Journal of Legal and Cultural Analytics (JLCA)
Vol. 5, No. 2, 2026 : 163 - 174

Juridical Issues and the Application of Criminal Law Principles in Content-Related Offenses under the Electronic Information and Transactions Law

Muhammad Tri Apriyansyah Idris[1]*, Adi Mansar[2]
[1]Magister Program in Law, Universitas Muhammadiyah Sumatera Utara
[2]Lecturer, Faculty of Law, Universitas Muhammadiyah Sumatera Utara
Corresponding Author: Muhammad Tri Apriyansyah Idris
triapriyansyah@gmail.com, adimansar@umsu.ac.id

A R T I C L E I N F O

Keywords: ITE Law, Cybercrime, Illegal Content, Law Enforcement, Effectiveness

Received : 05 March 2026
Revised : 15 April 2026
Accepted: 25 May 2026

A B S T R A C T

The Electronic Information and Transactions Law (ITE Law) is the primary legal framework in Indonesia, regulating various acts in the digital space as non-conventional crimes. This study aims to analyze the effectiveness and challenges of cybercrime law enforcement, with a particular focus on content crimes. Using a juridical-normative research method, this study examines the implementation of the principle of criminal responsibility and the validity of electronic evidence in judicial practice. The results indicate that while the ITE Law is quite effective in addressing technical crimes such as hacking, its effectiveness in combating content crimes remains limited due to the problem of "rubber articles" that are open to multiple interpretations, sanctions with a low deterrent effect, marked by a recidivism rate above 40%, and limited technical capacity of law enforcement officers. Therefore, reformulation and harmonization of regulations with the Criminal Code and the Personal Data Protection Law (PDP) are needed to create adaptive, equitable law enforcement that still guarantees freedom of expression in cyberspace.

DOI : https://doi.org/10.55927/jlca.v5i2.16415
ISSN-E: 2961-807X
https://journal.formosapublisher.org/index.php/jlca

INTRODUCTION

The massive development of information technology has shifted the paradigm of crime from conventional forms to non-conventional crimes occurring in the digital space (Cahyono et al., 2025). This phenomenon encompasses a broad spectrum, from electronic transaction fraud and online gambling to data manipulation and insults on social media. In response to these dynamics, the Electronic Information and Transactions Law (UU ITE) has emerged as the primary legal framework in Indonesia, aiming to protect technology users, ensure legal certainty, and regulate content that is detrimental to society.

Normatively, the ITE Law criminalizes various behaviors in cyberspace, broadly divided into the clusters of content violations, economic crimes, and technical attacks. However, the primary focus of debate in criminal law discourse is content-related crimes (Budiyanto, 2025). This cluster is regulated in Articles 27 to 28 of the ITE Law, which encompass content that violates morality, gambling, insults or defamation, extortion, and the spread of false news that harms consumers.

From a criminal law perspective, the applicability of the ITE Law in prosecuting content crimes must be in line with the principle of legality (nullum delictum nulla poena sine praevia lege poenali) (Mansar, 2017). Researchers highlight that one of the requirements of the legality principle is lex certa (the rules must be clear) and lex stricta (the rules must be firm). In this regard, criminal law expert Sudikno Mertokusumo emphasized that legal certainty demands clarity in the formulation of norms to prevent arbitrary interpretation (Mertokusumo, 2007). However, in practice, Articles 27 and 28 of the ITE Law are considered "rubber articles". This is in line with Andi Hamzah's criticism that the formulation of crimes in the ITE Law often adopts the concept of krenkeng (insult) from the Criminal Code but without rigid limitations, thus blurring the distinction between objective criticism and subjective insults (Hamzah, 2010). This broad interpretation threatens freedom of expression and creates a chilling effect phenomenon in society.

