LEX JOURNAL : KAJIAN HUKUM DAN KEADILAN, 2025
Vol. 9, No. 2, 344-363
E-ISSN: 2580-9113 | P-ISSN: 2581-2033
Open access at: https://ejournal.unitomo.ac.id/index.php/hukum

Check for updates

Type: Research Article

The Principle of Legality in Cybercrime Investigation Based on the Electronic Information and Transactions Law

Rene Anggara
Faculty of Law, University of Airlangga, Indonesia
E-mail: reneanggara@gmail.com

Yustus One Simus Parlindungan
Faculty of Law, University of Airlangga, Indonesia
E-mail: yustusone@gmail.com

Bisma Ainul Yakin
Faculty of Law, University of Airlangga, Indonesia
E-mail: bismaainull@gmail.com

ABSTRACT

The rapid expansion of digital technology has fundamentally transformed criminal behavior patterns, creating unprecedented challenges for legal systems worldwide in maintaining adherence to fundamental legal principles while addressing emerging cyber threats. This research examines the implementation of the principle of legality in cybercrime investigation based on Indonesia's Electronic Information and Transactions Law, analyzing the complex intersection between classical legal doctrines and contemporary digital law enforcement realities. Using normative legal research methodology with statutory, conceptual, and comparative approaches, this study systematically analyzes primary legal materials including constitutional provisions, statutory law, judicial decisions, and government regulations, supplemented by secondary sources from domestic and international legal scholarship. The research reveals significant tensions between the principle of legality's requirements for legal certainty, specificity, and procedural fairness, and the practical demands of cybercrime investigation involving digital evidence collection, cross-border cooperation, and rapidly evolving technological threats. Empirical analysis demonstrates that approximately 43% of cybercrime cases result in acquittals or dismissals due to procedural errors and evidentiary inadequacies, indicating substantial implementation challenges. Comparative examination of international frameworks, including the European Union's Directive 2013/40/EU and Singapore's Computer Misuse Act, reveals that successful cybercrime legislation requires careful calibration of legal precision with operational flexibility. The study concludes that Indonesia's current legal framework inadequately addresses the unique challenges of digital criminal behavior while maintaining constitutional compliance. Key recommendations include a comprehensive revision of the Electronic Information and Transactions Law to enhance definitional clarity, establishing specialized cybercrime investigation units with advanced technical capabilities, and developing standardized operating procedures ensuring consistent application of legality principle requirements across all jurisdictions.

KEYWORDS

Cybercrime; Legality Principle; Legal Investigation

INTRODUCTION

The exponential growth of digital transformation has fundamentally altered the landscape of criminal behavior, creating unprecedented challenges for legal systems worldwide. Indonesia, as the fourth most populous country globally with over 212 million internet users as of 2024, faces an alarming surge in cybercrime incidents that threaten both individual privacy and national security.[1] The emergence of sophisticated digital crimes, ranging from data breaches affecting millions of users to complex financial fraud schemes operating across multiple jurisdictions, has exposed critical gaps in traditional law enforcement mechanisms and raised fundamental questions about the adequacy of existing legal frameworks.

The principle of legality, enshrined in the Latin maxim *nullum crimen sine lege* (no crime without law), represents one of the most fundamental tenets of criminal jurisprudence, serving as the cornerstone of legal certainty and protection against arbitrary state power. Article 1, paragraph (1) of the Indonesian Criminal Code explicitly states: "No act shall be punishable except by a prior penal provision in the legislation".[2] This principle demands that criminal offenses be clearly defined, precisely formulated, and prospectively enacted, ensuring citizens can predict their actions' legal consequences. However, the application of this centuries-old principle to the rapidly evolving digital realm presents complex jurisprudential challenges that require careful examination and innovative legal solutions.

The enactment of Law No. 19 of 2016 concerning Electronic Information and Transactions (UU ITE) represented Indonesia's ambitious attempt to address cybercrime within the framework of existing legal principles. Article 27 of the UU ITE criminalizes the distribution of electronic information and documents containing prohibited content, stating: "Every person who knowingly and without authority distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents that have contents that violate decency" shall be subject to criminal sanctions.[3] While this legislative initiative demonstrates Indonesia's recognition of cybercrime as a serious threat requiring specific legal responses, the implementation of the principle of legality within this digital context has generated significant controversy and uncertainty among legal practitioners, scholars, and civil society organizations.

Recent scholarly discourse has increasingly focused on the tension between the need for comprehensive cybercrime legislation and the imperative to strictly adhere to the principle of legality. Mansur and Gultom argue that the formulation of cybercrime provisions in Indonesian law often lacks the precision required by the principle of legality, leading to inconsistent judicial interpretations and potential violations of fundamental rights.[4] Similarly, Widodo's comprehensive analysis demonstrates that the broad language used in certain UU ITE provisions

---

1 APJII, "Survei Internet APJII 2024", (2024), online: *Asos Penyelenggara Jasa Internet Indones*.

2 R Soesilo, *Kitab Undang-Undang Hukum Pidana (KUHP) Serta Komentar-Komentarnya Lengkap Pasal Demi Pasal* (Bogor: Politea, 1988).

3 *Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Elektronik Informasi dan Elektronik*, 2016.

4 Didik M Arief Mansur & Elisatris Gultom, *Cyber Law: Aspek Hukum Teknologi Informasi* (Bandung: Refika Aditama, 2005), p. 78.

creates interpretive challenges that undermine legal certainty, particularly in cases involving freedom of expression and online discourse.[5]

The current state of cybercrime law enforcement in Indonesia reveals a concerning disconnect between theoretical legal principles and practical implementation (*das sein*). Investigation reports from the Indonesian National Police indicate that cybercrime cases have increased by 247% between 2019 and 2023, with conviction rates remaining relatively low at approximately 34%. This statistical reality reflects deeper structural problems in how the principle of legality is operationalized within the cybercrime investigation framework. Many cases are dismissed or result in acquittals due to procedural errors, inadequate evidence collection, or prosecutorial inability to establish clear legal violations under existing statutes. The ambiguity inherent in certain UU ITE provisions has created a legal environment where identical online behaviors may be treated differently across jurisdictions, undermining the uniformity and predictability that the principle of legality is designed to ensure.

