negligence accompanying the act.

According to Sudarto (1990) in his book entitled *Principles of Criminal Law*, criminal liability requires the existence of intent (*dolus*) or negligence (*culpa*) on the part of the perpetrator. (Sudarto., 1990). Arief (2011) in his book entitled *Hukum Pidana dan Pertanggung jawaban*, adds that the perpetrator's capacity to understand the consequences of their actions (*toerekeningsvatbaarheid* (criminal responsibility capacity or imputability, the ability of a person to be held legally accountable for their conduct)) is also an important requirement before they can be punished. Building upon the reconstructed legal framework discussed earlier, the application of criminal liability in cases of false information dissemination must be carefully evaluated within both objective and subjective dimensions. In the context of spreading false information, criminal liability must assess whether the perpetrator:

a. Spread false information, meaning that the perpetrator actively disseminates information that is factually incorrect or misleading to the public.
b. Did so intentionally or negligently, indicating whether the act was carried out with deliberate intent to mislead or due to a lack of due care in verifying the information.

ISSN [Online]: 2808-2923

This assessment is crucial in distinguishing between deliberate disinformation and unintentional misinformation within legal proceedings.

### 2.3. Spreading False Information

The spread of false information or hoaxes has become an important phenomenon in the digital age (Wardle & Derakhshan, 2017). False information can be divided into:

a. Misinformation: false information shared without intent to mislead,
b. Disinformation: false information deliberately created and spread to deceive,
c. Malinformation: genuine information used maliciously to harm others.

This distinction is important in legal analysis because criminal liability generally requires intent, making disinformation more likely to fall within criminal sanctions compared to misinformation. Lazer et al., (2018) state that hoaxes are deliberately made to resemble legitimate news to influence public opinion and can cause social or political harm. In the Indonesian legal framework, particularly under the ITE Law, the classification of false information is closely linked to the interpretation of "false and misleading news," which directly affects legal enforcement and judicial reasoning. Furthermore, the ITE Law categorizes the spread of false information as a formal offense, whereby the act of spreading false information is punishable without waiting for actual social impacts to occur.

### 2.4. The Indonesian Criminal Justice System

The Indonesian criminal law system consists of the Criminal Code as general criminal law and special laws as lex specialis, including the ITE Law. According to Friedman (1975) in his work entitled *The Legal System: A Social Science Perspective*, the legal system consists of:

a. Legal structure (law enforcement institutions),
b. Legal substance (written rules),
c. Legal culture (Friedman, 1975)

In the context of spreading false information, the police act as investigators, the prosecutor's office as prosecutors, and the courts as adjudicators. Legal culture refers to societal attitudes, values, and behaviors toward law, including how individuals use, obey, or resist legal norms. In the digital era, legal culture influences how people perceive and share information online, which in turn affects law enforcement effectiveness. For example, the widespread habit of forwarding unverified messages on social media platforms or messaging applications demonstrates a low level of digital legal awareness, which can contribute to the rapid spread of false information. The interaction between these components determines the effectiveness of law enforcement. Weak coordination or differing interpretations among institutions may lead to inconsistent application of the ITE Law. Additionally, digital legal culture such as the tendency to share information without verification—can hinder enforcement efforts and increase the spread of hoaxes. Another example can be seen in cases where viral misinformation pressures law enforcement agencies to act quickly, sometimes leading to inconsistent or reactive legal responses.

### 2.5. ITE Law 2024

The Electronic Information and Transactions Law (ITE Law) is a special regulation that governs electronic-based criminal acts. This law was first passed through Law No. 11 of 2008, amended by Law No. 19 of 2016, and last updated in 2024. Historically, the enactment of the ITE Law in 2008 marked Indonesia's initial effort to regulate activities in the digital sphere, particularly in response to the rapid growth of internet usage and electronic transactions. The 2016 amendment was introduced to address public criticism, especially concerning provisions on defamation and freedom of expression, by providing clearer limitations and

ISSN [Online]: 2808-2923

reducing the potential for misuse. The most recent update in 2024 further reflects the government's attempt to adapt the law to ongoing technological developments and emerging forms of digital interaction.Important provisions related to false information include prohibitions on:

a. The dissemination of false news that harms consumers, which refers to the distribution of misleading or inaccurate information that may cause financial or non-financial losses to consumers.
b. The dissemination of content that incites hatred or slander, meaning content that provokes hostility or defames individuals or groups based on certain attributes.
c. Defamation, which involves damaging a person's reputation through false statements or allegations.