Furthermore, the application of the ITE Law to content crimes is closely related to the principle of criminal responsibility. The application of the ITE Law is closely related to the principle of fault (geen straf zonder schuld). Judges, when deciding cyber cases, must apply general principles that require fault (mens rea), an unlawful act (actus reus), and the perpetrator's capacity to take responsibility without any excuse (Pakpahan, 2024). In content crimes, proving mens rea becomes particularly complex. Referring to Moeljatno's doctrine, criminal acts and criminal responsibility are two separate entities (dualism) (Moeljatno, 2002). In the digital context, intent (dolus) is often distorted by the anonymity and speed of interaction. Researchers observe that law enforcement officials often fall into the trap of legal positivism, which only examines the fulfillment of the elements of a crime textually (formally) without delving deeper into the subjective aspects or the digital cultural context underlying the upload. This is complicated by a system of evidence that relies on electronic evidence, such as electronic

information, electronic documents, and printouts, which are recognized as valid under Article 5 of the ITE Law and used alongside evidence in the Criminal Procedure Code (KUHAP).

The evidentiary system relying on electronic evidence under Article 5 of the ITE Law is a manifestation of the principle of Lex Specialis Derogat Legi Generali, where the ITE Law serves as a special regulation that overrides general criminal procedure law (KUHAP) regarding the expansion of evidence. However, challenges arise in the aspect of digital integrity. Without strict digital forensics procedures in accordance with ISO standards, electronic evidence is vulnerable to manipulation, which in turn can violate the principle of Individualization of Criminal Procedure (CRI) that punishment must be targeted to the perpetrator who is truly guilty (Natsir, 2024).

Although the ITE Law provides a strong basis for prosecuting various forms of cybercrime, the effectiveness of its law enforcement in reducing crime rates is still considered limited. This is reflected in data showing that crime trends continue to increase, yet many cases remain unresolved. Furthermore, current criminal justice practices are considered weak and have a low deterrent effect, as evidenced by a recidivism rate of over 40% (Putra, 2023). Researchers assess that the sanctions imposed are relatively light compared to the social impact or economic losses resulting from these crimes.

From the perspective of the Relational or Objective Theory (Doeltheorieen), criminal justice should aim to protect society and rehabilitate. The relatively light sanctions compared to the social impacts (such as cyberbullying leading to depression or massive financial losses) indicate an imbalance in the application of the Principle of Proportionality. Researchers assess that the current criminal policy in the ITE Law is more reactive than preventative-educational, thus failing to create a substantial deterrent effect in cyberspace.

Another obstacle that arises in enforcing the law on content crimes is the lack of technical capacity of law enforcement officials and adequate digital forensic infrastructure. Problems with inter-agency coordination and challenges in handling cross-border crime also weaken the ITE Law's position as a crime prevention instrument. Jurisdiction and international cooperation often act as barriers when perpetrators of content crimes operate from outside Indonesia but target domestic electronic systems.

On the other hand, there is a problem of overlapping regulations between the ITE Law and the Criminal Code (KUHP). This regulatory disharmony requires reformulation to make the ITE Law more adaptable to future technological developments such as artificial intelligence (AI) and crypto, while also aligning with the Personal Data Protection Law (PDP Law). Without harmonization, legal uncertainty in the application of sanctions to perpetrators of content crimes will persist.

Based on the above description, there is a significant gap between the normative objective of the ITE Law to create order in the digital space and the reality of law enforcement, which still faces challenges in interpretation, enforcement capacity, and the effectiveness of sanctions. Therefore, this research

is crucial in analyzing how to reconstruct criminal policy regarding content crimes under the ITE Law to ensure justice without compromising human rights and freedom of expression in Indonesia.

LITERATURE REVIEW

In criminal law doctrine, the principle of legality not only requires written rules (lex scripta) but also demands clarity of formulation (lex certa) and strict limitations on interpretation (lex stricta) (Kurniawan et al., 2023). The ITE Law, in regulating content crimes such as insults, defamation, and the spread of false news (Articles 27 and 28), is deemed to fail to meet the lex certa standard.

Researchers highlight that many articles in the ITE Law are open to multiple interpretations, known academically as "rubber articles." The unclear parameters of the criminal elements in these articles lead to overly broad discretion by law enforcement, which in turn threatens freedom of expression and the right to criticize the government (Oktaviani, 2024). This situation creates legal uncertainty, where content can be interpreted differently depending on the subjectivity of officials, thus undermining the essence of the ITE Law's original purpose: to provide legal certainty in the digital space. According to Sudikno Mertokusumo, legal certainty is not merely the certainty of the law, but also the assurance of protection against arbitrary action by those in power (Mertokusumo, 1990). The unclear parameters of criminal elements in the "rubber articles" of the ITE Law align with Jan Remmelink's concern that vague legal norms will result in judges acting as lawmakers (rechter als wetgever), which violates the principle of the separation of powers. The excessive discretion of law enforcement resulting from the absence of lex certa directly threatens freedom of expression as a constitutional right (Jan, 2003).