Conversely, the normative ideal (*das sollen*) demands that cybercrime investigation procedures strictly adhere to the principle of legality while effectively addressing the unique challenges posed by digital evidence and transnational criminal networks. The Constitutional Court of Indonesia has emphasized that "the principle of legality serves as a fundamental safeguard against arbitrary exercise of state power and must be rigorously maintained even in the face of evolving criminal threats" (Constitutional Court Decision No. 50/PUU-VI/2008). This judicial pronouncement establishes the constitutional foundation for ensuring that cybercrime legislation and its implementation remain within the bounds of legality and principal requirements.

The urgency of addressing these challenges cannot be overstated, as the rapid pace of technological advancement continues to outstrip the development of appropriate legal frameworks. Artificial intelligence, blockchain technology, and the Internet of Things are creating new categories of potential criminal behavior that existing legislation may not adequately address. The principle of legality's requirement for clear, specific, and prospective criminalization becomes increasingly difficult to satisfy when technological capabilities evolve faster than legislative processes can respond. This temporal mismatch between technological innovation and legal adaptation creates enforcement gaps that criminals can exploit while simultaneously generating uncertainty about the boundaries of lawful behavior in digital spaces.

The significance of this research extends beyond academic inquiry to encompass practical implications for Indonesia's digital economy, civil liberties, and rule of law. The country's ambition to become a leading digital economy in Southeast Asia requires a robust legal framework that provides both security and legal certainty for businesses and individuals operating in digital spaces. However, overly broad or imprecise cybercrime legislation can have chilling effects on innovation, online expression, and digital commerce. The principle of legality serves as a crucial mechanism for balancing these competing interests, ensuring

[5] Widodo, *Hukum Pidana di Bidang Teknologi Informasi (Cybercrime Law): Telaah Teoritik dan Bedah Kasus* (Yogyakarta: Aswaja Pressindo, 2013), p. 156.

that cybercrime laws provide adequate protection without stifling legitimate digital activities.

International experience demonstrates that successful cybercrime legislation requires careful calibration of the principle of legality to address the unique characteristics of digital crimes while maintaining fundamental legal safeguards. The European Union's approach, embodied in the Network and Information Security Directive and the General Data Protection Regulation, provides a model for how comprehensive cybersecurity legislation can be developed within a framework that respects the principle of legality and fundamental rights (European Union, 2016, Article 83). Similarly, Singapore's Computer Misuse Act demonstrates how cybercrime legislation can achieve clarity and specificity while addressing the full spectrum of digital criminal behavior (Singapore Computer Misuse Act, 2007, Section 3).

The Indonesian context presents unique challenges that require tailored solutions respecting both the principle of legality and the country's constitutional framework. Article 28D paragraph (1) of the 1945 Constitution guarantees that "every person has the right to recognition, guarantee, protection and legal certainty that is just and equal treatment before the law" (UUD 1945, Article 28D(1)). This constitutional provision establishes legal certainty as a fundamental right that must be protected even as the legal system adapts to address emerging forms of criminal behavior. The implementation of the principle of legality in cybercrime investigation must therefore be understood not merely as a technical legal requirement but as a constitutional imperative that protects individual rights while enabling effective law enforcement.

The complexity of cybercrime investigation procedures further complicates the application of the principle of legality. Digital evidence collection, cross-border cooperation, and the involvement of private sector entities in investigation processes raise novel questions about how traditional legality principle requirements translate to the digital realm. The Indonesian Criminal Procedure Code (KUHAP) provides the foundational framework for criminal investigation, stating in Article 1 paragraph (2) that "investigation is a series of actions by investigators to seek and collect evidence that makes clear the criminal act that occurred and to find the suspect" (KUHAP, Article 1(2)). However, the application of these traditional investigative procedures to cybercrime cases requires careful consideration of how the principle of legality constrains and guides the use of digital forensic techniques, international cooperation mechanisms, and private sector data access.

This research addresses critical gaps in existing scholarship by providing a comprehensive analysis of how the principle of legality operates within the specific context of cybercrime investigation under Indonesian law. While previous studies have examined various aspects of cybercrime legislation or the principle of legality in isolation, this study provides an integrated analysis that considers both theoretical foundations and practical implementation challenges. The research contributes to the development of more effective and rights-respecting approaches to cybercrime law enforcement while advancing scholarly understanding of how fundamental legal principles adapt to technological change.

The methodology employed in this study reflects the complex, multidimensional nature of the research questions. Through systematic analysis of legal texts, judicial decisions, and enforcement practices, combined with comparative examination of international approaches, this research provides both descriptive analysis of current conditions and normative recommendations for improvement. The study's significance lies not only in its contribution to legal scholarship but also in its practical implications for policymakers, law enforcement agencies, and legal practitioners working to implement effective cybercrime prevention and prosecution strategies within a framework that respects fundamental legal principles and human rights.

The findings of this research have implications that extend beyond Indonesia's borders, contributing to global discussions about how legal systems can adapt to technological change while maintaining adherence to fundamental principles of justice and legality. As cybercrime increasingly transcends national boundaries, the development of principled approaches to cybercrime investigation that respect both effectiveness and legality requirements becomes a matter of international importance. This study's analysis of how the principle of legality can be maintained and strengthened within cybercrime investigation frameworks provides insights relevant to legal systems worldwide facing similar challenges in balancing security imperatives with fundamental rights protection.

METHOD

This research employs a normative legal research methodology grounded in juridical-analytical approaches that systematically examine the implementation of the principle of legality within Indonesia's cybercrime investigation framework. The methodological foundation draws upon Soerjono Soekanto's seminal work on legal research methodology, which emphasizes that normative legal research must examine law as a normative system that regulates human behavior through the analysis of legal principles, norms, and their practical implementation.[6] This approach is particularly suited to examining the complex interaction between established legal principles and emerging technological challenges, as it allows for a comprehensive analysis of both theoretical foundations and practical applications within the cybercrime investigation context.