The ITE Law serves as the normative basis (*lex specialis*) for the dissemination of digital information. However, critics argue that it allows multiple interpretations particularly due to the vague formulation of key terms such as "false information" and "public harm," which may be interpreted differently by law enforcement officers, prosecutors, and judges, potentially leading to inconsistent legal outcomes and uncertainty for the public and risk excessive criminalization (overuse of criminal sanctions for acts that may be better addressed through civil or administrative mechanisms) (Roxin, 2006). In practice, the Indonesian criminal justice system faces several challenges in enforcing the ITE Law in the digital context, including difficulties in digital evidence collection, jurisdictional issues in cross-border information flows, and the rapid spread of information through social media platforms. Additionally, limitations in digital literacy among both law enforcement officials and the public further complicate efforts to effectively address the dissemination of false information.

### 2.6. Cybercrime Law and Electronic Information Offenses

Cybercrime law emerged to regulate criminal acts in the digital space. The dissemination of false information falls under the category of electronic information offenses, where the mechanisms of proof and criminal liability differ from those of conventional criminal law (Arief, 2011). The cybercrime law approach considers:

a. The perpetrator's intent, which determines whether the act constitutes disinformation or mere misinformation, The social impact of the dissemination of information, including potential harm to public order, economy, or national security,
b. The role of digital platforms as a means of dissemination. including potential harm to public order, economy, or national security,

For example, cases involving the spread of hoaxes during elections illustrate how false information can influence public opinion and disrupt democratic processes, highlighting the need for a more adaptive criminal liability model.

## III. Research Method

This study is a normative legal study (juridical normative) that aims to analyze and reconstruct the model of criminal liability for the dissemination of false information in the Indonesian criminal law system, particularly based on the provisions of the Electronic Information and Transactions Law after the 2024 amendment. This study focuses on the study of written legal norms and relevant criminal law doctrines (Marzuki, 2017; Soekanto, 2014). Additionally, this study ensures originality by proposing a reconstructed model of criminal liability that integrates the principle of fault with a contextual interpretation of false information in digital spaces, which has not been comprehensively developed in prior studies. Moreover, the findings of this study are expected to contribute to the existing literature by enriching the discourse on criminal liability in cyber law, as well as providing practical guidance for law enforcers and policymakers in

ISSN [Online]: 2808-2923

handling cases of false information dissemination. This study also takes into account ethical considerations in normative legal research, particularly by ensuring the responsible use and interpretation of legal sources, maintaining academic integrity, and avoiding bias in legal analysis. Several sentences have been simplified and broken down to improve clarity and readability.

The approaches used in this study are interconnected and applied sequentially. To improve coherence, smoother transitions are introduced between the statute, conceptual, and comparative approaches. The study begins with a statute approach by examining the provisions in the Electronic Information and Transaction Law and the Criminal Code. Subsequently, the analysis moves to the conceptual approach, which is used to examine the theory of criminal liability, the principle of fault, and the theory of punishment (Marzuki, 2017). To a limited extent, a comparative approach was also used to enrich the analysis of legal reconstruction (Ibrahim, 2006). Furthermore, this research introduces a novel analytical framework that combines doctrinal analysis with a digital-contextual perspective in assessing criminal responsibility. This framework also serves as a reference for future research in developing more adaptive and context-sensitive legal analyses in the digital era. Ethical considerations are also reflected in the selection and evaluation of legal materials, ensuring that all sources are credible, properly cited, and used in accordance with academic standards.