The application of the principle of criminal responsibility in content crimes requires careful proof of the duality between the unlawful act (actus reus) and the fault or malicious intent (mens rea) (Mansar & Lubis, 2023). In cyberspace, proving these two elements relies heavily on electronic evidence recognized as valid under Article 5 of the ITE Law, such as electronic information, electronic documents, and their printouts.

According to Moeljatno, his dualistic teachings emphasize a clear separation between criminal acts and criminal responsibility (Moeljatno, 2002). In the cyber context, researchers observe that proving mens rea is often overlooked. As explained by Romli Atmasasmita, in cybercrime, the aspect of "intent" must be explored through in-depth digital forensics because the actus reus in cyberspace is often automatic or triggered by algorithms. Without the support of credible digital evidence and objective expert interpretation, substantive justice is difficult to achieve because judges tend to be trapped by rigid legal positivism without considering the sociological-digital context of a post.

However, critical reviews reveal significant gaps in technical capacity and digital forensic infrastructure. Without adequate technical capacity, proving mens rea often becomes bogged down in the formalities of evidence, without

delving deeply into the perpetrator's subjective motives. This limitation, coupled with a lack of institutional coordination, results in incomplete law enforcement against complex content crimes. Judges are required to apply the principle of general accountability, but without the support of credible digital evidence and objective expert interpretation, substantive justice for both defendants and victims is difficult to achieve.

Referring to Jeremy Bentham's Relative Theory or Objective Theory (Doeltheorieën), punishment should provide the benefit of deterrence.

If recidivism rates are high, the specific deterrent function is deemed to have failed (Bentham, 2006). Barda Nawawi Arif emphasized that criminal policy must integrate penal (criminal law) and non-penal (literacy and technology) policies (Arief, 1998). Light sentences or sentences disproportionate to the social damage indicate that the ITE Law has not been able to achieve its goals of restorative justice or distributive justice in the digital space.

Although the ITE Law imposes quite severe sanctions, such as up to six years in prison and billions of rupiah in fines for defamation or fraud, in practice, the sentences imposed are often deemed too lenient or disproportionate to the social damage caused. These weak sanctions, combined with low public awareness of digital security, have led to a continued rise in content crime without any significant practical reduction.

The ITE Law's ineffectiveness is also rooted in overlapping regulations with the Criminal Code and the challenges of cross-border crime. The ITE Law does have extraterritorial reach (Article 37), but its enforcement often runs up against the sovereignty of other countries and a lack of international cooperation.

Therefore, reformulation and harmonization of the ITE Law with the national criminal code (KUHP), the Personal Data Protection Law (PDP), and the Cyber Security and Resilience Law (KKS) are needed. This reform must include strengthening the technical capacity of the authorities and increasing cybersecurity literacy among the public. Without harmonized regulations that adapt to future technologies like AI and crypto, the ITE Law will remain a reactive instrument full of loopholes for multiple interpretations, rather than a just protector of digital sovereignty.

METHODOLOGY

This research employs a normative legal research method, emphasizing the study of positive legal norms, principles, and criminal law doctrines relevant to cybercrimes (Hadjon, 2003). The primary focus of this study is to analyze the consistency between the formulation of articles in the ITE Law and the basic principles of substantive criminal law through a statute approach, specifically regarding the cluster of prohibited acts in Articles 27 to 37. This approach allows researchers to map the main framework for handling cybercrimes, both technical in nature and those related to illegal content.

Furthermore, this research employs a conceptual approach to examine academic discourse on the phenomenon of "rubber articles" and potential threats to freedom of expression in the digital space. To provide a limited overview of

law enforcement practices, a case approach is also used, analyzing patterns of legal application in several specific crimes (Soekanto & Mamudji, 2001). These cases include defamation through social media, the distribution of online gambling links, electronic transaction fraud, such as concert ticket fraud, and data manipulation on fake accounts.