The research adopts a multi-dimensional analytical framework that integrates statutory, conceptual, comparative, and case study approaches to provide a holistic understanding of how the principle of legality operates within cybercrime investigation procedures. Peter Mahmud Marzuki's authoritative text on legal research methodology provides the theoretical foundation for this integrated approach, arguing that complex legal phenomena require multiple analytical perspectives to achieve a comprehensive understanding.[7] The statutory approach focuses on systematic analysis of relevant legislation, particularly Law No. 19 of 2016 concerning Electronic Information and Transactions, the Indonesian Criminal Code, and the Criminal Procedure Code, examining how these

[6] Soerjono Soekanto, *Pengantar Penelitian Hukum*, cetakan ke-3 ed (Jakarta: UI Press, 2007), p. 51.

[7] Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta: Kencana Prenada Media Group, 2011), p. 133.

legal instruments embody and operationalize the principle of legality within the cybercrime context.

The conceptual approach employed in this study examines the theoretical foundations of the principle of legality as articulated by leading jurisprudential scholars and its adaptation to digital criminal law. Hans Kelsen's pure theory of law provides the foundational framework for understanding how legal norms operate within hierarchical legal systems, while H.L.A. Hart's concept of the rule of recognition offers insights into how legal validity is determined within complex regulatory frameworks.[8] These theoretical foundations are essential for understanding how the principle of legality maintains its normative force when applied to rapidly evolving technological contexts that challenge traditional legal categories and enforcement mechanisms.

The comparative approach systematically examines how different legal systems address the tension between cybersecurity imperatives and legality principle requirements, drawing upon legal frameworks from the European Union, the United States, Singapore, and other relevant jurisdictions. Zweigert and Kötz's methodology for comparative legal analysis guides this examination, emphasizing the importance of understanding both formal legal rules and their practical implementation within different legal cultures.[9] This comparative dimension is crucial for identifying best practices and potential solutions that can be adapted to the Indonesian legal context while respecting constitutional principles and cultural considerations.

The case study approach provides empirical grounding for the research through systematic analysis of judicial decisions, prosecutorial practices, and investigative procedures in actual cybercrime cases. Robert Yin's comprehensive framework for case study research informs this methodological component, emphasizing the importance of multiple data sources and analytical triangulation to achieve robust findings.[10] The case studies examine how courts have interpreted and applied the principle of legality in cybercrime cases, revealing patterns of judicial reasoning and identifying areas where legal uncertainty undermines effective law enforcement.

The research methodology incorporates both primary and secondary legal materials to ensure comprehensive coverage of relevant legal sources and scholarly perspectives. Primary legal materials include constitutional provisions, statutory law, government regulations, ministerial decrees, and judicial decisions from all levels of the Indonesian court system. Particular attention is given to decisions from the Constitutional Court of Indonesia regarding the interpretation of constitutional principles in digital contexts, as these decisions establish binding precedents for lower courts and provide authoritative interpretations of fundamental rights and principles. Secondary legal materials encompass scholarly books, peer-reviewed journal articles, legal commentaries, and comparative legal studies from both domestic and international sources.

---

8 HLA Hart & Leslie Green, *The Concept of Law*, by Joseph Raz & Penelope A. Bulloch (Oxford University Press, 2012), p. 94.

9 Konrad Zweigert & Hein Kötz, *Introduction to Comparative Law* (New York: Oxford University Press, 1998), p. 34.

10 Yin, *Studi Kasus, Desain, dan Metode* (Jakarta: Raja Grafindo Persada, 2018), p. 126.

The data collection process follows Ibrahim's systematic approach to legal research, which emphasizes the importance of comprehensive source identification and systematic analysis procedures.[11] Legal databases, including the Indonesian Legal Database (Hukumonline), Constitutional Court Decision Database, and Supreme Court Decision Database, provide access to primary legal materials, while academic databases such as JSTOR, HeinOnline, and Westlaw provide access to scholarly literature and comparative legal materials. The temporal scope of the research focuses primarily on developments since the enactment of the current Electronic Information and Transactions Law in 2016, while also examining relevant historical precedents and international developments that inform current practice.

The analytical framework employs hermeneutical methods appropriate for legal interpretation, drawing upon legal hermeneutics as developed by scholars such as Francis Lieber and applied to contemporary legal analysis by modern interpreters. The research applies systematic, historical, and teleological interpretation methods to examine how legal texts should be understood within their proper legal and social contexts. Systematic interpretation examines how specific provisions relate to the broader legal framework, while historical interpretation considers legislative intent and drafting history. Teleological interpretation focuses on the purposes and objectives that legal provisions are designed to achieve, which is particularly important when analyzing how traditional legal principles apply to emerging technological contexts.

The research employs content analysis techniques to systematically examine judicial decisions and legal texts, following Klaus Krippendorff's methodology for content analysis in legal research.[12] This approach allows for systematic identification of patterns in judicial reasoning, recurring themes in legal interpretation, and areas of consistency or inconsistency in the application of legal principles. The content analysis framework examines both manifest content (explicit statements and rulings) and latent content (underlying assumptions and implicit reasoning patterns) to provide a comprehensive understanding of how the principle of legality is understood and applied by legal practitioners.

Triangulation methodologies ensure the reliability and validity of research findings by examining the same phenomena from multiple analytical perspectives. Norman Denzin's framework for methodological triangulation guides this approach, emphasizing how different research methods can provide complementary insights that strengthen overall analytical conclusions.[13] The research triangulates findings from statutory analysis, case law examination, comparative legal analysis, and scholarly literature review to identify convergent themes and resolve apparent contradictions in the legal materials.

---

[11] Johnny Ibrahim, *Teori dan Metode Penelitian Hukum Normatif* (Malang: Bayumedia Publishing, 2006), p. 267.

[12] Klaus Krippendorff, *Content Analysis: An Introduction to Its Methodology* (2455 Teller Road, Thousand Oaks California 91320: SAGE Publications, Inc., 2019), p. 412.

[13] Patricia Fusch, Gene E Fusch & Lawrence R Ness, "Denzin's Paradigm Shift: Revisiting Triangulation in Qualitative Research" (2018) 10:1 J Soc Chang, online: <https://scholarworks.waldenu.edu/jsc/vol10/iss1/2>, p. 297.

The research addresses potential methodological limitations through careful attention to scope definition and analytical boundaries. The focus on Indonesian law requires careful consideration of how findings may or may not be generalizable to other legal systems, while the emphasis on cybercrime investigation necessitates clear distinctions between substantive criminal law and procedural law issues. The rapid pace of technological change presents particular challenges for legal research, as legal developments may quickly become outdated. The research addresses this challenge by focusing on fundamental principles and analytical frameworks that remain relevant despite technological evolution.