The legal materials used consist of primary legal materials in the form of legislation and court decisions, secondary legal materials in the form of literature and scientific journals, and tertiary legal materials as supporting materials (Soekanto, 2014). Primary legal materials were obtained from official government sources, including statutory regulations and published court decisions. Secondary legal materials were collected from academic books, journals, and legal databases, while tertiary materials were derived from legal dictionaries and encyclopedias. The selection of legal materials was based on relevance to the research topic, particularly those related to criminal liability, false information, and cyber law. Inclusion criteria include sources addressing the ITE Law and criminal liability doctrines, while exclusion criteria include outdated or irrelevant sources. In addition, the sampling process for selecting legal materials was conducted using a purposive sampling technique, where legal sources were deliberately selected based on their relevance, authority, and contribution to the research objectives. This approach ensures that the selected materials are representative and allows the study to be replicable.

Then, legal materials were organized according to their type (primary, secondary, and tertiary) and classified based on key issues such as criminal liability, interpretation of false information, and enforcement practices. In the data collection stage, Legal materials were collected through literature studies using systematic search procedures, including keyword identification (e.g., "false information," "criminal liability," "ITE Law"), source selection, and document screening, followed by reading and categorizing relevant materials. In this stage, specific tools such as academic databases (e.g., Scopus, Google Scholar), reference management software (e.g., Mendeley), and document analysis techniques were utilized to systematically organize, store, and review the collected legal materials. Throughout this process, ethical principles such as transparency, accuracy, and accountability were upheld to ensure the reliability of the research.

The materials were then analyzed qualitatively using grammatical, systematic, and teleological interpretation methods (Marzuki, 2017), by interpreting legal provisions, comparing doctrinal views, and evaluating their application. In addition, the qualitative analysis is strengthened through an integrated doctrinal-thematic coding approach, where legal texts are coded into key thematic categories (e.g., criminal liability elements, intent, and digital misinformation patterns) before interpretation, allowing a more structured and innovative analytical process in normative legal research. This process ensures a more detailed and structured interpretation of qualitative data. Finally, the analysis in this study is descriptive-analytical and prescriptive in nature, i.e., it describes the applicable regulations, identifies their weaknesses, and formulates a model for reconstructing criminal liability that better guarantees legal certainty, justice, and benefit (Arief, 2011). This prescriptive outcome further reflects the originality of the study by offering a distinct and applicable reconstruction model grounded in both doctrinal theory and contemporary digital legal challenges. In addition, the results of this study are expected to provide practical implications for improving

ISSN [Online]: 2808-2923

legal policy formulation and law enforcement practices, particularly in addressing the challenges of misinformation in digital environments.

## IV. Result and Discussion

### 4.1. Provisions on Criminal Liability for the Dissemination of Information

Criminal liability in the Indonesian criminal justice system is based on the principle that a person can only be punished if there is a criminal act (actus reus) and an element of fault (*mens rea*) (Moeljatno, 2008). This principle reflects the principles of legality and fault, which are also recognized in other countries' legal systems as the basis for criminal liability for the dissemination of information (Bassiouni, 2014). In the context of Indonesian criminal law, the principle of legality as reflected in Article 1 paragraph (1) of the Criminal Code emphasizes that no act can be punished unless it is based on existing legislation. This principle requires the formulation of clear norms (*lex certa*) that are not open to multiple interpretations so that law enforcement officials cannot arbitrarily expand their meaning (Hamzah, 2015). In cases involving the dissemination of digital information, clarity of the elements of the offense becomes even more important due to the fast-paced and massive nature of cyberspace (Chazawi, 2016).

Normative provisions regarding the dissemination of false information in Indonesia are regulated in the Electronic Information and Transactions Law after the 2024 amendment (Republic of Indonesia, 2024), which requires the elements of "intentional" and "unauthorized" in the dissemination of electronic media information. In this study, key terms are defined to avoid ambiguity. "False information" refers to any information that is factually incorrect or misleading and has the potential to create misunderstanding among the public. Meanwhile, a "hoax" is defined more specifically as deliberately fabricated information that is intentionally created and disseminated to deceive or manipulate public perception. Furthermore, this study distinguishes between "misinformation" (false information shared without intent to mislead) and "disinformation" (false information deliberately created and disseminated with the intention to deceive), as these distinctions are essential in determining criminal liability, particularly in relation to the element of intent (mens rea).

