

Penegakan Hukum terhadap Modus Penipuan Berbasis Digital sebagai Bentuk Kejahatan Siber di Indonesia

Law Enforcement Against Digital Fraud Schemes as a Form of Cybercrime in Indonesia

Imam Aldina Rouf, Ni Nyoman Tri Partini

Fakultas Hukum, Universitas Safin Pati, Pati, Indonesia
imamaldina93@gmail.com

Abstract

*This study aims to analyze the legal framework for law enforcement against digital fraud schemes as a form of cybercrime in Indonesia from the perspective of substantive criminal law and criminal procedural law. The rapid development of information technology has transformed conventional fraud into cyber-enabled offences conducted through electronic systems, including phishing, social engineering, fake online stores, fraudulent investment schemes, and digital identity misuse. These developments have generated significant legal issues, including regulatory overlap between the Indonesian Criminal Code and the Electronic Information and Transactions Law, challenges in electronic evidence, and the limited effectiveness of criminal procedural law in addressing technology-based offences. These conditions underline the necessity of developing a comprehensive law enforcement framework capable of ensuring legal certainty in combating digital fraud. This research employs a normative juridical method using statutory, conceptual, and case approaches through qualitative analysis of primary, secondary, and tertiary legal materials. The novelty of this study lies in developing an integrated law enforcement framework that combines the Electronic Information and Transactions Law as *lex specialis*, the Indonesian Criminal Code as *lex generalis*, and the Criminal Procedure Code as the procedural basis for electronic evidence in digital fraud cases. The findings demonstrate that effective law enforcement depends upon harmonized criminal legislation, consistent application of the *lex specialis derogat legi generali* principle, strengthened digital forensic evidence, and enhanced inter-agency as well as cross-border cooperation to ensure legal certainty, justice, and legal utility in addressing cybercrime.*

Keywords: *Cybercrime; Digital Fraud; Law Enforcement*

Abstrak

Penelitian ini bertujuan menganalisis konstruksi penegakan hukum terhadap modus penipuan berbasis digital sebagai bentuk kejahatan siber di Indonesia dalam perspektif hukum pidana materiil dan hukum acara pidana. Perkembangan teknologi informasi telah mengubah karakteristik penipuan konvensional menjadi kejahatan siber yang memanfaatkan sistem elektronik melalui berbagai modus, seperti *phishing*, *social engineering*, toko daring fiktif, investasi ilegal, dan penyalahgunaan identitas digital. Perkembangan tersebut memunculkan persoalan hukum berupa tumpang tindih pengaturan antara Kitab Undang-Undang Hukum Pidana dan Undang-Undang Informasi dan Transaksi Elektronik, kompleksitas pembuktian elektronik, serta belum optimalnya penerapan hukum acara pidana dalam menangani kejahatan berbasis teknologi. Kondisi tersebut menunjukkan pentingnya perumusan konstruksi penegakan hukum yang mampu memberikan kepastian hukum terhadap penanganan penipuan digital. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan kasus melalui analisis kualitatif terhadap bahan hukum primer, sekunder, dan tersier. Kebaruan penelitian terletak pada pengembangan konstruksi penegakan hukum yang mengintegrasikan penerapan Undang-Undang Informasi dan Transaksi Elektronik sebagai *lex specialis*,

Kitab Undang-Undang Hukum Pidana Nasional sebagai *lex generalis*, dan Kitab Undang-Undang Hukum Acara Pidana sebagai sistem pembuktian dalam perkara penipuan digital. Hasil penelitian menunjukkan bahwa efektivitas penegakan hukum ditentukan oleh harmonisasi norma hukum pidana, konsistensi penerapan asas *lex specialis derogat legi generali*, penguatan pembuktian elektronik berbasis forensik digital, serta peningkatan koordinasi antarlembaga dan kerja sama lintas yurisdiksi untuk mewujudkan kepastian hukum, keadilan, dan kemanfaatan dalam penanganan kejahatan siber.

Kata kunci: Kejahatan Siber; Penegakan Hukum; Penipuan Digital

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang berlangsung pesat telah membawa transformasi mendasar dalam pola interaksi sosial dan ekonomi masyarakat. Di balik kemudahan yang ditawarkannya, kemajuan tersebut turut melahirkan ragam kejahatan baru yang dikenal sebagai kejahatan siber (*cybercrime*). Salah satu bentuk yang paling marak adalah penipuan berbasis digital, yang memanfaatkan ruang siber sebagai sarana untuk mengelabui korban. Indonesia bahkan mencatat lebih dari empat ratus juta insiden siber sepanjang tahun 2023, sebuah angka yang menggambarkan betapa seriusnya ancaman ini.¹

Modus penipuan digital terus berkembang mengikuti laju teknologi, mulai dari pengelabuan melalui tautan palsu (*phishing*), toko daring fiktif, arisan dan investasi bodong, hingga pemalsuan identitas dengan teknologi kecerdasan buatan. Salah satu kasus yang menyita perhatian publik adalah penipuan menggunakan teknologi *deepfake* yang memalsukan wajah pejabat negara untuk memperdaya korban.² Keberagaman modus ini menunjukkan bahwa penipuan digital bukan sekadar pergeseran sarana, melainkan evolusi kualitatif yang menuntut respons hukum yang adaptif.

Secara konvensional, penipuan diatur dalam Pasal 378 Kitab Undang-Undang Hukum Pidana, yang mengancam pelaku dengan pidana penjara paling lama empat tahun bagi siapa pun yang menggunakan nama palsu, tipu muslihat, atau rangkaian kebohongan untuk menggerakkan orang lain menyerahkan sesuatu.³ Dalam rekodifikasi hukum pidana, ketentuan penipuan ini dimuat dalam Pasal 492 Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, yang berlaku efektif sejak 2 Januari 2026.⁴

¹ Fauzan Mahdi Irawan, Muhammad Zibran Al Habsy, and Asmak Ul Hosnah, "Pertanggungjawaban Pidana Pelaku *Phishing* Dan Efektivitas Penegakan Hukum Berdasarkan UU Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik," *Jurnal Komputer, Informasi Dan Teknologi* 5, no. 2 (2025), <https://doi.org/10.53697/jkomitek.v5i2.3159>.

² Siti Yona Hukmana, "Kasus Penipuan *Deepfake* AI: Polri Buru Pelaku Pemalsuan Wajah Presiden Prabowo," *Media Indonesia*, 2025, <https://mediaindonesia.com/politik-dan-hukum/737308/kasus-penipuan-deepfake-ai-polri-buru-pelaku-pemalsuan-wajah-presiden-prabowo>.

³ Alfany Restu Anda, Sri Astutik, and Ernu Widodo, "Analisis Pertimbangan Hakim Dalam Penerapan Pasal 378 KUHP Pada Perkara Penipuan Kredit," *RIGGS: Journal of Research and Innovation in Global Governance Studies* 5, no. 1 (2025), <https://doi.org/10.31004/riggs.v5i1.6281>.