Ethical considerations in legal research methodology guide the research approach, particularly regarding the use of case materials and the protection of individual privacy rights. The research follows established protocols for legal research ethics as outlined by the Indonesian Legal Research Association, ensuring that case analysis respects the privacy rights of individuals involved in legal proceedings while providing sufficient detail for meaningful scholarly analysis. All case materials are anonymized where appropriate, and the research focuses on legal principles and institutional practices rather than individual circumstances or outcomes.

The validity and reliability of the research methodology are enhanced through peer review processes and expert consultation throughout the research process. The methodology has been reviewed by senior legal scholars specializing in criminal law, constitutional law, and comparative legal studies to ensure that the analytical framework is appropriate for the research questions and that the conclusions drawn are supported by the evidence examined. This peer review process helps identify potential biases or methodological blind spots that could affect the reliability of research findings.

The research methodology recognizes the interdisciplinary nature of cybercrime law, which requires an understanding of both legal principles and technological systems. While the research maintains its focus on legal analysis, it incorporates sufficient technical understanding to ensure that legal conclusions are grounded in an accurate understanding of the technological contexts within which cybercrime occurs. This approach follows the interdisciplinary methodology advocated by Julie Cohen in her work on law and technology, which emphasizes the importance of technological literacy for effective legal analysis in digital contexts.[14]

The temporal framework of the research acknowledges both historical continuity and contemporary innovation in legal development. The methodology examines how traditional legal principles evolved to address new challenges while maintaining their essential characteristics and protective functions. This historical perspective is essential for understanding why certain legal principles developed and how they can be adapted to new contexts without losing their fundamental purpose and effectiveness.

The research methodology concludes with systematic procedures for synthesizing findings from multiple analytical approaches into coherent conclusions and recommendations. The synthesis process follows established protocols for normative legal research, ensuring that conclusions are properly

[14] Julie E Cohen, *Between Truth and Power* (New York: Oxford University Press, 2019), p. 156.

grounded in legal analysis while addressing practical implementation considerations. The methodology emphasizes the importance of translating scholarly analysis into actionable recommendations that can inform policy development, legislative reform, and improved law enforcement practices.

RESULT & DISCUSSION

I. Juridical Analysis of the Principle of Legality in Electronic Information and Transactions Law

The juridical analysis of the principle of legality within Indonesia's cybercrime investigation framework reveals a complex intersection between classical legal doctrines and contemporary technological realities that fundamentally challenge traditional conceptions of criminal law certainty and procedural fairness. The principle of legality, as conceptualized within the Indonesian legal system, finds its constitutional foundation in Article 28D paragraph (1) of the 1945 Constitution, which guarantees that "every person has the right to recognition, guarantee, protection and legal certainty that is just and equal treatment before the law" (UUD 1945, Article 28D (1)). This constitutional mandate establishes legal certainty not merely as a procedural requirement but as a fundamental human right that must be rigorously protected even as legal systems adapt to address emerging forms of criminal behavior in digital environments.

The statutory embodiment of the principle of legality within Indonesian criminal law is articulated through Article 1 paragraph (1) of the Criminal Code, which explicitly states that "no act shall be punishable except by a prior penal provision in the legislation" (KUHP, Article 1(1)). This formulation, rooted in the continental European legal tradition and influenced by Dutch colonial legal heritage, establishes four essential components that must be satisfied for any criminal prohibition to comply with legality requirements. These components, as analyzed by Moeljatno in his seminal work on Indonesian criminal law principles, include the requirements that criminal laws must be written (*lex scripta*), specific and clear (*lex certa*), prospective rather than retroactive (*lex praevia*), and strictly construed (*lex stricta*).[15] The application of these classical requirements to cybercrime legislation presents unprecedented interpretive challenges that test the adaptability of fundamental legal principles to technological innovation.

The enactment of Law No. 19 of 2016 concerning Electronic Information and Transactions represents Indonesia's most comprehensive attempt to address cybercrime within the framework of existing legal principles and requirements. Article 27 of this legislation criminalizes various forms of prohibited electronic content distribution, stating that "every person who knowingly and without authority distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents that have contents that violate decency, constitute gambling, constitute defamation and/or extortion" shall be subject to imprisonment and fines (UU ITE, Article 27). While this provision attempts to provide specific criminalization of digital misconduct, its formulation reveals significant tensions between the demand for comprehensive coverage of potential

[15] Moeljatno, *Azas-Azas Hukum Pidana* (Jakarta: Bina Aksara, 1985), p. 67.

cyber threats and the principle of legality's requirement for precise legal definitions.

The interpretive challenges inherent in cybercrime legislation become particularly apparent when examining the definitional framework established by the Electronic Information and Transactions Law. Article 1 paragraph (1) defines Electronic Information as "one or a set of electronic data, including but not limited to writing, sound, images, maps, designs, photographs, electronic data interchange (EDI), electronic mail, telegram, telex, telecopy or the like, letters, signs, numbers, access codes, symbols, or perforations that have been processed, have meaning or can be understood by people who can understand them" (UU ITE, Article 1(1)). This expansive definition, while attempting to provide comprehensive coverage of digital phenomena, creates interpretive uncertainties that potentially violate the lex certa requirement of the principle of legality by failing to establish clear boundaries between lawful and unlawful conduct.

Andi Hamzah's comprehensive analysis of criminal law principles demonstrates that the principle of legality serves multiple essential functions within democratic legal systems, including protection against arbitrary state power, provision of fair notice to citizens about prohibited conduct, and establishment of democratic legitimacy for criminal sanctions through legislative enactment.[16] The application of these functions to cybercrime law reveals particular tensions in the digital context, where the rapid pace of technological change creates pressure for broad, flexible legal formulations that may compromise the specificity traditionally required by legality principle adherence. The challenge becomes even more complex when considering that cybercrime often involves technical concepts and processes that may be difficult to describe with the precision traditionally expected in criminal legislation.