In this study, "false information" refers to information that is factually incorrect and capable of misleading the public, while a "hoax" specifically refers to information that is deliberately fabricated and disseminated with the intention to deceive. This element indicates that criminal liability requires intent or specific purpose on the part of the perpetrator (Chazawi, 2016). This is in line with international studies that regulations on digital information need to require the element of intent to avoid widespread criminalization of content that is false but unintentional (Citron & Norton, 2011). The element of "without rights" in this provision also has important implications, as it indicates that not all dissemination of false information is automatically unlawful. It must be proven that there has been a violation of certain legal norms or interests. In criminal law doctrine, this element of unlawfulness can be formal or material, depending on the construction of the norm used (Moeljatno, 2008). Therefore, proving the elements of intent and without right becomes the central point in assessing whether or not a person can be held criminally liable.

Furthermore, although the ITE Law is the main instrument, the general principles in the Criminal Code remain a reference for the principle of legality and the form of participation (deelneming). The principle of legality requires clear and predictable criminal provisions (Hamzah, 2015), while the principle of fault ensures that a person is only punished if it can be proven that there was intent or negligence that can be held criminally responsible. The concept of participation *(deelneming)* is relevant in the context of digital information dissemination because content can be produced by one party and disseminated by another. The Criminal Code recognizes the forms of perpetrator, participant, and accomplice, each of which has different consequences in terms of liability (Chazawi, 2016). In cyber space practice, this distinction is important in determining whether a person is the main content creator or merely a redistributor.

From a comparative perspective, legal systems such as those in the European Union emphasize stricter standards on platform responsibility and clearer categorization of illegal content, particularly through regulatory frameworks that distinguish between illegal content and harmful but lawful content. In contrast, the Indonesian ITE Law still tends to use broader formulations, which may create a higher risk of multiple

ISSN [Online]: 2808-2923

interpretations in law enforcement. This difference highlights the need for clearer normative boundaries in the Indonesian context. However, the adoption of international models must be carefully adapted to the Indonesian legal and institutional context. Unlike the European Union, which has a more developed regulatory framework and stronger institutional coordination, Indonesia's legal system is characterized by the coexistence of general criminal law (Criminal Code) and special laws such as the ITE Law, as well as varying levels of digital literacy among law enforcement officials and the public.

Elements derived from international practices—such as clearer categorization of content, stricter standards for intent, and differentiated platform responsibility—need to be contextualized within Indonesia's legal structure, particularly by aligning them with the principles of legality, existing statutory provisions, and institutional capacities of law enforcement agencies. In addition to these theoretical challenges, empirical indications from law enforcement practices in Indonesia further reveal inconsistencies in the application of criminal liability. Several cases have shown that individuals who merely redistributed information through social media platforms were still subjected to criminal sanctions, despite the absence of clear intent to mislead the public. This reflects the difficulty in consistently proving the element of mens rea in digital contexts, particularly when information is shared rapidly without verification. Empirical studies also indicate that law enforcement officials often face limitations in distinguishing between misinformation and disinformation, especially due to the high speed of information circulation and limited digital verification capacity (Kusumaningrum, 2023). This condition is exacerbated by the digital culture of society, where users tend to share information without prior verification, thereby contributing to the widespread dissemination of false information without clear malicious intent.

