Dewantara: Jurnal Pendidikan Sosial Humaniora
Volume 5, Nomor 2, Juni 2026
e-ISSN: 2962-1127; p-ISSN: 2962-1135, Hal. 178-191
DOI: https://doi.org/10.30640/dewantara.v5i2.6623
Tersedia: https://jurnaluniv45sby.ac.id/index.php/Dewantara

Problematika Pembuktian Digital dalam Penegakan Hukum Tindak Pidana Siber di Indonesia

Eka Fitri Lestari[1*], Rahmayanti[2], Donly Calner Aruan[3]
[1-3]Program Magister Ilmu Hukum, Universitas Pembangunan Panca Budi, Indonesia
Email: ekafitrilestari03@gmail.com[1], rahmayanti@dosen.pancabudi.ac.id[2], aruandonly@gmail.com[3]
**Penulis Korespondensi:* ekafitrilestari03@gmail.com

Abstract. *The development of information and communication technology has accelerated digital transformation, but it has also led to increasingly complex cybercrimes. The characteristics of cybercrime—anonymity, cross-jurisdictional nature, and reliance on electronic systems—make evidentiary processes a major challenge in criminal law enforcement in Indonesia. In this context, electronic evidence and digital forensics play a crucial role in uncovering crimes and linking perpetrators to criminal acts. Although electronic information and documents have been legally recognized as evidence under the Law on Electronic Information and Transactions, their implementation still faces various challenges. This study aims to analyze the legal framework of digital evidence, identify existing obstacles, and formulate strategies to optimize digital proof systems in criminal law enforcement. The research employs a normative legal method with statutory, conceptual, and case approaches. The findings reveal key challenges, including the volatility of electronic evidence, limited human resources and digital forensic infrastructure, lack of standardized procedures, difficulties in obtaining data from electronic service providers, and jurisdictional barriers due to the transnational nature of cybercrime. Additionally, differing interpretations among law enforcement officers regarding the validity and integrity of electronic evidence remain an issue. To address these challenges, efforts are needed to strengthen regulations, enhance institutional capacity, standardize digital forensic practices, improve inter-agency coordination, and expand international cooperation.*

Keywords: *Cybercrime; Digital Evidence; Digital Forensics; Electronic Evidence; Law Enforcement.*

Abstrak. Perkembangan teknologi informasi dan komunikasi telah mendorong transformasi digital, namun juga memunculkan tindak pidana siber yang semakin kompleks. Karakteristik cybercrime yang anonim, lintas yurisdiksi, dan berbasis sistem elektronik menjadikan pembuktian sebagai tantangan utama dalam penegakan hukum pidana di Indonesia. Dalam hal ini, alat bukti elektronik dan digital forensik memiliki peran penting dalam mengungkap tindak pidana serta menghubungkan pelaku dengan peristiwa hukum. Pengakuan terhadap informasi dan dokumen elektronik sebagai alat bukti sah telah diatur dalam Undang-Undang Informasi dan Transaksi Elektronik, namun implementasinya masih menghadapi kendala. Penelitian ini bertujuan menganalisis pengaturan hukum pembuktian digital, mengidentifikasi hambatan, serta merumuskan upaya optimalisasi dalam penegakan hukum pidana. Metode yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan, konseptual, dan kasus. Hasil penelitian menunjukkan bahwa kendala utama meliputi volatilitas barang bukti elektronik, keterbatasan sumber daya manusia dan infrastruktur digital forensik, belum seragamnya standar penanganan, kesulitan akses data dari penyedia layanan elektronik, serta hambatan yurisdiksi akibat sifat transnasional cybercrime. Selain itu, terdapat perbedaan pemahaman aparat penegak hukum terkait keabsahan dan integritas alat bukti elektronik. Upaya yang diperlukan meliputi penguatan regulasi, peningkatan kapasitas aparat, standardisasi forensik digital, optimalisasi koordinasi antar lembaga, serta perluasan kerja sama internasional.

Kata Kunci: Alat Bukti Elektronik; Digital Forensik; Pembuktian Digital; Penegakan Hukum; Tindak Pidana Siber.

1. LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan fundamental dalam berbagai aspek kehidupan masyarakat modern. Pemanfaatan internet, perangkat digital, komputasi awan, kecerdasan buatan, dan sistem elektronik telah mentransformasi cara manusia berinteraksi, bertransaksi, dan menyelenggarakan aktivitas pemerintahan. Digitalisasi tersebut memberikan manfaat yang signifikan dalam meningkatkan efisiensi, efektivitas, dan keterhubungan antarindividu maupun antarinstansi. Namun

Naskah Masuk: 17 Maret 2026; Revisi:16 April 2026; Diterima: 13 Juni 2026; Terbit: 15 Juni 2026

demikian, kemajuan teknologi tidak hanya menghadirkan dampak positif, tetapi juga menciptakan peluang bagi lahirnya berbagai bentuk kejahatan baru yang memanfaatkan teknologi sebagai sarana utama. Salah satu bentuk kejahatan yang berkembang paling pesat adalah tindak pidana siber (cybercrime), yaitu perbuatan melawan hukum yang dilakukan dengan menggunakan sistem elektronik, jaringan komputer, atau internet sebagai alat, sasaran, maupun media kejahatan (Widodo, 2012).

Tindak pidana siber memiliki karakteristik yang berbeda secara mendasar dengan kejahatan konvensional. Kejahatan ini dapat dilakukan secara anonim, tidak mengenal batas yurisdiksi negara, serta memanfaatkan kecanggihan teknologi untuk menyembunyikan identitas pelaku dan menghilangkan jejak kejahatan. Modus operandi cybercrime sangat beragam, mulai dari akses ilegal terhadap sistem elektronik, pencurian data pribadi, penipuan daring, carding, phishing, penyebaran malware, serangan ransomware, hingga manipulasi data elektronik. Kompleksitas kejahatan ini menimbulkan tantangan serius bagi aparat penegak hukum, khususnya dalam menemukan, mengamankan, dan membuktikan keterkaitan antara pelaku dengan peristiwa pidana yang terjadi (Sigid Suseno, 2020).

Indonesia merupakan salah satu negara dengan tingkat pertumbuhan pengguna internet yang sangat tinggi, sehingga rentan terhadap berbagai bentuk kejahatan siber. Digitalisasi sektor pemerintahan, perbankan, pendidikan, perdagangan elektronik, dan pelayanan publik telah meningkatkan ketergantungan masyarakat terhadap sistem elektronik. Dalam beberapa tahun terakhir, berbagai kasus kebocoran data pribadi, peretasan situs lembaga negara, dan penipuan berbasis digital menunjukkan bahwa ancaman cybercrime tidak lagi bersifat teoritis, melainkan telah menjadi persoalan nyata yang berdampak luas terhadap masyarakat dan negara. Kondisi ini menuntut adanya sistem penegakan hukum yang responsif dan adaptif terhadap perkembangan teknologi informasi (Badan Siber dan Sandi Negara, 2022).

Dalam sistem peradilan pidana, pembuktian merupakan inti dari proses penegakan hukum. Keberhasilan penuntutan dan penjatuhan pidana sangat ditentukan oleh kemampuan aparat penegak hukum untuk menghadirkan alat bukti yang sah dan meyakinkan hakim mengenai adanya tindak pidana serta kesalahan terdakwa. M. Yahya Harahap menegaskan bahwa pembuktian merupakan ketentuan yang mengatur alat bukti yang dibenarkan undang-undang dan tata cara penggunaannya untuk membentuk keyakinan hakim. Dengan demikian, tanpa sistem pembuktian yang kuat, proses peradilan pidana tidak akan mampu menghasilkan putusan yang mencerminkan keadilan, kepastian hukum, dan kemanfaatan (M. Yahya Harahap, 2016a).

Pembuktian dalam perkara cybercrime memiliki tingkat kompleksitas yang lebih tinggi dibandingkan dengan tindak pidana konvensional. Hal ini disebabkan karena bukti utama yang digunakan umumnya berupa data elektronik, dokumen digital, log aktivitas, metadata, rekaman sistem, atau informasi yang tersimpan pada server. Bukti digital tersebut bersifat sangat mudah diubah, disalin, dipindahkan, bahkan dihapus dalam hitungan detik. Oleh karena itu, penanganan alat bukti elektronik memerlukan prosedur khusus untuk menjamin keaslian (authenticity), integritas (integrity), dan keterandalan (reliability) sehingga dapat diterima sebagai alat bukti yang sah di persidangan (Eoghan Casey, 2011a).

Pengakuan hukum terhadap informasi elektronik dan/atau dokumen elektronik sebagai alat bukti yang sah telah diberikan melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024. Selain itu, pembaruan mendasar juga terjadi melalui Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana yang menggantikan KUHAP lama. Regulasi ini memperkuat sistem pembuktian modern dengan memberikan landasan yang lebih komprehensif terhadap penggunaan alat bukti elektronik, pemeriksaan digital, serta mekanisme perlindungan hak-hak pihak yang terlibat dalam proses peradilan pidana (Undang-Undang Nomor 1 Tahun 2024).