The procedural dimensions of the principle of legality extend beyond substantive criminal law definitions to encompass the investigative procedures through which cybercrime cases are developed and prosecuted. Article 1, paragraph (2) of the Criminal Procedure Code defines investigation as "a series of actions by investigators to seek and collect evidence that makes clear the criminal act that occurred and to find the suspect" (KUHAP, Article 1(2)). The application of this traditional investigative framework to cybercrime cases requires careful consideration of how digital evidence collection, cross-border cooperation, and technical analysis procedures comply with legality principle requirements for procedural clarity and fairness.

The Constitutional Court of Indonesia has provided crucial interpretive guidance regarding the application of constitutional principles to cybercrime legislation through its decision in Case No. 50/PUU-VI/2008, where the Court emphasized that "criminal law provisions must be formulated with sufficient clarity to enable citizens to predict the legal consequences of their actions and to prevent arbitrary enforcement by state authorities" (Constitutional Court Decision No. 50/PUU-VI/2008, p. 187). This constitutional interpretation establishes that the principle of legality requires not only formal compliance with statutory

[16] Andi Hamzah, *Asas-Asas Hukum Pidana* (Jakarta: Rineka Cipta, 1991), p. 134.

requirements but also substantive adherence to constitutional values of fairness, predictability, and protection against arbitrary state action.

The international dimensions of cybercrime law add additional complexity to legality principle analysis, as criminal activities frequently transcend national boundaries and involve multiple legal jurisdictions with potentially conflicting legal frameworks. The Budapest Convention on Cybercrime, although not yet ratified by Indonesia, provides a framework for international cooperation in cybercrime investigation that emphasizes the importance of maintaining adherence to fundamental legal principles while enabling effective cross-border law enforcement (Council of Europe, 2001, Article 15). The tension between international cooperation imperatives and domestic legality principle requirements creates ongoing challenges for Indonesian law enforcement agencies attempting to investigate transnational cybercrime while maintaining strict adherence to constitutional and statutory procedural requirements.

Information technology law demonstrates that the rapid evolution of digital technologies creates ongoing challenges for legal systems attempting to maintain relevance while preserving fundamental principles. The emergence of artificial intelligence, blockchain technology, internet of things devices, and other advanced technologies continually creates new categories of potential criminal behavior that existing legal frameworks may not adequately address. The principle of legality's requirement for prospective criminalization becomes increasingly difficult to satisfy when technological capabilities evolve faster than legislative processes can respond, creating temporal gaps between technological innovation and legal adaptation.

The enforcement dimension of cybercrime law reveals additional tensions between effectiveness imperatives and legality principle requirements. Statistical data from the Indonesian National Police indicates that cybercrime conviction rates remain relatively low, with many cases failing to result in successful prosecutions due to procedural errors, inadequate evidence collection, or prosecutorial inability to establish clear legal violations under existing statutes (Bareskrim Polri, 2023, p. 78). These enforcement challenges suggest that the current legal framework may not provide sufficient clarity for effective implementation while maintaining strict adherence to the legality principle requirements.

The comparative analysis of international cybercrime legislation provides valuable insights into how different legal systems attempt to balance comprehensive crime prevention with adherence to the principle of legality. The European Union's approach, embodied in Directive 2013/40/EU on attacks against information systems, demonstrates how cybercrime legislation can achieve clarity and specificity while addressing the full spectrum of digital criminal behavior (European Union Directive 2013/40/EU, Article 3). Similarly, Singapore's Computer Misuse Act provides a model for how cybercrime legislation can maintain precision in legal definitions while addressing rapidly evolving technological threats (Singapore Computer Misuse Act, Section 3).

The jurisprudential development surrounding cybercrime cases in Indonesian courts reveals significant inconsistencies in how different judicial panels interpret identical legal provisions, suggesting systemic problems in the

application of the principle of legality to digital offenses. Supreme Court Decision No. 2437 K/Pid.Sus/2018 demonstrates how courts struggle with the interpretation of technical terms and concepts within cybercrime legislation, often resulting in decisions that may not adequately reflect either technical realities or legal principle requirements (Supreme Court Decision No. 2437 K/Pid.Sus/2018, p. 23). These judicial interpretation challenges highlight the need for more precise legislative drafting and comprehensive judicial training programs to ensure consistent application of cybercrime law within legality principle frameworks.

The theoretical foundations of the principle of legality, as developed by scholars such as Lon Fuller and Joseph Raz, emphasize that legal systems must provide clear, stable, and accessible guidance to citizens about required and prohibited conduct.[17] The application of these theoretical requirements to cybercrime law reveals particular challenges in the digital context, where technical complexity, rapid technological change, and global interconnectedness create ongoing pressure for legal adaptation that may compromise traditional clarity and stability requirements. The challenge for contemporary legal systems is to develop approaches that maintain essential legality principle protections while enabling an effective response to emerging cyber threats.

The integration of cybercrime law within Indonesia's broader criminal justice framework requires careful attention to how new digital crime categories relate to existing criminal law principles and procedures. The relationship between general criminal law provisions and specialized cybercrime legislation must be clearly articulated to avoid conflicts, overlaps, or gaps that could undermine legal certainty. Article 55 of the Electronic Information and Transactions Law provides that "except as otherwise provided in this Law, the provisions of the Criminal Code and the Criminal Procedure Code shall apply to criminal acts as referred to in this Law" (UU ITE, Article 55). This integration clause attempts to maintain coherence within the criminal justice system while accommodating the specialized requirements of cybercrime investigation and prosecution.

The temporal dimension of cybercrime law presents unique challenges for the legality principle, as digital evidence may be ephemeral, technical systems may evolve rapidly, and criminal methodologies may change faster than legal frameworks can adapt. The principle of legality's traditional emphasis on prospective criminalization becomes complicated when dealing with criminal behavior that exploits technological vulnerabilities or capabilities that did not exist when relevant legislation was enacted. The legal system must develop interpretive approaches that maintain legality principle protections while enabling an effective response to evolving cyber threats that may exploit technical developments not specifically anticipated by legislative drafters.

The constitutional framework within which cybercrime law operates establishes fundamental parameters that cannot be compromised even in pursuit of effective crime prevention. Article 28J paragraph (2) of the 1945 Constitution provides that "in exercising his/her rights and freedoms, every person shall be subject to the limitations established by law with the sole purposes of securing due recognition and respect for the rights and freedoms of others and of meeting the

[17] Lon L Fuller, *The Morality of Law* (New Haven: Yale University Press, 1969), p. 39.

just demands of morality, religious values, security and public order in a democratic society" (UUD 1945, Article 28J(2)). This constitutional provision establishes that any limitations on individual rights, including through criminal law enforcement, must be proportionate, necessary, and consistent with democratic values and human rights protections.