During the COVID-19 pandemic, the spread of false health-related information significantly influenced public behavior, including vaccine hesitancy and misinformation about medical treatments. However, not all individuals involved in disseminating such information could be clearly categorized as intentional perpetrators, which illustrates the gap between normative legal provisions and their practical enforcement. Conflicts between law enforcement and freedom of expression must be placed within the framework of lawful and proportional restrictions. The principle of proportionality in international law requires that restrictions on rights must have a legitimate purpose, be necessary, and not be excessive (Bassiouni, 2014). Therefore, the formulation of criminal norms related to false information must avoid excessive criminalization that could hinder public participation in the digital space. Accordingly, normative refinement should include clearer definitions of false information, stricter limitations on interpretation, and more consistent evidentiary standards, particularly in proving intent and unlawfulness, in order to ensure legal certainty and protect fundamental rights. Overall, although normative constructs regarding criminal liability are already in place, further refinement of norms is needed to ensure legal certainty and maintain a balance between law enforcement and the right to freedom of expression.

### 4.2. The Ideal Criminal Liability Model to be Reconstructed

The ideal criminal liability model must consider two aspects simultaneously: protecting society from the negative impact of false information and respecting freedom of expression as a fundamental right. According to modern criminal law theory, criminal law should be used as a last resort (ultimum remedium) when other mechanisms are insufficient (Sudarto, 2010; Ashworth, 2013). The principle of ultimum remedium emphasizes that criminal law is not the first instrument in resolving social problems. In the context of digital information, mechanisms such s correction, clarification, the right of reply, or administraive sanctions should be prioritized before imposing criminal penalties (Ashworth, 2013). This approach is in line with criminal law policies that place criminal punishment as a last resort in order to maintain proportionality (Sudarto., 2010). First, the definition of "false information" needs to be formulated clearly and restrictively. A formulation that is too broad has the potential to violate the principle of lex certa in the principle of legality and can lead to subjective interpretations by law enforcement officials (Hamzah, 2015). Several international publications also state that defining clear boundaries is crucial to guaranteeing the right to freedom of expression while providing legal certainty for digital media users (Marsden, 2017).

A restrictive definition is also important to distinguish between factual errors, opinions, satire, and deliberate disinformation. Communication law literature emphasizes that not all inaccurate information can

ISSN [Online]: 2808-2923

be classified as a criminal offense without proof of intent and significant impact (Marsden, 2017). Thus, an intent- and impact-based approach is relevant in the reconstruction model. Second, the criminal liability model must emphasize the proof of intent as a key element. Not all false information should be criminalized if there is no intent or purpose to cause harm. This is reinforced by Cipin (2019), who emphasizes the importance of intent in determining criminal liability for digital content.

Third, the *ultimum remedium* approach needs to be emphasized so that criminal law is only used when administrative or civil efforts are ineffective. This model is recommended in various international studies as a proportional approach to regulating digital content (Bygrave, 2017). Fourth, the ideal model must distinguish between (a) primary content creators, (b) redistributors who knowingly share false information, and (c) electronic system operators who facilitate dissemination, based on their roles and levels of fault. The criteria for this differentiation include the level of control over content, awareness of the falsity of information, and the intention to disseminate it. This hierarchical approach has been proposed in international literature to ensure fairness in digital law enforcement (Kaye, 2019). This role differentiation approach is also in line with the principle of criminal individualization in modern criminal law, which requires judges to consider the degree of fault and contribution of each perpetrator (Ashworth, 2013). Thus, criminal liability is not collective or automatic, but rather based on proof of a concrete role in the criminal act.

Empirically, this model is relevant considering the increasing number of digital information cases in Indonesia, where the lack of clear differentiation between actors has led to inconsistent legal outcomes. By applying a structured liability model, law enforcement can more accurately determine responsibility and avoid unjust criminalization. Furthermore, the proposed model is justified both normatively and theoretically, as it aligns with the principles of legality, fault, proportionality, and legal certainty, which are fundamental in modern criminal law systems. With this reconstruction, the ideal model of criminal liability allows for legal certainty, effective protection of society, and respect for freedom of expression within the Indonesian criminal justice system. To enhance practical implementation, this model can be applied through several concrete steps, including: (1) clarifying the definition of "false information" in legal provisions, (2) developing guidelines for proving intent (mens rea) in digital contexts, (3) applying proportionality in determining sanctions based on the role and level of fault, and (4) prioritizing non-penal measures such as correction mechanisms and administrative actions.