The legal sources in this study are categorized into primary and secondary legal sources to ensure doctrinal depth of analysis. The primary legal sources are primarily derived from the regulations of the Electronic Information and Transactions (ITE) Law, which regulate content that violates morality, extortion, fake news, and electronic system disruption (Eddy & Manurung, n.d.). Meanwhile, secondary legal sources are obtained from previous research, which summarizes approximately 16 types of prohibited acts, as well as literature on the principles of criminal liability involving the elements of fault (mens rea) and unlawful acts (actus reus).

The legal sources were collected through a literature review, which inventoried data related to the validity of electronic evidence, including electronic information and documents under the ITE Law. Using deductive reasoning, this study evaluates the challenges of cross-border law enforcement and the limitations of the technical capacity of authorities to formulate recommendations for regulatory harmonization that adapt to future technological developments.

RESEARCH RESULT

Typology and Categorization of Content Crimes Within the ITE Law

Based on a normative legal review of positive law in Indonesia, the Electronic Information and Transactions Law (ITE Law) constructs various acts in cyberspace as non-conventional crimes. The legal rationale (legal objective) of this regulation is oriented towards protecting legal subjects, ensuring legal certainty, and mitigating the spread of destructive content within society. Specifically, within the content-related crimes cluster, this study identifies 16 typologies of unlawful acts regulated prescriptively in Articles 27 to 37 of the ITE Law.

The following is a classification of content crimes and their corresponding criminal penalties based on the provisions of the ITE Law:

Table 1. Categories of Content-Based Offenses and Corresponding Criminal Penalties under the ITE Law

Tipologi Delik	Landasan Yuridis & Karakteristik	Ancaman Pidana Maksimal
Defamasi/Pencemaran Nama Baik	Pasal 27(3) jo. Pasal 45(1); terkualifikasi sebagai delik aduan.	Pidana penjara 6 tahun dan/atau denda Rp1 miliar.
Penyelenggaraan Perjudian Daring	Pasal 27(2) jo. Pasal 45(2); mencakup distribusi tautan situs perjudian.	Merujuk pada yurisprudens in concreto: pidana penjara 1 tahun 8 bulan & denda Rp250 juta.*
Disinformasi (Berita Bohong/Hoaks)	Pasal 28(1) jo. Pasal 45A(1); berdampak pada kerugian konsumen.	Pidana penjara hingga 6 tahun dan/atau denda.
Ujaran Kebencian Berbasis SARA	Pasal 28(2); distribusi informasi yang mendiseminasi permusuhan.	Mengikuti ketentuan ancaman pidana pada Pasal 45A.

Beyond content offenses, the ITE Law also accommodates technical-based crimes (computer-related crimes) such as illegal access hacking, illegal interception, and electronic data manipulation as stipulated in Articles 30 to 36. The significance of this regulation lies in the adoption of the extraterritorial principle, which allows for the expansion of jurisdiction to unlawful acts committed outside Indonesian territory, as long as they impact the national jurisdictional electronic system.

Implementation of the Doctrine of Criminal Responsibility and the Dimension of Proof

In the practical context of cybercriminal justice, the panel of judges imperatively applies the principle of conventional criminal responsibility, based on Simons' doctrine of strafbaar feit, which requires proof of both subjective fault (mens rea) and the material unlawful act (actus reus) (Mansar, 2017). In this regard, Moeljatno, through his dualism doctrine, emphasizes that criminal punishment must distinguish between the criminal act and criminal responsibility (Moeljatno, 2002).

Criminal liability can only be realized if the legal subject possesses the capacity to be accountable for their actions (toerekeningsvatbaarheid)—as Van Hamel emphasizes, that the capacity to be responsible is a psychological state such that an act can be held accountable to the perpetrator. Furthermore, the perpetrator must be free from any justification (rechtvaardigingsgrond) or excuse (schulduitsluitingsgrond).

The evidentiary dimension (bewijsrecht) in cybercrime represents a particular characteristic through the existence of electronic evidence. Referring to Article 5 of the ITE Law, this instrument has legal legitimacy as an extension of the evidence regulated in Article 184 of the Criminal Procedure Code (KUHAP). In this regard, Andi Hamzah argues that the evidentiary system in cyber cases

must not abandon the principle of negatief wettelijk stelsel (a negative system of proof based on law), where a judge's conviction must rely on at least two valid pieces of evidence (Hamzah, 2010).