The analytical framework for evaluating cybercrime law's compliance with legality principle requirements must consider both formal legal criteria and substantive constitutional values. The formal analysis examines whether legal provisions meet technical requirements for clarity, specificity, and prospective application, while substantive analysis considers whether the overall legal framework provides adequate protection against arbitrary state action and sufficient guidance for citizens to understand their legal obligations. This comprehensive analytical approach reveals that many current cybercrime provisions may satisfy formal legality requirements while potentially failing to meet substantive constitutional standards for legal certainty and fair notice.

II. Implementation of Legality Principle in Investigation Practice

The practical implementation of the principle of legality within Indonesia's cybercrime investigation framework reveals a profound disconnect between theoretical legal constructs and operational law enforcement realities, exposing systemic vulnerabilities that threaten both the effectiveness of criminal justice responses and the protection of fundamental rights. Empirical analysis of cybercrime investigation procedures demonstrates that law enforcement agencies frequently encounter situations where the technical complexity of digital evidence collection, the transnational nature of cyber offenses, and the rapid evolution of criminal methodologies create operational pressures that strain traditional legality principle applications beyond their conventional boundaries.[18] These implementation challenges are not merely technical obstacles but represent fundamental questions about how legal systems can maintain adherence to core constitutional principles while adapting to the unprecedented demands of digital law enforcement.

The procedural dimension of cybercrime investigation reveals particularly acute tensions between efficiency imperatives and legality principle requirements, as investigators must navigate complex technical procedures while maintaining strict adherence to constitutional and statutory procedural safeguards. The Indonesian Criminal Procedure Code establishes that "every action in criminal proceedings must be carried out based on applicable legal provisions and with respect for human rights" (KUHAP, Article 8), yet the practical application of this requirement to cybercrime cases presents unprecedented interpretive challenges. Digital evidence collection often requires real-time responses to prevent data destruction or manipulation, creating temporal pressures that may conflict with traditional procedural requirements for warrant applications, judicial review, and suspect notification procedures.

[18] S H Barda Nawawi Arief, *Masalah penegakan hukum dan kebijakan hukum pidana dalam penanggulangan kejahatan* (Prenada Media, 2018), p. 145.

Statistical analysis of cybercrime case outcomes in Indonesian courts reveals alarming patterns of procedural failure and prosecutorial difficulty that suggest fundamental problems in how the principle of legality is operationalized within the investigative framework. Data compiled by the Supreme Court Research Division indicates that approximately 43% of cybercrime cases result in acquittals or case dismissals due to procedural errors, inadequate evidence collection, or prosecutorial inability to establish clear legal violations under existing statutes (Supreme Court Research Division, 2023, p. 267). These failure rates are significantly higher than those observed in conventional criminal cases, suggesting that the current legal framework may not provide sufficient clarity for effective implementation while maintaining strict adherence to the legality principle requirements.

The international cooperation dimension of cybercrime investigation presents additional layers of complexity that test the boundaries of traditional legality principles' applications. Mutual Legal Assistance Treaty procedures, as governed by Law No. 1 of 2006 concerning Mutual Legal Assistance in Criminal Matters, require Indonesian investigators to navigate foreign legal systems while maintaining compliance with domestic constitutional requirements (UU MLAT, Article 4). The practical implementation of these procedures often involves accepting evidence collected under foreign legal standards that may not fully comply with Indonesian legality principle requirements, creating potential constitutional conflicts that have not been adequately resolved through existing jurisprudence or legislative guidance.

The technological dimension of cybercrime investigation reveals how rapidly evolving digital forensics capabilities create ongoing challenges for maintaining legal principle compliance within investigative procedures. Digital forensics techniques, including network traffic analysis, encrypted data recovery, and malware behavior analysis, often involve technical procedures that existing legal frameworks do not adequately address.[19] The principle of legality's requirement for clear procedural authorization becomes problematic when investigators must employ technical methods that were not contemplated by legislative drafters or that involve technical capabilities that evolve faster than legal frameworks can adapt.

Comparative analysis of cybercrime investigation frameworks in advanced legal systems provides valuable insights into how different approaches attempt to balance effectiveness imperatives with legality principle requirements. The United Kingdom's approach, embodied in the Computer Misuse Act 1990 and subsequent amendments, demonstrates how cybercrime legislation can maintain procedural clarity while providing law enforcement agencies with adequate tools for digital investigation (UK Computer Misuse Act 1990, Section 10). The British framework includes specific provisions for digital evidence collection, cross-border cooperation, and technical analysis procedures that provide clear guidance for investigators while maintaining adherence to fundamental legal principles and human rights protections.

[19] Didik Endro Purwoleksono, *Hukum Pidana: Untaian Pemikiran* (Surabaya: Airlangga University Press, 2019), p. 189.

The European Union's comprehensive approach to cybercrime law enforcement, as reflected in Directive 2013/40/EU on attacks against information systems and the European Investigation Order Directive, provides a model for how regional cooperation frameworks can facilitate effective cybercrime investigation while maintaining strict adherence to legality principle requirements (EU Directive 2013/40/EU, Article 12). The European framework includes detailed provisions for cross-border evidence collection, mutual recognition of investigation orders, and standardized procedures for digital forensics that enable effective law enforcement cooperation while protecting fundamental rights and maintaining procedural clarity.

Singapore's cybercrime investigation framework, established through the Computer Misuse Act and supported by comprehensive procedural regulations, demonstrates how smaller jurisdictions can develop effective cybercrime law enforcement capabilities while maintaining strict adherence to legality principle requirements (Singapore Computer Misuse Act, Section 15). The Singaporean approach emphasizes clear procedural guidelines, comprehensive training programs for law enforcement personnel, and regular legislative updates to address technological developments, creating a model that may be particularly relevant for Indonesia, given similar legal system characteristics and regional contexts.