Meskipun kerangka normatif telah berkembang, praktik penegakan hukum masih menghadapi berbagai hambatan. Aparat penegak hukum seringkali dihadapkan pada keterbatasan sumber daya manusia yang memiliki keahlian digital forensik, minimnya laboratorium forensik digital di daerah, kurangnya perangkat lunak khusus, serta belum seragamnya standar operasional penanganan barang bukti elektronik. Keterbatasan tersebut dapat memengaruhi kualitas penyidikan dan menimbulkan keraguan terhadap validitas alat bukti yang diajukan di persidangan (Andi Hamzah, 2019).

Digital forensik memiliki peranan yang sangat penting dalam pembuktian tindak pidana siber. Melalui metode ilmiah, digital forensik memungkinkan penyidik dan ahli untuk mengidentifikasi, mengamankan, mengekstraksi, dan menganalisis data elektronik guna menemukan hubungan antara pelaku, perangkat, dan peristiwa pidana. Berbagai kajian akademik menunjukkan bahwa validitas alat bukti digital sangat ditentukan oleh prosedur pemeriksaan yang sistematis dan dapat dipertanggungjawabkan secara ilmiah (Rahmayanti, n.d.). Selain itu, penguatan kapasitas laboratorium forensik dan kompetensi penyidik merupakan faktor penting untuk memastikan bahwa alat bukti elektronik memiliki nilai pembuktian yang kuat di persidangan (Suci Ramadani, n.d.).

Selain aspek teknis, pembuktian digital juga menghadapi tantangan yurisdiksi. Banyak data elektronik yang relevan tersimpan di server luar negeri dan dikuasai oleh perusahaan teknologi global. Untuk memperoleh data tersebut, aparat penegak hukum harus menempuh mekanisme kerja sama internasional seperti mutual legal assistance. Proses tersebut sering memerlukan waktu yang panjang, sedangkan data elektronik memiliki sifat yang dinamis dan rentan hilang. Oleh karena itu, efektivitas pembuktian digital juga sangat bergantung pada kemampuan negara membangun kerja sama lintas negara yang efisien dan responsif (United Nations Office on Drugs and Crime, 2013).

Permasalahan lain yang tidak kalah penting adalah belum seragamnya pemahaman aparat penegak hukum mengenai standar penerimaan alat bukti elektronik. Dalam praktik peradilan, masih sering muncul perbedaan pandangan mengenai kekuatan pembuktian tangkapan layar, rekaman digital, metadata, maupun komunikasi elektronik. Eddy O.S. Hiariej menegaskan bahwa setiap alat bukti harus memenuhi syarat legalitas, relevansi, dan keandalan agar dapat dipergunakan untuk membentuk keyakinan hakim (Eddy O.S. Hiariej, 2021).

Dari perspektif kebijakan hukum pidana, pembuktian digital merupakan bagian integral dari upaya penanggulangan cybercrime. Barda Nawawi Arief menegaskan bahwa hukum pidana harus senantiasa menyesuaikan diri dengan perkembangan masyarakat dan teknologi agar tetap efektif dalam melindungi kepentingan hukum. Oleh karena itu, implementasi Undang-Undang Nomor 20 Tahun 2025 tentang KUHAP harus diikuti dengan peningkatan kompetensi aparat, standardisasi laboratorium digital forensik, dan penguatan koordinasi antarlembaga penegak hukum (Barda Nawawi Arief, 2016).

Berdasarkan uraian tersebut, penelitian berjudul "Problematika Pembuktian Digital dalam Penegakan Hukum Tindak Pidana Siber di Indonesia" menjadi penting untuk dilakukan. Penelitian ini bertujuan untuk menganalisis landasan normatif pembuktian digital, mengidentifikasi berbagai kendala yang dihadapi aparat penegak hukum, serta merumuskan upaya optimalisasi sistem pembuktian elektronik dalam penanganan tindak pidana siber. Hasil penelitian diharapkan dapat memberikan kontribusi teoritis terhadap pengembangan hukum pidana dan hukum acara pidana, serta menjadi rekomendasi praktis bagi aparat penegak hukum dan pembuat kebijakan dalam menghadapi tantangan penegakan hukum di era digital.