While this normative construction provides a comprehensive legal basis for the pro-justitia phase, the validation of electronic evidence requires technical capabilities and the availability of standardized digital forensics infrastructure. As warned by Indriyanto Seno Adji, the integrity of electronic evidence is highly dependent on a chain of custody mechanism to ensure data authenticity and prevent manipulation that could violate the defendant's rights to due process (Subhan Suryadi Putra, 2024).

Critical Analysis: Effectiveness, Normative Ambiguity, and Law Enforcement Challenges

Although the implementation of the ITE Law is considered quite optimal in responding to technical cybercrimes, its effectiveness in addressing content-based crimes still shows disparities and limitations. Referring to Lawrence M. Friedman's postulate, legal effectiveness is highly dependent on three components of the legal system: structure, substance, and legal culture (Friedman, 1975). In the context of the ITE Law, several fundamental problems distort the effectiveness of this regulation, including:

1. Ambiguity of Legal Norms (Catch-all Provisions): The formulation of Articles 27 and 28 often triggers multiple interpretations. Sudikno Mertokusumo emphasized that the law must comply with the principle of certainty (rechtssicherheit) to prevent arbitrariness (Mertokusumo, 1990). The non-limiting wording of the norms in the ITE Law implies that this regulation is vulnerable to being used as an instrument of repression against freedom of speech. This aligns with Jan Remmelink's critique of the dangers of vague norms, which grant authorities too much discretion, risking criminalizing legitimate public criticism (Jan, 2003).
2. Ineffectiveness of the Deterrent Effect: Prescription of sanctions and sentencing practices are deemed disproportionate. Barda Nawawi Arief states that criminal policy must be a rational effort by society to combat crime (Arief, 2011). The high recidivism rate, exceeding 40%, confirms the failure of special prevention, as proposed by Jeremy Bentham's theory of the deterrent effect. According to Bentham, sanctions are only effective if the resulting suffering exceeds the benefits derived from crime (the utility principle) (Bentham, 2006).
3. Institutional Capacity Gap: Operational constraints stem from asymmetries in the technical capabilities of the authorities. Romli Atmasasmita, in his Integrative Legal Theory, emphasizes the importance of synergy between legal norms and bureaucratic behavior (Atmasasmita, 2012). The limited distribution of digital forensic infrastructure at the regional level hampers scientific crime

investigation, making legal certainty difficult to achieve outside major urban areas.

4. The Complexity of Transnational Jurisdiction: Law enforcement against organized cybercrime often encounters jurisdictional rigidity. Mochtar Kusumaatmadja reminds us that state sovereignty remains a fundamental principle in international law (Kusumaatmadja, 2002), but in cyberspace, this often becomes a stumbling block. Disharmony in cross-border cooperation instruments complicates prosecution of perpetrators located beyond Indonesia's territorial sovereignty.

Empirical data indicates an exponential curve in the prevalence of cybercrime, which, paradoxically, is not matched by a case clearance rate. This condition confirms Satjipto Rahardjo's postulate that the law often stumbles to catch up with the changing times (law lags behind the times) (Rahardjo, 2000). Furthermore, the overlapping of legal norms between the ITE Law and the Criminal Code degrades the principle of Lex Specialis Derogat Legi Generali, which according to Andi Hamzah should be applied consistently to ensure legal certainty and avoid dualism of prosecution that is detrimental to the accused (Afiah & Hamzah, 1989).

Strengthening Strategy: Legal Policy Reformulation and Synchronization

To address these various structural and substantial weaknesses, regulatory reform is absolutely necessary through a reformulation and synchronization of the ITE Law with related legal instruments. Barda Nawawi Arief emphasized that criminal law reform is essentially part of social policy, criminal policy, and law enforcement policy, which must be implemented in an integrated manner (Arif, 1997). This harmonization must involve reforming the National Criminal Code, the Personal Data Protection Law (PDP Law), and the urgent ratification of the Cyber Security and Resilience Bill (KKS).