In relation to previous studies, this finding both supports and extends existing scholarship on criminal liability in digital information regulation. Prior research has emphasized the importance of intent (mens rea) as a fundamental element in determining criminal responsibility for the dissemination of false information (Cipin, 2019; Citron & Norton, 2011). This study supports these arguments by reaffirming that intent remains a central requirement in avoiding excessive criminalization. However, this study goes further by proposing a more structured approach through the differentiation of actors, namely between primary content creators, intentional redistributors, and electronic system operators. While earlier studies tend to focus primarily on the element of intent, they often do not provide a systematic framework for distinguishing levels of responsibility among different actors in the digital ecosystem. In addition, compared to previous literature that highlights the ambiguity of legal norms in the ITE Law (Nugroho, 2021; Kusumaningrum, 2023), this study expands the discussion by offering a prescriptive reconstruction model that integrates clarity of definitions, strict evidentiary standards, and proportionality in sanctions. Therefore, this study not only confirms existing theoretical perspectives but also contributes by refining and operationalizing them into a more applicable model of criminal liability within the Indonesian criminal justice system.

Despite its normative and theoretical strengths, the implementation of this model may face several potential challenges. These include differences in interpretation among law enforcement officials, limited technical capacity in handling digital evidence, and varying levels of digital literacy among the public. In addition, institutional resistance may arise due to the need for adjustments in existing legal practices, particularly in adopting stricter standards for proving intent and differentiating the roles of actors. Furthermore, the coexistence of general criminal law and special regulations such as the ITE Law may create overlapping interpretations, which could hinder consistent application. Therefore, effective implementation of this model requires institutional coordination, capacity building for law enforcement agencies, and the development of clear technical guidelines to minimize resistance and ensure consistency in practice.

ISSN [Online]: 2808-2923

## V. Conclusion

Based on the discussion, criminal liability for the dissemination of false information in Indonesia requires a more precise and consistent legal framework, particularly in ensuring clarity of definitions, proper assessment of intent, and proportional application of sanctions. While the ITE Law after the 2024 amendment provides a normative basis, its implementation still faces challenges related to ambiguity, inconsistent interpretation, and potential conflicts with freedom of expression. Therefore, the reconstruction of the criminal liability model emphasizes the need for clearer legal definitions, stricter standards in proving intent, and the application of proportionality, while positioning criminal law as an ultimum remedium. The model also highlights the importance of differentiating the roles of actors within the digital ecosystem to ensure fair and balanced accountability. Practically, this model can serve as a guideline for law enforcement officials and judges in determining criminal responsibility more proportionally and consistently, particularly in distinguishing cases that require criminal sanctions from those better addressed through administrative or civil mechanisms.

For future research, further empirical studies are needed to examine the implementation of the ITE Law in practice, including case-based analysis and comparative studies with other jurisdictions, in order to evaluate the effectiveness of the proposed model and refine its application. Future research should more specifically focus on empirical case studies of court decisions related to the dissemination of false information, particularly in analyzing how judges interpret the elements of intent (mens rea) and differentiate the roles of actors. In addition, comparative studies with jurisdictions that have more developed digital content regulations may provide insights into best practices for improving legal clarity and institutional coordination in Indonesia. With this approach, the criminal liability system for the dissemination of false information in Indonesia is expected to guarantee legal certainty, provide effective protection for the public, and continue to respect freedom of expression as a constitutional right in a state governed by the rule of law. Moving forward, the evolution of Indonesia's criminal law regarding the dissemination of digital information must continuously adapt to technological advancements and the shifting landscape of online communication. This requires strengthening regulatory frameworks, enhancing the capacity of law enforcement, and integrating digital literacy into broader legal policy. Future reforms should transcend mere normative clarity; they must focus on cultivating an adaptive and responsive legal system capable of addressing emerging forms of digital misinformation while meticulously balancing law enforcement objectives with the protection of fundamental rights..