2. KAJIAN TEORITIS

Berdasarkan uraian latar belakang di atas, maka rumusan masalah dalam penelitian yang berjudul "Problematika Pembuktian Digital dalam Penegakan Hukum Tindak Pidana Siber di Indonesia" adalah sebagai berikut: Bagaimana pengaturan hukum mengenai

pembuktian digital dalam penegakan hukum tindak pidana siber di Indonesia?. Apa saja problematika yang dihadapi aparat penegak hukum serta bagaimana upaya optimalisasi pembuktian digital dalam penegakan hukum tindak pidana siber di Indonesia?.

3. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif, yaitu penelitian yang dilakukan dengan menelaah norma-norma hukum yang tertuang dalam peraturan perundang-undangan, putusan pengadilan, doktrin, dan berbagai literatur yang berkaitan dengan permasalahan yang diteliti. Penelitian hukum normatif bertujuan untuk menemukan asas, konsep, dan kaidah hukum yang mengatur pembuktian digital dalam penegakan hukum tindak pidana siber di Indonesia, serta untuk menganalisis kesesuaian antara norma hukum dengan kebutuhan praktik penegakan hukum di era digital.

Pendekatan yang digunakan dalam penelitian ini meliputi pendekatan perundang-undangan (statute approach), pendekatan konseptual (conceptual approach), dan pendekatan kasus (case approach). Pendekatan perundang-undangan dilakukan dengan menelaah berbagai peraturan yang relevan, antara lain Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana, 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 27 Tahun 2022 tentang Perlindungan Data Pribadi. Pendekatan konseptual digunakan untuk mengkaji teori-teori tentang pembuktian, alat bukti elektronik, digital forensik, dan kebijakan hukum pidana, sedangkan pendekatan kasus dilakukan melalui analisis terhadap perkara-perkara tindak pidana siber yang relevan.

Bahan hukum yang digunakan dalam penelitian ini terdiri atas bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Bahan hukum primer meliputi seluruh peraturan perundang-undangan yang berkaitan dengan pembuktian digital dan tindak pidana siber. Bahan hukum sekunder terdiri dari buku-buku karya para ahli, jurnal ilmiah, artikel akademik, dan hasil penelitian terdahulu, termasuk tulisan dari dosen Fakultas Hukum Universitas Pembangunan Panca Budi yang relevan dengan topik penelitian. Adapun bahan hukum tersier meliputi kamus hukum, ensiklopedia, dan sumber referensi lain yang membantu menjelaskan istilah dan konsep yang digunakan dalam penelitian. Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (library research), yaitu dengan menelusuri, membaca, dan mengkaji berbagai peraturan perundang-undangan, buku, jurnal, karya ilmiah, dan dokumen lainnya yang relevan. Seluruh bahan hukum yang telah dikumpulkan kemudian

dianalisis secara kualitatif dengan menggunakan metode deskriptif-analitis. Analisis dilakukan dengan menguraikan ketentuan hukum yang berlaku, membandingkan pendapat para ahli, serta menghubungkannya dengan permasalahan aktual yang dihadapi dalam praktik pembuktian digital pada perkara tindak pidana siber.

Hasil analisis selanjutnya disusun secara sistematis untuk menjawab rumusan masalah penelitian. Melalui metode ini diharapkan dapat diperoleh pemahaman yang komprehensif mengenai pengaturan hukum pembuktian digital, problematika yang dihadapi aparat penegak hukum, serta formulasi solusi yang tepat untuk mengoptimalkan penegakan hukum terhadap tindak pidana siber di Indonesia.

4. PEMBAHASAN

Pengaturan Hukum Mengenai Pembuktian Digital dalam Penegakan Hukum Tindak Pidana Siber di Indonesia

Pembuktian merupakan unsur sentral dalam proses peradilan pidana karena menjadi sarana bagi hakim untuk memperoleh keyakinan mengenai telah terjadinya suatu tindak pidana dan mengenai siapa pelaku yang harus dimintai pertanggungjawaban pidana. Dalam sistem hukum Indonesia, pembuktian tidak hanya dipahami sebagai proses formal menghadirkan alat bukti, tetapi juga sebagai mekanisme untuk menyeimbangkan kepentingan penegakan hukum dengan perlindungan hak asasi manusia. Keberadaan sistem pembuktian yang jelas dan adaptif menjadi sangat penting, terutama ketika objek pembuktian tidak lagi terbatas pada bukti fisik konvensional, tetapi juga mencakup data elektronik yang memiliki karakteristik khusus (M. Yahya Harahap, 2016).