This synchronization is crucial for constructing a future-proof cybercriminal justice system that adapts to the convergence of cutting-edge technologies. According to Romli Atmasasmita, in facing disruptions such as Artificial Intelligence and crypto assets, the law should not be limited to a conventional, positivistic approach, but rather must transform toward an Integrative Legal Theory that combines legal certainty, utility, and substantive justice (Atmasasmita, 2012).

Beyond the legislative dimension, strengthening interventions must be accompanied by a massive increase in cybersecurity awareness. This aligns with Soerjono Soekanto's view on the factors influencing law enforcement, stating that public legal awareness is an essential element for the law to function effectively as a means of social control (Soekanto, 1981). Furthermore, a comprehensive capacity-building program for law enforcement officers is needed to minimize disparities in technical understanding in the field.

Through this holistic approach, the ITE Law can transform from a mere retributive-punitive instrument, as criticized by Modernists (such as Van Hamel, who emphasizes the need for public protection), into a key pillar guaranteeing

cyber resilience and justice in the national digital ecosystem. As Roscoe Pound postulated that law is a tool of social engineering (Pound & DeRosa, 2017), the reform of the ITE Law must be able to direct the behavior of digital communities toward a cyber civilization that is ethical and based on sustainable legal certainty.

CONCLUSION AND RECOMMENDATION

Based on the discussion outlined above, it can be concluded that the ITE Law is the primary legal instrument in Indonesia for combating non-conventional cybercrimes, which encompass illegal content, economic crimes, and technical attacks. Although the ITE Law provides a strong legal foundation—particularly in recognizing valid electronic evidence—its implementation in practice still faces serious dogmatic challenges. The unclear wording of several articles, often referred to as "rubber articles," gives rise to multiple interpretations, which risk threatening freedom of expression and creating legal uncertainty.

Furthermore, the ITE Law's effectiveness in reducing cybercrime is considered limited. This is indicated by the relatively high recidivism rate, above 40%, and criminal sanctions that are deemed insufficient to provide a maximum deterrent effect for perpetrators of complex crimes. Technical obstacles such as limited digital forensic infrastructure, insufficient law enforcement capacity, and legal challenges in handling transnational crimes are the main obstacles to achieving thorough and just law enforcement.

To strengthen the effectiveness of cybercrime law enforcement in Indonesia, it is necessary to reformulate and harmonize regulations between the ITE Law and the Criminal Code, the PDP Law, and the KKS Bill to be more adaptive to the latest technological developments such as artificial intelligence (AI), crypto, and transnational crime. Furthermore, the government must prioritize increasing the technical capacity of law enforcement officers and strengthening digital forensic infrastructure to ensure the process of proving cybercrime is carried out professionally and accurately. Given the often cross-border nature of cybercrime, strengthening international cooperation in jurisdictional matters and information exchange is crucial for prosecuting perpetrators operating outside Indonesia. Finally, increasing cybersecurity literacy among the public and businesses is crucial to raise awareness of rights and obligations in the digital space so that potential criminal acts can be prevented early.

REFERENCES

Afiah, R. N., & Hamzah, A. (1989). *Barang bukti dalam proses pidana*. Sinar Grafika.
Arief, B. N. (1998). *Beberapa aspek kebijakan penegakan dan pengembangan hukum pidana*. Citra Aditya Bakti.

Arief, B. N. (2011). *Reformasi sistem peradilan: sistem penegakan hukum di Indonesia*.Badan Penerbit, Universitas Diponegoro.

Arif, B. N. (1997). Beberapa Pokok Pemikiran Kebijakan Penanggulangan Tindak Pidana Korupsi. *Seminar Sehari Tentang Mencari Solusi Dan Model-Model Pemberantasan Korupsi, Kolusi, Dan Manipulasi Di Lembaga Penegakkan Hukum Indonesia,(Semarang 1997)*.

Atmasasmita, R. (2012). *Teori Hukum Integratif: Rekonstruksi Terhadap teori Hukum Pembangunan dan Teori Hukum Progresif*. Genta Publishing.

Bentham, J. (2006). Teori Perundang-Undangan Prinsip-Prinsip Legislasi, Hukum Perdata dan Hukum Pidana. *Bandung: Penerbit Nusamedia & Penerbit Nuansa*.