## References

Allcott, H., & Gentzkow, M. (2017). Social Media and Fake News in the 2016 Election. Journal of Economic Perspectives, 31(2), 211–236.

Anriani, R. (2020). Protection of Freedom of Expression in Information and Electronic Transaction Law. Journal of Law and Development, 50(3), 512–530.

Arief, B. N. (2011). Anthology of Criminal Law Policy. jakarta: Kencana.

Ashworth, A. (2013). Principles of Criminal Law. Journal of Legal Studies. Oxford

Barda Nawawi Arief. (2019). Criminal Law Policy and Punishment. jakarta: Kencana.

Bassiouni, M. C. (2014). International Criminal Law. Journal of International Criminal Justice.

Bygrave, L. A. (2017). Data Protection Law: Approaching its Second Generation. Computer Law & Security Review.

Castells, M. (2009). Communication Power. Oxford University Press.

Chazawi, A. (2016). Criminal Law Lessons Part I. Jakarta: RajaGrafindo Persada.

Cipin, R. (2019). Intent and Criminal Responsibility in Digital Speech Regulation. International Journal of Law and Information Technology.

Citron, D. K., & Norton, H. (2011). Intermediaries and Hate Speech: Fostering Digital Citizenship for the Information Age. Harvard Civil Rights–Civil Liberties Law Review.

De Hert, P., & Papakonstantinou, V. (2016). The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals? Computer Law & Security Review.

Friedman, L. M. (1975). The Legal System: A Social Science Perspective. New York: Russell Sage Foundation.

Hamzah, A. (2015). Principles of Criminal Law. Jakarta: Rineka Cipta.

ISSN [Online]: 2808-2923

Ibrahim, J. (2006). Theory and Methodology of Normative Legal Research. Malang: Bayumedia Publishing.
Law Number 11 concerning Electronic Information and Transactions. State Gazette of the Republic of Indonesia Year 2008 Number 58., (2008).
Kaye, D. (2019). Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. United Nations Human Rights Council.
Kusumaningrum, D. (2023). Legal Challenges in Hoax Prosecution in Indonesia. Journal of Southeast Asian Legal Studies.
Republic of Indonesia., (2024).
Lazer, David M. J., et al. (2018). *The Science of Fake News*. *Science*, Vol. 359, No. 6380, pp. 1094–1096.
Marsden, C. T. (2017). Internet Co-Regulation and Constitutionalization of the Data Environment. Journal of Law and Society.
Moeljatno. (2008). Principles of Criminal Law. Jakarta: Rineka Cipta.
Muhammad, A. (2019). Hoaxes and Political Polarization in Indonesia. Journal of Social and Political Sciences, 22(1), 89–104.
Nugroho, S. (2021). The contradiction between freedom of expression and the crackdown on hoaxes in Indonesia. Journal of Legal Science, 18(2), 345–362.
Peter Mahmud Marzuki. (2017). Legal Research. Kencana.
Rahardjo, S. (2009). Progressive Law: A Synthesis of Indonesian Law. Yogyakarta: Genta Publishing.
Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions. State Gazette of the Republic of Indonesia of 2024., (2024).
Roxin, C. (2006). *Strafrecht Allgemeiner Teil*. Band I: Grundlagen. Der Aufbau der Verbrechenslehre. München: C.H. Beck.
Shirky, C. (2011). Cognitive Surplus: Creativity and Generosity in a Connected Age.
Situmorang, D. (2022). The Challenge of Proving Mens Rea in Cybercrime. Journal of Criminal Law and Criminology, 14(1), 98.
Soekanto, S. (2014). Introduction to Legal Research. Jakarta: UI Press.
Sudarto. (1990). Principles of Criminal Law. Bandung: Alumni.
Sudarto. (2010). Criminal Law I. Semarang: Sudarto Foundation.
Wardle, C., & Derakhshan, H. (2017). *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*. Strasbourg: Council of Europe.