⁴ Indonesia, "Undang-Undang Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana" (2023), <https://peraturan.bpk.go.id/Details/234935/uu-no-1-tahun-2023>.

Untuk mengisi kekosongan hukum tersebut, negara mengandalkan Undang-Undang Informasi dan Transaksi Elektronik sebagai *lex specialis*.⁵ Pasal 28 ayat (1) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 melarang setiap orang mendistribusikan informasi elektronik yang berisi pemberitahuan bohong yang mengakibatkan kerugian materiel bagi konsumen dalam transaksi elektronik.⁶ Pelanggaran atas ketentuan tersebut diancam pidana penjara paling lama enam tahun dan/atau denda paling banyak satu miliar rupiah berdasarkan Pasal 45A ayat (1). Pembaruan ini memperlihatkan upaya negara menyesuaikan instrumen hukum dengan dinamika kejahatan digital.

Sejumlah penelitian terdahulu telah mengkaji penegakan hukum terhadap berbagai bentuk kejahatan siber di Indonesia. Penelitian yang dilakukan oleh Tuju (2025) menganalisis penegakan hukum terhadap tindak pidana penipuan jual beli *online* melalui perspektif kriminologi. Penelitian tersebut menunjukkan bahwa penipuan digital umumnya dilakukan melalui media sosial dan *marketplace* dengan memanfaatkan identitas palsu, iklan fiktif, serta harga yang tidak wajar. Hasil penelitiannya menegaskan bahwa efektivitas penegakan hukum masih terkendala keterbatasan regulasi, rendahnya literasi digital masyarakat, serta kesulitan penelusuran pelaku lintas yurisdiksi. Fokus penelitian tersebut lebih menitikberatkan pada faktor kriminologis dan strategi penanggulangan kejahatan penipuan *online*, tanpa membahas harmonisasi pengaturan hukum pidana materil dan hukum acara pidana dalam penanganan penipuan digital.⁷

Penelitian lain yang dilakukan oleh Dzaky (2025) mengkaji strategi pencegahan kejahatan siber melalui sinergi antara Undang-Undang Informasi dan Transaksi Elektronik dengan kebijakan keamanan digital nasional. Penelitian tersebut menyimpulkan bahwa keberadaan Undang-Undang Informasi dan Transaksi Elektronik telah memberikan dasar hukum dalam penanggulangan kejahatan siber, namun implementasinya masih menghadapi berbagai kendala, seperti lemahnya koordinasi antarlembaga, keterbatasan kapasitas aparat penegak hukum, serta belum optimalnya kebijakan keamanan digital. Meskipun memberikan kontribusi terhadap pengembangan strategi pencegahan kejahatan siber, penelitian tersebut belum secara khusus mengkaji penegakan hukum terhadap berbagai modus penipuan berbasis digital sebagai tindak pidana siber yang terus berkembang seiring kemajuan teknologi informasi.⁸

⁵ Indonesia, “Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik” (2024), <https://peraturan.bpk.go.id/Details/269741/uu-no-1-tahun-2024>.

⁶ Muhammad Rafi Nugraha, “Cara Menentukan Pasal Untuk Menjerat Pelaku Penipuan *Online*,” *Klinik Hukumonline* (Hukumonline, 2024), <https://www.hukumonline.com/klinik/a/cara-menentukan-pasal-untuk-menjerat-pelaku-penipuan-online-i-lt5d1ad428d8fa3/>.

⁷ Marselino Clifer Tuju, Suci Ramadani, and Chairuni Nasution, “Penegakan Hukum Terhadap Tindak Pidana Cyber Dalam Kasus Penipuan Jual Beli *Online* Dalam Perspektif Kriminologi,” *Penegakan Hukum Terhadap Tindak Pidana Cyber Dalam Kasus Penipuan Jual Beli Online Dalam Perspektif Kriminologi* 5, no. 2 (2025): 1763–76, <https://doi.org/10.31004/innovative.v5i2.18499>.

⁸ Muhammad Aabid, Tyas Dzaky, and Ibrahim Fikma Edrisy, “Strategi Pencegahan Kejahatan Siber Di Indonesia: Sinergi Antara UU ITE Dan Kebijakan Keamanan Digital,” *PESHUM: Jurnal Pendidikan, Sosial Dan Humaniora* 4, no. 2 (2025): 12, <https://doi.org/10.56799/peshum.v4i2.8311>.

Selanjutnya, penelitian Kristiyenda (2025) membahas pencegahan kejahatan *deepfake* melalui studi kasus penipuan yang menggunakan manipulasi wajah Presiden Prabowo Subianto. Penelitian tersebut menitikberatkan pada analisis penyalahgunaan teknologi *artificial intelligence* dalam kejahatan siber, efektivitas regulasi yang berlaku, serta pentingnya penguatan deteksi dini dan literasi digital masyarakat. Hasil penelitian menunjukkan bahwa perkembangan teknologi *deepfake* menghadirkan tantangan baru bagi aparat penegak hukum karena regulasi yang ada belum sepenuhnya mampu mengakomodasi karakteristik kejahatan berbasis kecerdasan buatan. Akan tetapi, ruang lingkup penelitian tersebut terbatas pada modus *deepfake* sehingga belum membahas berbagai bentuk penipuan digital lain, seperti *phishing*, toko daring fiktif, investasi bodong, *social engineering*, maupun penyalahgunaan identitas digital yang saat ini mendominasi kejahatan siber di Indonesia.⁹

Berdasarkan ketiga penelitian tersebut, dapat diketahui bahwa kajian terdahulu masih berfokus pada aspek kriminologi, strategi pencegahan kejahatan siber, atau analisis terhadap modus tertentu, seperti *deepfake*. Belum terdapat penelitian yang menganalisis secara komprehensif penegakan hukum terhadap berbagai modus penipuan berbasis digital dengan mengintegrasikan ketentuan dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, serta Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana sebagai kerangka hukum yang saling berkaitan. Kesenjangan penelitian (*gap analysis*) tersebut menunjukkan perlunya kajian yang tidak hanya menelaah pengaturan hukum materiil, tetapi juga efektivitas hukum acara pidana, pembuktian digital, serta harmonisasi antara rezim hukum umum (*lex generalis*) dan rezim hukum khusus (*lex specialis*) dalam penegakan hukum terhadap penipuan digital. Kontribusi ilmiah (*scientific contribution*) penelitian ini terletak pada perumusan konstruksi penegakan hukum yang mengintegrasikan hukum pidana materiil dan hukum acara pidana terhadap berbagai modus penipuan berbasis digital sebagai bentuk kejahatan siber di Indonesia, sehingga menghasilkan parameter yang lebih komprehensif bagi aparat penegak hukum dalam menghadapi perkembangan kejahatan digital yang semakin kompleks. Berdasarkan uraian tersebut, penelitian ini bertujuan untuk menganalisis penegakan hukum terhadap berbagai modus penipuan berbasis digital sebagai bentuk kejahatan siber di Indonesia serta merumuskan arah penguatan sistem penegakan hukum yang adaptif terhadap perkembangan teknologi digital.