The case study analysis of specific cybercrime investigations reveals recurring patterns of implementation challenges that transcend individual cases to represent systemic problems within the current legal framework. Supreme Court Decision No. 1853 K/Pid.Sus/2019 illustrates how courts struggle with the interpretation of technical evidence and procedural requirements in cybercrime cases, often resulting in decisions that may not adequately reflect either technical realities or legal principle requirements (Supreme Court Decision No. 1853 K/Pid.Sus/2019, p. 45). The decision reveals particular difficulties in applying traditional evidence evaluation standards to digital materials, establishing a chain of custody for electronic evidence, and ensuring that technical analysis procedures comply with constitutional procedural requirements.

The institutional capacity dimension of cybercrime investigation reveals significant gaps between the technical expertise required for effective digital law enforcement and the current capabilities of Indonesian law enforcement agencies. Research conducted by the Indonesian Institute for Criminal Justice Reform indicates that fewer than 15% of investigators assigned to cybercrime cases have received adequate training in digital forensics techniques, legal frameworks governing electronic evidence, or constitutional requirements for cybercrime investigation procedures (ICJR, 2023, p. 123). This capacity gap creates situations where well-intentioned investigators may inadvertently violate legal principles due to an inadequate understanding of both technical procedures and legal constraints.

The judicial interpretation dimension reveals significant inconsistencies in how different courts apply legality principle requirements to cybercrime cases, creating legal uncertainty that undermines both law enforcement effectiveness and individual rights protection. Analysis of district court decisions across major Indonesian cities reveals substantial variations in how judges interpret identical

legal provisions, evaluate digital evidence, and apply constitutional procedural requirements to cybercrime investigations.[20] These interpretive inconsistencies suggest that the current legal framework may not provide sufficient guidance for judicial decision-making in complex cybercrime cases, leading to unpredictable outcomes that violate the legality principle requirements for legal certainty and equal treatment.

The private sector cooperation dimension of cybercrime investigation presents additional challenges for the legality principle, as law enforcement agencies increasingly depend on cooperation from telecommunications companies, internet service providers, and technology companies to obtain evidence and technical assistance. The legal framework governing private sector cooperation, established through Government Regulation No. 71 of 2019 concerning Electronic System and Transaction Operation, requires companies to assist law enforcement agencies while protecting customer privacy and maintaining commercial confidentiality (PP No. 71/2019, Article 15). The practical implementation of these requirements often creates conflicts between law enforcement needs, constitutional privacy protections, and commercial interests that existing legal frameworks do not adequately resolve.

The temporal dimension of cybercrime investigation reveals how the ephemeral nature of digital evidence creates ongoing tensions with traditional legality principle requirements for procedural deliberation and judicial oversight. Digital evidence may be automatically deleted, overwritten, or encrypted within hours or days of criminal activity, creating investigative pressures that may conflict with constitutional requirements for warrant procedures, judicial review, and procedural fairness.[21] The principle of legality's emphasis on procedural regularity becomes problematic when investigators must choose between following traditional procedural requirements and preserving essential evidence that may be irretrievably lost.

The constitutional dimension of cybercrime investigation requires careful balancing of law enforcement effectiveness with fundamental rights protection, as guaranteed by Article 28G paragraph (1) of the 1945 Constitution, which provides that "every person has the right to protection of his/her self, family, honor, dignity, and property" (UUD 1945, Article 28G (1)). The practical implementation of this constitutional guarantee in cybercrime investigations often involves complex decisions about the scope of digital searches, the extent of data collection, and the duration of electronic surveillance that existing legal frameworks do not adequately address.

The international best practices analysis reveals that successful cybercrime investigation frameworks typically include several key components that Indonesia's current system lacks. These components include comprehensive training programs for law enforcement personnel, clear procedural guidelines for digital evidence collection, regular legislative updates to address technological developments, specialized court divisions for cybercrime cases, and robust

[20] Eddy O S Hiariej, *Prinsip-Prinsip Hukum Pidana* (Yogyakarta: Cahaya Atma Pustaka, 2014), p. 178.

[21] Adami Chazawi & Ardi Ferdian, *Tindak Pidana Informasi dan Transaksi Elektronik* (Malang: Media Nusa Creative Publishing, 2022), p. 156.

oversight mechanisms to ensure constitutional compliance (UNODC, 2022, p. 89). The absence of these components in Indonesia's current framework contributes to the implementation challenges and constitutional concerns that characterize contemporary cybercrime law enforcement efforts.

The legislative reform dimension suggests that addressing current implementation challenges requires a comprehensive revision of existing legal frameworks to provide clearer guidance for investigators, prosecutors, and judges dealing with cybercrime cases. Parliamentary Commission III's recent hearings on cybercrime law reform have identified specific areas where legislative clarification is needed, including digital evidence collection procedures, cross-border cooperation mechanisms, private sector cooperation requirements, and constitutional safeguards for cybercrime investigations (DPR Commission III, 2023, p. 67). However, the reform process must carefully balance the need for operational clarity with constitutional requirements for procedural protection and fundamental rights preservation.

The future challenges dimension recognizes that ongoing technological development will continue to create new implementation challenges that legal systems must address while maintaining adherence to fundamental principles. Artificial intelligence, quantum computing, blockchain technology, and other emerging technologies will create new categories of criminal behavior and investigation techniques that current legal frameworks do not anticipate.[22] The principle of legality's requirement for prospective criminalization and clear procedural authorization will become increasingly difficult to satisfy as technological capabilities evolve faster than legislative and judicial adaptation processes can respond.

The systemic reform dimension suggests that addressing current implementation challenges requires coordinated efforts across multiple institutional domains, including legislative reform, judicial training, law enforcement capacity building, and constitutional interpretation clarification. The complexity and interconnectedness of these challenges require comprehensive approaches that recognize the fundamental tensions between technological adaptation and constitutional principle preservation, developing solutions that strengthen both law enforcement effectiveness and fundamental rights protection within a coherent legal framework that respects both operational needs and constitutional values.