Budiyanto, S. H. (2025). *Pengantar Cybercrime dalam Sistem Hukum Pidana di Indonesia*. Sada Kurnia Pustaka.

Cahyono, S. T., Erni, W., & Hidayat, T. (2025). Rikonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cyber Crime) Dalam Sistem Peradilan Pidana Indonesia: Rekonstruksi Hukum Pidana terhadap Kejahatan Siber (Cyber Crime) dalam Sistem Peradilan Pidana Indonesia. *Dame Journal of Law*, *1*(1), 111–133.

Eddy, T., & Manurung, R. S. (n.d.). *Metodologi Penelitian Dalam Ilmu Hukum Lingkungan Metodologi Penelitian*.

Friedman, L. M. (1975). *The legal system: A social science perspective*. Russell Sage Foundation.

Hadjon, P. M. (2003). *Penelitian hukum normatif*. Kumpulan Tulisan, Fakultas Hukum Universitas Airlangga.

Hamzah, A. (2010). *Hukum acara pidana Indonesia*. Sinar Grafika.

Jan, R. (2003). *Hukum Pidana: Komentar atas Pasal-Pasal Terpenting dari Kitab Undang-undang Hukum Pidana Belanda dan Padanannya dalam Kitab Undangundang Hukum Pidana Indonesia*. Gramedia Pustaka Utama.

Kurniawan, M. A., Eddy, T., & Mansar, A. (2023). Perlindungan Hukum Terhadap Anak Yang Berkonflik Dengan Hukum Dalam Sistem Peradilan Pidana Anak. *Seminar Nasional Hukum, Sosial Dan Ekonomi*, *2*(1), 89–98. Kusumaatmadja, M. (2002). *Konsep-konsep hukum dalam Pembangunan*. Alumni.

Mansar, A. (2017). Bunga Rampai Politik Hukum Pidana Pemberantasan Korupsi Melalui Hukum Responsif. In *Pustaka Prima*. Pustaka Prima.

Mansar, A., & Lubis, I. (2023). Harmonization of Indonesian criminal law through the new criminal code towards humane law. *Journal of Law and Sustainable Development*, *11*(12), e2381–e2381.

Mertokusumo, S. (1990). *Mengenal Hukum Suatu Pengantar*. Liberty.

Mertokusumo, S. (2007). *Penemuan hukum: Sebuah pengantar*.

Moeljatno. (2002). *Asas-asas Hukum Pidana*. Rineka Cipta.

Natsir, M. (2024). *Formulasi Pemidanaan Dalam Tindak Pidana Manipulasi Dokumen Elektronik Berbasis Keadilan (Studi Kasus: Putusan PN Pangkalan Bun, No. 134/Pid. Sus/2023/PN. Pbu)*. Universitas Islam Sultan Agung Semarang.

Oktaviani, S. (2024). Konstitusi Dan Kebebasan Berpendapat Di Indonesia: Analisis Keterbatasan Dan Perlindungan: Kebebasan Perpendapat di Indonesia. *Jurnal Ilmiah Ekonomi Dan Manajemen*, *2*(7), 174–186.

Pakpahan, J. (2024). Pertanggungjawaban Pidana Perbuatan Ujaran Kebencian Yang Berkonten SARA Dalam Perspektif Peraturan Perundang-Undangan. *Journal of Law Education and Business*, *2*(2).

Pound, R., & DeRosa, M. L. (2017). *An introduction to the philosophy of law*. Routledge.

Putra, J. S. A. A. M. (2023). hacking as a challenge for change and the development of cyber law in Indonesia. *Jurnal Ilmu Hukum Tambun Bungai*, *8*(2), 344–355.

Rahardjo, S. (2000). *Ilmu hukum*. Citra Aditya Bakti.

Soekanto, S. (1981). *Fungsi Hukum dan Perubahan Sosial*. Alumni.

Soekanto, S., & Mamudji, S. (2001). Penelitian Hukum Normatif: Suatu Tinjauan Singkat. In *PT Raja Grafindo Persada*. PT Raja Grafindo Persada.

Subhan Suryadi Putra. (2024). *Kekuatan Bukti Elektronik Dalam Pembuktian Perkara Tindak Pidana Korupsi Di Indonesia*. Universitas Islam Sultan Agung Semarang.