2. METODE

Penelitian ini menggunakan metode penelitian hukum yuridis normatif dengan menempatkan hukum sebagai suatu sistem norma yang terdiri atas asas hukum, kaidah hukum,

⁹ Yoan Shevila Kristiyenda, Jasmine Faradila, and Christina Basanova, "Pencegahan Kejahatan *Deepfake*: Studi Kasus Terhadap Modus Penipuan *Deepfake* Prabowo Subianto Dalam Tawaran Bantuan Uang," *ALADALAH: Jurnal Politik, Sosial, Hukum Dan Humaniora* 3, no. 2 (2025): 149–64, <https://doi.org/10.59246/aladalah.v3i2.1263>.

doktrin, serta peraturan perundang-undangan yang mengatur penegakan hukum terhadap tindak pidana penipuan berbasis digital.¹⁰ Metode ini dipilih karena penelitian berfokus pada analisis sinkronisasi dan harmonisasi norma hukum yang mengatur penegakan hukum kejahatan siber, khususnya ketentuan dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, serta Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana. Pendekatan penelitian yang digunakan meliputi *statute approach* untuk menganalisis pengaturan hukum positif, *conceptual approach* untuk mengkaji konsep penegakan hukum, kejahatan siber, dan pertanggungjawaban pidana, serta *case approach* melalui analisis terhadap putusan pengadilan dan praktik penegakan hukum yang berkaitan dengan penipuan berbasis digital. Spesifikasi penelitian bersifat deskriptif-analitis, yaitu menggambarkan pengaturan hukum yang berlaku sekaligus menganalisis penerapannya terhadap perkembangan modus penipuan digital di Indonesia.

Jenis data yang digunakan berupa data sekunder yang terdiri atas bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier.¹¹ Bahan hukum primer meliputi Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta putusan pengadilan yang relevan. Bahan hukum sekunder terdiri atas buku, artikel ilmiah, hasil penelitian, dan pendapat para ahli yang berkaitan dengan penegakan hukum siber dan hukum pidana. Adapun bahan hukum tersier berupa kamus hukum, ensiklopedia, dan sumber pendukung lainnya yang digunakan untuk memperjelas konsep hukum. Pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*) dengan menelusuri peraturan perundang-undangan, literatur ilmiah, serta publikasi akademik yang relevan. Seluruh bahan hukum dianalisis secara kualitatif melalui tahapan inventarisasi, klasifikasi, sistematisasi, interpretasi gramatikal, sistematis, dan teleologis, kemudian disusun secara preskriptif untuk menghasilkan argumentasi hukum mengenai efektivitas penegakan hukum terhadap modus penipuan berbasis digital sebagai bentuk kejahatan siber di Indonesia.

3. HASIL DAN PEMBAHASAN

3.1 Penipuan Digital sebagai Bentuk Kejahatan Siber

Kejahatan siber pada dasarnya merupakan perbuatan melawan hukum yang dilakukan dengan memanfaatkan teknologi informasi sebagai sarana maupun sasaran. Penipuan digital menempati posisi khas, karena ruang siber tidak sekadar menjadi alat, tetapi turut membentuk modus operandi

¹⁰ Nelvitia Purba et al., *Metode Penelitian Hukum*, ed. Joharsah Joharsah (Medan: Pustaka Media Publishing, 2024).

¹¹ Zainuddin Ali, *Metode Penelitian Hukum* (Jakarta: Sinar Grafika, 2022).

yang baru.¹² Jika penipuan konvensional menuntut kontak langsung antara pelaku dan korban, penipuan digital justru mengandalkan anonimitas, jangkauan lintas wilayah, dan kecepatan penyebaran informasi. Karakteristik inilah yang membedakannya dari penipuan biasa dan menuntut perangkat hukum yang lebih spesifik.

Dalam perspektif teori pertanggungjawaban pidana, seorang pelaku baru dapat dipidana apabila terpenuhi dua unsur utama, yaitu perbuatan melawan hukum (*actus reus*) dan kesalahan batin berupa kesengajaan (*mens rea*).¹³ Dalam konteks penipuan digital, unsur kesengajaan tampak dari perancangan modus yang sistematis untuk mengelabui korban, sedangkan unsur perbuatan melawan hukum tampak dari penyebaran informasi bohong yang menimbulkan kerugian.

Perkembangan teknologi digital telah mengubah karakteristik tindak pidana penipuan dari kejahatan konvensional yang mengandalkan interaksi langsung menjadi kejahatan siber yang memanfaatkan jaringan elektronik sebagai media utama. Transformasi tersebut menyebabkan objek perlindungan hukum tidak lagi terbatas pada harta kekayaan korban, tetapi juga meliputi keamanan sistem elektronik, kepercayaan masyarakat terhadap transaksi digital, serta kepastian hukum dalam pemanfaatan teknologi informasi. Karakteristik tersebut menjadikan penipuan digital memiliki tingkat kompleksitas yang lebih tinggi dibandingkan penipuan konvensional karena pelaku dapat menyembunyikan identitas, menggunakan akun anonim, memanfaatkan *virtual private network* (VPN), serta mengoperasikan jaringan lintas negara yang menyulitkan proses identifikasi maupun penegakan hukum.¹⁴ Kondisi ini menunjukkan bahwa ruang siber tidak lagi berfungsi sebagai sarana komunikasi semata, melainkan telah berkembang menjadi lingkungan baru (*cyberspace*) yang melahirkan bentuk-bentuk kejahatan dengan karakteristik berbeda dari kejahatan konvensional.

Dalam perspektif hukum pidana, perubahan modus tersebut berimplikasi terhadap perluasan objek pengaturan hukum. Apabila penipuan konvensional lebih menitikberatkan pada penggunaan tipu muslihat untuk memperoleh keuntungan secara melawan hukum, penipuan digital berkembang melalui manipulasi sistem elektronik, penyalahgunaan data pribadi, rekayasa identitas digital, serta eksploitasi kelemahan keamanan siber. Modus seperti *phishing*, *social engineering*, *business email compromise*, *fake online shop*, dan investasi digital fiktif menunjukkan bahwa perkembangan teknologi tidak hanya meningkatkan efisiensi aktivitas ekonomi, tetapi juga memperluas peluang terjadinya kejahatan yang sulit dideteksi menggunakan mekanisme penegakan hukum konvensional.¹⁵ Oleh karena itu, pembentuk undang-undang memperluas ruang lingkup perlindungan melalui Undang-Undang Informasi dan Transaksi Elektronik dengan

¹² Dwi Anggriani, Rahmattullah Lihawa, and Roy Marthen Moonti, "Konsep Penegakan Hukum Terhadap Tindak Pidana Siber Di Indonesia," *Jurnal Hukum Dan Keadilan* 8, no. 2 (2024), <https://doi.org/10.35905/jhk.v8i2.8086>.