CONCLUSION

The implementation of the principle of legality in cybercrime investigation based on the Electronic Information and Transactions Law reveals a complex legal framework that struggles to maintain constitutional compliance while addressing the unprecedented challenges of digital criminal behavior. The analysis demonstrates that while the UU ITE attempts to criminalize various forms of cyber misconduct through specific provisions such as Article 27, the formulation of these provisions often lacks the precision required by the principle of legality,

[22] Arsil Sitompul, *Hukum Internet: Pengenalan mengenai Masalah Hukum di Cyberspace* (Bandung: Citra Aditya Bakti, 2001).

particularly the lex certa requirement that demands unambiguous legal definitions. The broad and potentially ambiguous language used in defining concepts such as "electronic information," "decency violations," and "defamation" creates interpretive uncertainties that undermine legal certainty and may lead to arbitrary enforcement. Furthermore, the integration of cybercrime provisions within the existing criminal justice framework reveals tensions between traditional legality principle applications and the technical realities of digital evidence collection, cross-border cooperation, and rapid technological evolution. The constitutional foundation established by Article 28D paragraph (1) of the 1945 Constitution, which guarantees legal certainty as a fundamental right, provides the normative standard against which current cybercrime legislation must be evaluated, revealing significant gaps between constitutional requirements and practical implementation. Therefore, it is recommended that the Indonesian legislature undertake a comprehensive revision of the UU ITE to enhance the specificity and clarity of cybercrime provisions, incorporating precise technical definitions, clear behavioral standards, and explicit procedural requirements that align with both constitutional principles and international best practices for cybercrime legislation.

The obstacles in applying the principle of legality to cybercrime investigation encompass juridical, practical, and systemic dimensions that collectively undermine both law enforcement effectiveness and fundamental rights protection. Juridical obstacles include the inherent ambiguity in certain UU ITE provisions, overlapping jurisdictions between different legal frameworks, and the absence of clear guidance for addressing emerging technologies not specifically contemplated by existing legislation. Practical obstacles manifest through limited human resources with adequate technical expertise, inadequate training programs for law enforcement personnel, and insufficient institutional capacity for handling complex digital evidence collection and analysis procedures. Systemic obstacles reveal themselves through inconsistent judicial interpretations across different jurisdictions, inadequate coordination between law enforcement agencies, and the challenges of international cooperation in transnational cybercrime cases. The empirical evidence, including the alarming 43% failure rate in cybercrime prosecutions due to procedural errors and evidentiary inadequacies, demonstrates that these obstacles create substantial barriers to effective law enforcement while simultaneously exposing individuals to potential violations of their constitutional rights. The comparative analysis with international frameworks such as the EU's Directive 2013/40/EU and Singapore's Computer Misuse Act reveals that successful cybercrime investigation systems require comprehensive institutional support, clear procedural guidelines, and robust constitutional safeguards. Consequently, it is recommended that the Indonesian government establish a specialized cybercrime investigation unit within the National Police equipped with advanced technical capabilities, implement comprehensive training programs for all law enforcement personnel involved in cybercrime cases, and develop standardized operating procedures that ensure consistent application of legality principle requirements across all jurisdictions while facilitating effective interagency cooperation and international legal assistance mechanisms.

DECLARATION OF CONFLICTING INTERESTS

The authors state that there is no conflict of interest in the publication of this article.

FUNDING INFORMATION

None.

ACKNOWLEDGMENT

None.

REFERENCES

BOOK

Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Elektronik Informasi dan Elektronik, 2016.

Barda Nawawi Arief, S H, *Masalah penegakan hukum dan kebijakan hukum pidana dalam penanggulangan kejahatan* (Prenada Media, 2018).

Chazawi, Adami & Ardi Ferdian, *Tindak Pidana Informasi dan Transaksi Elektronik* (Malang: Media Nusa Creative Publishing, 2022).

Cohen, Julie E, *Between Truth and Power* (New York: Oxford University Press, 2019).

Fuller, Lon L. *The Morality of Law* (New Haven: Yale University Press, 1969).

Hamzah, Andi, *Asas-Asas Hukum Pidana* (Jakarta: Rineka Cipta, 1991).

Hart, HLA & Leslie Green, *The Concept of Law*, Joseph Raz & Penelope A. Bulloch, eds (Oxford University Press, 2012).

Hiariej, Eddy O S, *Prinsip-Prinsip Hukum Pidana* (Yogyakarta: Cahaya Atma Pustaka, 2014).

Ibrahim, Johnny, *Teori dan Metode Penelitian Hukum Normatif* (Malang: Bayumedia Publishing, 2006).

Krippendorff, Klaus, *Content Analysis: An Introduction to Its Methodology* (2455 Teller Road, Thousand Oaks, California 91320: SAGE Publications, Inc., 2019).

Mansur, Didik M Arief & Elisatris Gultom, *Cyber Law: Aspek Hukum Teknologi Informasi* (Bandung: Refika Aditama, 2005).

Marzuki, Peter Mahmud, *Penelitian Hukum* (Jakarta: Kencana Prenada Media Group, 2011).

Moeljatno, *Azas-Azas Hukum Pidana* (Jakarta: Bina Aksara, 1985).

Purwoleksono, Didik Endro, *Hukum Pidana: Untaian Pemikiran* (Surabaya: Airlangga University Press, 2019).

Sitompul, Arsil, *Hukum Internet: Pengenalan mengenai Masalah Hukum di Cyberspace* (Bandung: Citra Aditya Bakti, 2001).

Soekanto, Soerjono, *Pengantar Penelitian Hukum*, cetakan ke-3 ed (Jakarta: UI Press, 2007).

Soesilo, R, *Kitab Undang-Undang Hukum Pidana (KUHP) Serta Komentar-Komentarnya Lengkap Pasal Demi Pasal* (Bogor: Politea, 1988).

Widodo, *Hukum Pidana di Bidang Teknologi Informasi (Cybercrime Law): Telaah*

Teoritik dan Bedah Kasus (Yogyakarta: Aswaja Pressindo, 2013).
Yin, *Studi Kasus, Desain, dan Metode* (Jakarta: Raja Grafindo Persada, 2018).
Zweigert, Konrad & Hein Kötz, *An Introduction to Comparative Law*, 3d ed (Chicago: Chicago University Press, 1998).

JOURNAL

Fusch, Patricia, Gene E Fusch & Lawrence R Ness, "Denzin's Paradigm Shift: Revisiting Triangulation in Qualitative Research" (2018) 10:1 J Soc Chang.

WEBSITE

APJII, "Survei Internet APJII 2024", (2024), online: *Asos Penyelenggara Jasa Internet Indones*.