¹³ Dian Putri Yasinta and Ernawati, "Analisis Pertanggungjawaban Pidana Terhadap Penipuan Online Melalui Aplikasi Telegram Dalam Perspektif Hukum Pidana Siber Indonesia," *Jurnal Education and Cyber Law (JERKIN)* 4, no. 3 (2026): 15696–705, <https://doi.org/10.31004/jerkin.v4i3.4295>.

¹⁴ Anggriani, Lihawa, and Moonti, "Konsep Penegakan Hukum Terhadap Tindak Pidana Siber Di Indonesia."

¹⁵ Andre Lavat, "Analisis Pertanggungjawaban Pidana Terhadap Penipuan Berbasis Aplikasi," *Jurnal Education and Cyber Law* 4, no. 1 (2025), <http://jerkin.org/index.php/jerkin/article/download/4295/3335/28371>.

mengakomodasi penggunaan informasi elektronik sebagai objek sekaligus alat terjadinya tindak pidana.

Kejahatan siber berkembang lebih cepat dibandingkan perkembangan regulasi sehingga efektivitas penegakan hukum tidak hanya ditentukan oleh keberadaan norma pidana, tetapi juga oleh kemampuan negara mengadaptasi instrumen hukum terhadap perubahan teknologi. Analisis tersebut menunjukkan bahwa penipuan digital merupakan bentuk kejahatan siber yang memiliki karakteristik khusus sehingga memerlukan pendekatan hukum yang berbeda dibandingkan penanganan tindak pidana penipuan konvensional.

Karakteristik khusus penipuan digital mengakibatkan pemenuhan unsur tindak pidana tidak lagi dapat dinilai hanya berdasarkan ketentuan penipuan dalam Kitab Undang-Undang Hukum Pidana. Unsur tipu muslihat, rangkaian kebohongan, dan maksud menguntungkan diri sendiri tetap menjadi inti delik penipuan, tetapi pelaksanaannya kini memanfaatkan informasi elektronik, sistem elektronik, dan media digital sebagai instrumen utama. Perubahan tersebut memperluas ruang lingkup pembuktian karena aparat penegak hukum tidak hanya harus membuktikan adanya kerugian dan niat pelaku, tetapi juga harus memastikan keaslian alat bukti elektronik, identitas digital pelaku, serta hubungan antara aktivitas elektronik dengan akibat hukum yang ditimbulkan.¹⁶ Dengan demikian, pembuktian dalam penipuan digital memiliki karakter yang lebih kompleks dibandingkan pembuktian tindak pidana konvensional.

Perkembangan tersebut menjadi dasar lahirnya pengaturan khusus melalui Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pasal 28 ayat (1) juncto Pasal 45A ayat (1) memberikan dasar pemidanaan terhadap penyebaran informasi bohong yang menimbulkan kerugian materiil dalam transaksi elektronik.¹⁷ Ketentuan tersebut menunjukkan bahwa pembentuk undang-undang tidak bermaksud menggantikan delik penipuan dalam Kitab Undang-Undang Hukum Pidana, melainkan memberikan pengaturan yang lebih spesifik terhadap perbuatan yang dilakukan melalui sistem elektronik. Oleh karena itu, keberadaan Undang-Undang Informasi dan Transaksi Elektronik harus dipahami sebagai instrumen hukum yang bersifat *lex specialis*, sedangkan ketentuan mengenai penipuan dalam Kitab Undang-Undang Hukum Pidana tetap berfungsi sebagai *lex generalis* yang berlaku terhadap perbuatan yang tidak memenuhi karakteristik transaksi elektronik.

Penerapan asas *lex specialis derogat legi generali* menjadi penting untuk menghindari ketidakpastian hukum dalam proses penegakan hukum. Pemilihan dasar hukum yang tidak tepat berpotensi menimbulkan disparitas putusan, tumpang tindih penerapan norma, bahkan pelanggaran terhadap asas kepastian hukum. Oleh karena itu, aparat penegak hukum perlu

¹⁶ V Vanessa, "Analysis of the Validity of Electronic Evidence in Criminal Trial Based on *Digital forensics* in Indonesia," *Indonesian Journal of Law and Economics Review*, 2025, <https://doi.org/10.21070/ijler.v26i0.1395>.

¹⁷ Agnes Debora Elisabeth Kaunang, "Menyebarkan Berita Bohong Menyebabkan Mengakibatkan Kerugian Konsumen Dalam Transaksi Elektronik Sebagai Tindak Pidana Menurut UU ITE (Putusan Mahkamah Agung Nomor 3905 K/Pid.Sus/2022)," *Lex Privatum* 13, no. 4 (2024), <https://ejournal.unsrat.ac.id/v3/index.php/lexprivatum/article/view/56557>.

mengidentifikasi terlebih dahulu karakteristik perbuatan, media yang digunakan, serta objek yang dirugikan sebelum menentukan ketentuan pidana yang akan diterapkan. Pendekatan tersebut sejalan dengan penelitian Kristian Hutasoit yang menyatakan bahwa penegakan hukum terhadap penipuan berbasis digital harus didasarkan pada karakteristik tindak pidana, bukan semata-mata pada akibat yang ditimbulkan, sehingga penerapan Undang-Undang Informasi dan Transaksi Elektronik dan Kitab Undang-Undang Hukum Pidana tetap berjalan secara harmonis dalam kerangka sistem hukum pidana nasional.

3.2 Dualisme Norma antara KUHP Nasional dan Undang-Undang ITE

Persoalan mendasar dalam penegakan hukum penipuan digital adalah keberadaan dua rezim yang mengatur perbuatan serupa. Di satu sisi, penipuan diatur secara umum dalam Pasal 492 KUHP Nasional sebagai *lex generalis*; di sisi lain, penipuan daring dapat dijerat dengan Pasal 28 ayat (1) juncto Pasal 45A ayat (1) Undang-Undang Informasi dan Transaksi Elektronik sebagai *lex specialis*. Asas *lex specialis derogat legi generali* menentukan bahwa ketentuan yang lebih khusus mengesampingkan ketentuan yang lebih umum, sehingga Undang-Undang Informasi dan Transaksi Elektronik semestinya menjadi rujukan utama terhadap penipuan yang memenuhi unsur transaksi elektronik.¹⁸

Asas *lex specialis derogat legi generali* tidak hanya berfungsi sebagai pedoman penyelesaian konflik norma, tetapi juga menjadi instrumen untuk menjaga konsistensi sistem hukum pidana. Penerapan asas tersebut menghendaki agar ketentuan yang mengatur secara khusus didahulukan sepanjang memuat unsur-unsur yang lebih spesifik dibandingkan ketentuan umum. Dalam konteks penipuan berbasis digital, keberadaan Undang-Undang Informasi dan Transaksi Elektronik merupakan respons terhadap perkembangan teknologi yang melahirkan bentuk-bentuk kejahatan baru yang tidak sepenuhnya dapat dijangkau oleh rumusan penipuan dalam Kitab Undang-Undang Hukum Pidana. Perbedaan tersebut tidak hanya terletak pada media yang digunakan, tetapi juga pada objek yang dilindungi, karakteristik perbuatan, serta mekanisme pembuktian yang melibatkan informasi elektronik dan sistem elektronik.

Penipuan yang dilakukan melalui transaksi elektronik pada dasarnya tidak hanya merugikan korban secara ekonomi, tetapi juga mengganggu kepercayaan masyarakat terhadap ekosistem digital. Oleh karena itu, pembentuk undang-undang memberikan pengaturan khusus melalui Pasal 28 ayat (1) Undang-Undang Nomor 1 Tahun 2024 yang secara eksplisit mengatur penyebaran informasi bohong yang mengakibatkan kerugian materiil dalam transaksi elektronik. Norma tersebut menunjukkan bahwa perlindungan hukum tidak lagi hanya diarahkan terhadap harta kekayaan korban sebagaimana delik penipuan konvensional, tetapi juga terhadap keamanan dan integritas transaksi elektronik sebagai bagian dari sistem ekonomi digital nasional. Perluasan objek perlindungan tersebut menjadi dasar yuridis mengapa Undang-Undang Informasi dan Transaksi Elektronik diposisikan sebagai *lex specialis* dalam penanganan penipuan digital.

¹⁸ Peppy Rahmawati, "Tindak Pidana Pencucian Uang Dan Penipuan Arisan Online Sebagai Kejahatan Asal," *Jurist-Diction* 4, no. 1 (2021): 273–94, <https://doi.org/10.20473/jd.v4i1.24302>.

Perkembangan kejahatan siber menuntut pembentukan norma pidana yang bersifat adaptif karena karakteristik tindak pidana digital tidak lagi identik dengan kejahatan konvensional. Efektivitas penegakan hukum ditentukan oleh kemampuan aparat dalam menerapkan instrumen hukum yang sesuai dengan karakteristik tindak pidana yang diperiksa. Oleh sebab itu, penerapan Pasal 492 KUHP Nasional seharusnya dilakukan terhadap penipuan yang bersifat umum, sedangkan penipuan yang memenuhi unsur transaksi elektronik lebih tepat dikenakan ketentuan Undang-Undang Informasi dan Transaksi Elektronik agar asas kepastian hukum tetap terjaga.

Meskipun demikian, dalam praktik peradilan kerap dijumpai dakwaan berlapis yang menggabungkan kedua ketentuan, misalnya dakwaan kesatu berdasarkan Pasal 28 ayat (1) juncto Pasal 45A Undang-Undang Informasi dan Transaksi Elektronik dan dakwaan kedua berdasarkan Pasal 378 KUHP.¹⁹ Praktik ini memperkuat peluang pemidanaan, tetapi menimbulkan ketidakpastian mengenai norma mana yang seharusnya diutamakan, sehingga berpotensi menimbulkan *overcriminalization* maupun disparitas putusan.

Praktik penyusunan dakwaan secara kumulatif menunjukkan bahwa masih terdapat perbedaan cara pandang dalam menentukan dasar hukum terhadap penipuan berbasis digital. Dari perspektif hukum acara pidana, penyusunan dakwaan alternatif maupun subsidair merupakan kewenangan penuntut umum untuk mengantisipasi kemungkinan tidak terbuktinya salah satu unsur tindak pidana. Akan tetapi, penggunaan beberapa ketentuan pidana terhadap satu perbuatan yang memiliki karakteristik sama berpotensi menimbulkan ketidakpastian hukum apabila tidak disertai parameter yang jelas mengenai ruang lingkup masing-masing norma. Kondisi tersebut dapat mengakibatkan perbedaan penerapan hukum terhadap perkara yang memiliki fakta serupa sehingga memunculkan disparitas putusan.²⁰

Permasalahan tersebut semakin kompleks setelah berlakunya Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana yang tetap mempertahankan delik penipuan sebagai tindak pidana umum. Kehadiran ketentuan baru tersebut tidak menghapus keberlakuan Undang-Undang Informasi dan Transaksi Elektronik, melainkan menempatkan kedua instrumen hukum dalam hubungan yang saling melengkapi. Oleh karena itu, aparat penegak hukum harus melakukan identifikasi terhadap objek tindak pidana, media yang digunakan, cara melakukan perbuatan, dan akibat hukum yang ditimbulkan sebelum menentukan dasar hukum yang akan diterapkan. Pendekatan tersebut akan menghasilkan penerapan hukum yang lebih proporsional sekaligus menghindari penggunaan ketentuan pidana secara berlebihan (*overcriminalization*).

Efektivitas penegakan hukum terhadap penipuan berbasis *online* bergantung pada ketepatan mengidentifikasi unsur tindak pidana, bukan hanya pada pembuktian adanya kerugian korban. Pendekatan demikian menunjukkan bahwa penerapan Undang-Undang Informasi dan Transaksi Elektronik maupun Kitab Undang-Undang Hukum Pidana tidak boleh diposisikan sebagai norma

¹⁹ Nugraha, "Cara Menentukan Pasal Untuk Menjerat Pelaku Penipuan *Online*."

²⁰ Kristian Hutasoit, "Tinjauan Yuridis Terhadap Tindak Pidana Penipuan Secara *Online* Dalam Perspektif Hukum Pidana Di Indonesia" (Medan: Fakultas Hukum Universitas Sumatera Utara, 2018), <https://repository.usu.ac.id/handle/123456789/4578>.

yang saling bersaing, melainkan sebagai satu kesatuan dalam sistem hukum pidana yang harus diterapkan berdasarkan karakteristik konkret dari setiap perkara.

Harmonisasi antara Kitab Undang-Undang Hukum Pidana Nasional dan Undang-Undang Informasi dan Transaksi Elektronik menjadi prasyarat utama dalam mewujudkan penegakan hukum yang memberikan kepastian, keadilan, dan kemanfaatan. Harmonisasi tersebut tidak cukup dilakukan melalui pengaturan normatif, tetapi memerlukan keseragaman interpretasi di tingkat penyidikan, penuntutan, dan pemeriksaan di pengadilan. Perbedaan penafsiran terhadap ruang lingkup Pasal 492 KUHP Nasional dan Pasal 28 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik berpotensi menghasilkan putusan yang tidak konsisten terhadap perkara yang memiliki karakteristik serupa. Kondisi tersebut dapat mengurangi kepastian hukum sekaligus menurunkan kepercayaan masyarakat terhadap sistem peradilan pidana.

Dari perspektif teori kepastian hukum, penerapan norma pidana harus memenuhi prinsip kejelasan rumusan (*lex certa*) dan konsistensi penerapan agar setiap orang dapat memperkirakan konsekuensi hukum atas perbuatannya. Penegakan hukum terhadap penipuan digital tidak hanya ditentukan oleh beratnya ancaman pidana, tetapi juga oleh kemampuan aparat penegak hukum dalam memilih norma yang tepat sesuai karakteristik perkara. Oleh karena itu, diperlukan pedoman penerapan yang memberikan batas yang tegas mengenai penggunaan Pasal 492 KUHP Nasional dan Pasal 28 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik. Parameter tersebut akan mengurangi potensi disparitas putusan sekaligus memperkuat efektivitas sistem peradilan pidana dalam menghadapi perkembangan modus penipuan berbasis digital. Pembahasan mengenai harmonisasi norma tersebut menjadi dasar untuk memahami pentingnya pembaruan hukum acara pidana dan penguatan mekanisme pembuktian elektronik yang akan dibahas pada subbab berikutnya.

3.3 Pembaruan Hukum Acara Pidana dan Tantangan Penegakannya

Penegakan hukum penipuan digital memasuki babak baru dengan berlakunya Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana, yang ditetapkan pada 17 Desember 2025 dan menggantikan Undang-Undang Nomor 8 Tahun 1981.²¹ Di antara materi muatan barunya adalah penguatan hak tersangka dan korban, penyempurnaan kewenangan penyidik dan penuntut umum, serta pengenalan mekanisme pengakuan bersalah (*plea bargain*) dan perjanjian penundaan penuntutan (*deferred prosecution agreement*). Mekanisme baru ini berpotensi mempercepat penyelesaian perkara penipuan digital yang kerap menumpuk.

Pembaruan hukum acara pidana melalui Undang-Undang Nomor 20 Tahun 2025 pada dasarnya tidak hanya mengubah aspek prosedural, tetapi juga menggeser paradigma penegakan hukum pidana menuju sistem yang lebih adaptif terhadap perkembangan teknologi informasi. Penanganan tindak pidana penipuan berbasis digital tidak lagi cukup mengandalkan mekanisme pembuktian konvensional karena sebagian besar jejak kejahatan tersimpan dalam bentuk informasi elektronik, data digital, maupun aktivitas pada sistem elektronik. Kondisi tersebut menempatkan

²¹ Indonesia, “Undang-Undang Nomor 20 Tahun 2025 Tentang Kitab Undang-Undang Hukum Acara Pidana” (2025), <https://peraturan.bpk.go.id/Details/337302/uu-no-20-tahun-2025>.

hukum acara pidana sebagai instrumen yang menentukan efektivitas penerapan hukum pidana materiil. Dengan kata lain, keberhasilan penegakan hukum terhadap penipuan digital tidak hanya bergantung pada rumusan delik dalam Kitab Undang-Undang Hukum Pidana maupun Undang-Undang Informasi dan Transaksi Elektronik, tetapi juga pada kemampuan hukum acara pidana mengakomodasi karakteristik pembuktian digital.

Perubahan tersebut memiliki arti penting karena pembuktian dalam perkara siber berbeda secara fundamental dengan pembuktian tindak pidana konvensional. Alat bukti elektronik bersifat mudah berubah, mudah dipindahkan, bahkan dapat dimanipulasi dalam waktu yang sangat singkat apabila tidak segera diamankan melalui prosedur yang tepat. Oleh sebab itu, penguatan mekanisme penyitaan data elektronik, pemeriksaan *digital evidence*, serta penggunaan hasil *digital forensic* menjadi kebutuhan yang tidak dapat dipisahkan dari proses pembuktian. Keberadaan pembaruan hukum acara pidana harus dipahami sebagai upaya membangun sistem pembuktian yang mampu menjamin keaslian (*authenticity*), integritas (*integrity*), dan keandalan (*reliability*) alat bukti elektronik sehingga memiliki nilai pembuktian yang memadai di persidangan.

Pandangan tersebut sejalan dengan penelitian mengenai pembuktian elektronik dalam kejahatan siber yang menyatakan bahwa efektivitas penegakan hukum tidak lagi ditentukan oleh banyaknya norma pidana, melainkan oleh kemampuan aparat penegak hukum mengelola dan memverifikasi alat bukti elektronik sesuai prinsip *due process of law*. Oleh karena itu, pembaruan Kitab Undang-Undang Hukum Acara Pidana harus dimaknai sebagai instrumen untuk memperkuat kualitas pembuktian, bukan sekadar mempercepat proses penyelesaian perkara.

Kendati kerangka substantif dan prosedural telah diperbarui, penegakan hukum di lapangan masih menghadapi sejumlah tantangan, antara lain: a. kesulitan pembuktian karena alat bukti elektronik mudah dimanipulasi dan menuntut keahlian forensik digital; b. anonimitas pelaku yang menyulitkan identifikasi; dan c. dimensi lintas yurisdiksi ketika pelaku dan korban berada di wilayah hukum yang berbeda. Ketiga tantangan ini saling berkelindan dan menjadikan penegakan hukum penipuan digital jauh lebih kompleks daripada penipuan konvensional, sehingga ketersediaan norma yang memadai perlu diimbangi dengan penguatan kapasitas kelembagaan serta kerja sama lintas lembaga dan lintas negara.

Kesulitan pembuktian dalam perkara penipuan digital tidak hanya disebabkan oleh penggunaan teknologi yang semakin kompleks, tetapi juga oleh karakteristik alat bukti elektronik yang berbeda dengan alat bukti konvensional. Informasi elektronik dapat mengalami perubahan tanpa meninggalkan jejak fisik sehingga proses penyitaan, penyimpanan, pemeriksaan, dan penyajian alat bukti harus memenuhi prinsip *chain of custody*. Prinsip tersebut bertujuan menjaga kesinambungan penguasaan barang bukti sejak pertama kali diperoleh hingga diajukan di persidangan agar tidak menimbulkan keraguan mengenai keaslian maupun integritas data. Apabila

prosedur tersebut diabaikan, nilai pembuktian alat bukti elektronik dapat dipersoalkan sehingga berpotensi menghambat pembuktian unsur tindak pidana.²²

Tantangan lain muncul dari penggunaan teknologi yang memungkinkan pelaku menyembunyikan identitas melalui *virtual private network* (VPN), akun anonim, identitas digital palsu, maupun server yang berada di luar wilayah hukum Indonesia. Kondisi tersebut menyebabkan identifikasi pelaku memerlukan kerja sama antara penyidik, penyelenggara sistem elektronik, penyedia layanan internet, lembaga forensik digital, serta otoritas di negara lain apabila kejahatan memiliki dimensi lintas batas.²³ Dengan demikian, efektivitas penegakan hukum tidak hanya bergantung pada kemampuan penyidik dalam menemukan alat bukti, tetapi juga pada efektivitas koordinasi antarlembaga serta mekanisme *mutual legal assistance* dalam memperoleh data elektronik dari yurisdiksi asing.

Pembuktian dalam tindak pidana penipuan berbasis elektronik memerlukan integrasi antara ketentuan Undang-Undang Informasi dan Transaksi Elektronik, hukum acara pidana, dan kemampuan teknis aparat dalam melakukan analisis forensik digital. Hal tersebut menunjukkan bahwa penguatan sumber daya manusia dan infrastruktur forensik digital memiliki kedudukan yang sama pentingnya dengan pembaruan regulasi dalam meningkatkan efektivitas penegakan hukum terhadap kejahatan siber.

Tabel 1. Dasar Hukum Penjeratan Modus Penipuan Berbasis Digital

Instrumen Hukum	Ketentuan	Ancaman Pidana
UU ITE (UU No. 1 Tahun 2024)	Pasal 28 ayat (1) jo. Pasal 45A ayat (1)	Penjara maks. 6 tahun / denda Rp1 miliar
KUHP lama	Pasal 378	Penjara maks. 4 tahun
KUHP Nasional (UU No. 1 Tahun 2023)	Pasal 492	Penjara maks. 4 tahun

Sumber: UU No. 1 Tahun 2024, UU No. 1 Tahun 2023, dan KUHP, diolah (2026).

Tabel di atas memperlihatkan bahwa terhadap satu perbuatan penipuan digital terdapat lebih dari satu dasar hukum yang dapat diterapkan, dengan ancaman pidana yang bervariasi. Undang-Undang Informasi dan Transaksi Elektronik menawarkan ancaman paling berat, yakni enam tahun penjara, dibandingkan empat tahun dalam KUHP maupun KUHP Nasional. Variasi ini menegaskan kedudukan Undang-Undang Informasi dan Transaksi Elektronik sebagai instrumen khusus yang lebih menjerakan, sekaligus menuntut kecermatan penegak hukum dalam memilih ketentuan yang paling tepat agar keadilan dan kepastian hukum tercapai secara seimbang.

²² Dwi Arya Pratama Handoyo, "Kedudukan Alat Bukti Surat Elektronik Dalam Hukum Acara Perdata Indonesia: Analisis Yuridis Terhadap Kepastian Hukum Dan Kekuatan Pembuktian," *Al Zayn: Jurnal Ilmu Sosial & Hukum* 4, no. 2 (2026), <https://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/AlZayn/article/view/4903>.

²³ Fran Casino et al., "SoK: Cross-Border Criminal Investigations and *Digital evidence*," *ArXiv*, 2022, <https://arxiv.org/abs/2205.12911>.

Perbedaan ancaman pidana sebagaimana ditunjukkan dalam tabel tidak dapat dijadikan satu-satunya dasar dalam menentukan ketentuan pidana yang akan diterapkan. Penegakan hukum pidana pada hakikatnya tidak bertujuan mencari ancaman pidana yang paling berat, tetapi memilih norma yang paling tepat berdasarkan karakteristik perbuatan yang dilakukan pelaku. Pendekatan tersebut sejalan dengan asas legalitas yang menghendaki agar setiap pemidanaan didasarkan pada rumusan delik yang secara tepat menggambarkan unsur-unsur perbuatan yang terbukti di persidangan. Oleh karena itu, penerapan Undang-Undang Informasi dan Transaksi Elektronik tidak boleh didasarkan semata-mata pada pertimbangan ancaman pidana yang lebih tinggi, melainkan harus mempertimbangkan apakah seluruh unsur tindak pidana dalam ketentuan tersebut benar-benar terpenuhi.

Di sisi lain, pembaruan hukum acara pidana harus diikuti dengan peningkatan kapasitas kelembagaan aparat penegak hukum. Penyidik, penuntut umum, dan hakim memerlukan pemahaman yang memadai mengenai pembuktian elektronik, *digital forensic*, serta perkembangan modus kejahatan siber agar mampu menerapkan hukum secara konsisten. Penguatan tersebut perlu didukung oleh penyusunan pedoman teknis mengenai penanganan barang bukti elektronik, peningkatan laboratorium forensik digital, serta optimalisasi kerja sama antara kepolisian, kejaksaan, pengadilan, Kementerian Komunikasi dan Digital, serta penyelenggara sistem elektronik. Melalui langkah tersebut, pembaruan hukum acara pidana tidak berhenti pada perubahan regulasi, tetapi menghasilkan sistem penegakan hukum yang lebih adaptif terhadap perkembangan teknologi informasi dan mampu memberikan kepastian hukum, keadilan, serta kemanfaatan dalam penanganan penipuan berbasis digital.

4. PENUTUP

Hasil penelitian menunjukkan bahwa penegakan hukum terhadap modus penipuan berbasis digital sebagai bentuk kejahatan siber di Indonesia harus dilaksanakan melalui penerapan norma yang terintegrasi antara Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik sebagai *lex specialis*, Kitab Undang-Undang Hukum Pidana Nasional sebagai *lex generalis*, dan Kitab Undang-Undang Hukum Acara Pidana sebagai landasan prosedural dalam pembuktian tindak pidana berbasis teknologi. Penerapan ketiga instrumen tersebut tidak dapat dilakukan secara terpisah karena efektivitas penegakan hukum ditentukan oleh ketepatan pemilihan dasar hukum sesuai karakteristik perbuatan, keabsahan alat bukti elektronik, serta kemampuan aparat penegak hukum menghadapi perkembangan modus kejahatan digital yang semakin kompleks. Kontribusi ilmiah penelitian ini terletak pada perumusan konstruksi penegakan hukum yang mengintegrasikan hukum pidana materiil dan hukum acara pidana sebagai satu kesatuan sistem dalam penanganan penipuan digital, sehingga memberikan parameter yang lebih jelas mengenai penerapan asas *lex specialis derogat legi generali* dan mekanisme pembuktian elektronik. Temuan tersebut menunjukkan bahwa pembaruan regulasi belum sepenuhnya menjamin efektivitas penegakan hukum tanpa didukung harmonisasi penerapan norma, peningkatan kapasitas forensik

digital, serta koordinasi antarlembaga dan kerja sama lintas yurisdiksi. Oleh karena itu, diperlukan pedoman penerapan yang seragam bagi aparat penegak hukum, penguatan infrastruktur pembuktian digital, dan optimalisasi kerja sama internasional agar penegakan hukum terhadap penipuan berbasis digital mampu mewujudkan kepastian hukum, keadilan, dan kemanfaatan dalam ekosistem digital Indonesia.

DAFTAR PUSTAKA

- Aabid, Muhammad, Tyas Dzaky, and Ibrahim Fikma Edrisy. "Strategi Pencegahan Kejahatan Siber Di Indonesia: Sinergi Antara UU ITE Dan Kebijakan Keamanan Digital." *PESHUM: Jurnal Pendidikan, Sosial Dan Humaniora* 4, no. 2 (2025): 12. <https://doi.org/10.56799/peshum.v4i2.8311>.
- Ali, Zainuddin. *Metode Penelitian Hukum*. Jakarta: Sinar Grafika, 2022.
- Anda, Alfany Restu, Sri Astutik, and Ernu Widodo. "Analisis Pertimbangan Hakim Dalam Penerapan Pasal 378 KUHP Pada Perkara Penipuan Kredit." *RIGGS: Journal of Research and Innovation in Global Governance Studies* 5, no. 1 (2025). <https://doi.org/10.31004/riggs.v5i1.6281>.
- Anggriani, Dwi, Rahmattullah Lihawa, and Roy Marthen Moonti. "Konsep Penegakan Hukum Terhadap Tindak Pidana Siber Di Indonesia." *Jurnal Hukum Dan Keadilan* 8, no. 2 (2024). <https://doi.org/10.35905/jhk.v8i2.8086>.
- Casino, Fran, Claudia Pina, Pablo López-Aguilar, Edgar Batista, Agustí Solanas, and Constantinos Patsakis. "SoK: Cross-Border Criminal Investigations and *Digital evidence*." *ArXiv*, 2022. <https://arxiv.org/abs/2205.12911>.
- Handoyo, Dwi Arya Pratama. "Kedudukan Alat Bukti Surat Elektronik Dalam Hukum Acara Perdata Indonesia: Analisis Yuridis Terhadap Kepastian Hukum Dan Kekuatan Pembuktian." *Al Zayn: Jurnal Ilmu Sosial & Hukum* 4, no. 2 (2026). <https://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/AlZayn/article/view/4903>.
- Hukmana, Siti Yona. "Kasus Penipuan *Deepfake* AI: Polri Buru Pelaku Pemalsuan Wajah Presiden Prabowo." *Media Indonesia*. 2025. <https://mediaindonesia.com/politik-dan-hukum/737308/kasus-penipuan-deepfake-ai-polri-buru-pelaku-pemalsuan-wajah-presiden-prabowo>.
- Hutasoit, Kristian. "Tinjauan Yuridis Terhadap Tindak Pidana Penipuan Secara *Online* Dalam Perspektif Hukum Pidana Di Indonesia." Medan: Fakultas Hukum Universitas Sumatera Utara, 2018. <https://repositori.usu.ac.id/handle/123456789/4578>.
- Indonesia. Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (2023). <https://peraturan.bpk.go.id/Details/234935/uu-no-1-tahun-2023>.
- . Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (2024). <https://peraturan.bpk.go.id/Details/269741/uu-no-1-tahun-2024>.
- . Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana (2025). <https://peraturan.bpk.go.id/Details/337302/uu-no-20-tahun-2025>.
- Irawan, Fauzan Mahdi, Muhammad Zibran Al Habsy, and Asmak Ul Hosnah. "Pertanggungjawaban Pidana Pelaku *Phishing* Dan Efektivitas Penegakan Hukum

- Berdasarkan UU Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik.” *Jurnal Komputer, Informasi Dan Teknologi* 5, no. 2 (2025). <https://doi.org/10.53697/jkomitek.v5i2.3159>.
- Kaunang, Agnes Debora Elisabeth. “Menyebarkan Berita Bohong Menyebabkan Mengakibatkan Kerugian Konsumen Dalam Transaksi Elektronik Sebagai Tindak Pidana Menurut UU ITE (Putusan Mahkamah Agung Nomor 3905 K/Pid.Sus/2022).” *Lex Privatum* 13, no. 4 (2024). <https://ejournal.unsrat.ac.id/v3/index.php/lexprivatum/article/view/56557>.
- Kristiyenda, Yoan Shevila, Jasmine Faradila, and Christina Basanova. “Pencegahan Kejahatan *Deepfake*: Studi Kasus Terhadap Modus Penipuan *Deepfake* Prabowo Subianto Dalam Tawaran Bantuan Uang.” *ALADALAH: Jurnal Politik, Sosial, Hukum Dan Humaniora* 3, no. 2 (2025): 149–64. <https://doi.org/10.59246/aladalah.v3i2.1263>.
- Lavat, Andre. “Analisis Pertanggungjawaban Pidana Terhadap Penipuan Berbasis Aplikasi.” *Jurnal Education and Cyber Law* 4, no. 1 (2025). <http://jerk.in.org/index.php/jerk.in/article/download/4295/3335/28371>.
- Nugraha, Muhammad Rafi. “Cara Menentukan Pasal Untuk Menjerat Pelaku Penipuan *Online*.” *Klinik Hukumonline*. *Hukumonline*, 2024. <https://www.hukumonline.com/klinik/a/cara-menentukan-pasal-untuk-menjerat-pelaku-penipuan-online-i-lt5d1ad428d8fa3/>.
- Purba, Nelvitia, Ismed Batubara, Zaenal Arifin, and Bahmid Bahmid. *Metode Penelitian Hukum*. Edited by Joharsah Joharsah. Medan: Pustaka Media Publishing, 2024.
- Rahmawati, Peppy. “Tindak Pidana Pencucian Uang Dan Penipuan Arisan *Online* Sebagai Kejahatan Asal.” *Jurist-Diction* 4, no. 1 (2021): 273–94. <https://doi.org/10.20473/jd.v4i1.24302>.
- Tuju, Marselino Clifer, Suci Ramadani, and Chairuni Nasution. “Penegakan Hukum Terhadap Tindak Pidana Cyber Dalam Kasus Penipuan Jual Beli *Online* Dalam Perspektif Kriminologi.” *Penegakan Hukum Terhadap Tindak Pidana Cyber Dalam Kasus Penipuan Jual Beli Online Dalam Perspektif Kriminologi* 5, no. 2 (2025): 1763–76. <https://doi.org/10.31004/innovative.v5i2.18499>.
- Vanessa, V. “Analysis of the Validity of Electronic Evidence in Criminal Trial Based on *Digital forensics* in Indonesia.” *Indonesian Journal of Law and Economics Review*, 2025. <https://doi.org/10.21070/ijler.v26i0.1395>.
- Yasinta, Dian Putri, and Ernawati. “Analisis Pertanggungjawaban Pidana Terhadap Penipuan *Online* Melalui Aplikasi Telegram Dalam Perspektif Hukum Pidana Siber Indonesia.” *Jurnal Education and Cyber Law (JERKIN)* 4, no. 3 (2026): 15696–705. <https://doi.org/10.31004/jerk.in.v4i3.4295>.