Secara teoritis, hukum pembuktian dalam perkara pidana di Indonesia menganut sistem pembuktian menurut undang-undang secara negatif (negatief wettelijk bewijsstelsel). Sistem ini menghendaki dua syarat kumulatif, yaitu adanya sekurang-kurangnya dua alat bukti yang sah dan keyakinan hakim mengenai kesalahan terdakwa. Sistem tersebut tetap dipertahankan dalam Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana (KUHAP), yang memperbarui berbagai ketentuan acara pidana agar lebih responsif terhadap perkembangan teknologi informasi. Dengan demikian, walaupun alat bukti elektronik telah diakui, penggunaannya tetap harus memenuhi prinsip legalitas, relevansi, dan reliabilitas agar dapat membentuk keyakinan hakim secara sah (Undang-Undang Nomor 20 Tahun 2025). Dalam konteks hukum acara pidana modern, pembuktian digital merupakan bagian dari perkembangan hukum pembuktian yang mengakomodasi penggunaan informasi elektronik dan dokumen elektronik sebagai alat bukti. Pembuktian digital dapat diartikan sebagai proses

memperoleh, mengamankan, memeriksa, dan menyajikan data elektronik secara sah untuk membuktikan adanya tindak pidana dan keterlibatan pelaku. Karakteristik bukti digital yang mudah berubah, disalin, dan dihapus menuntut adanya perlakuan khusus agar integritas dan autentisitas data tetap terjaga. Oleh sebab itu, pengaturan hukum mengenai pembuktian digital tidak hanya berkaitan dengan pengakuan normatif, tetapi juga dengan prosedur teknis yang menjamin keabsahan alat bukti elektronik (Eoghan Casey, 2011).

Landasan hukum utama mengenai alat bukti elektronik di Indonesia terdapat dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024. Undang-undang tersebut menegaskan bahwa informasi elektronik dan/atau dokumen elektronik beserta hasil cetaknya merupakan alat bukti hukum yang sah dan merupakan perluasan dari alat bukti yang diakui dalam hukum acara yang berlaku. Pengaturan ini memiliki arti penting karena memberikan legitimasi terhadap berbagai bentuk data digital, seperti surat elektronik, rekaman transaksi, log aktivitas, metadata, dan komunikasi daring untuk digunakan dalam proses peradilan pidana (Undang-Undang Nomor 1 Tahun 2024).

Selain Undang-Undang ITE, Undang-Undang Nomor 20 Tahun 2025 tentang KUHAP memberikan dasar yang lebih komprehensif bagi modernisasi sistem pembuktian pidana. KUHAP baru menegaskan bahwa alat bukti elektronik memiliki kedudukan yang setara dengan alat bukti lainnya sepanjang diperoleh secara sah, dijaga keasliannya, dan dapat dipertanggungjawabkan secara ilmiah maupun hukum. Pengaturan ini menunjukkan bahwa hukum acara pidana Indonesia telah mengadopsi perkembangan teknologi sebagai bagian integral dari proses peradilan, sekaligus menegaskan pentingnya standar penanganan barang bukti digital (Undang-Undang Nomor 20 Tahun 2025).

Dalam praktik penegakan hukum, validitas alat bukti elektronik sangat bergantung pada terpenuhinya tiga prinsip utama, yaitu autentisitas (authenticity), integritas (integrity), dan reliabilitas (reliability). Autentisitas berkaitan dengan kemampuan membuktikan bahwa data benar-benar berasal dari sumber yang dinyatakan. Integritas menunjukkan bahwa data tidak mengalami perubahan sejak pertama kali diperoleh, sedangkan reliabilitas menyangkut tingkat kepercayaan terhadap metode dan perangkat yang digunakan untuk memperoleh dan menganalisis data tersebut. Ketiga prinsip tersebut merupakan fondasi utama dalam menentukan kekuatan pembuktian alat bukti elektronik (Eoghan Casey, 2011). Pengaturan hukum mengenai pembuktian digital juga tidak dapat dipisahkan dari peranan digital forensik. Digital forensik merupakan cabang ilmu yang digunakan untuk mengidentifikasi, mengamankan, mengekstraksi, dan menganalisis bukti elektronik dengan metode yang dapat

dipertanggungjawabkan secara ilmiah. Hasil pemeriksaan digital forensik biasanya disampaikan melalui keterangan ahli dan laporan teknis yang mendukung pembuktian di persidangan. Dengan demikian, digital forensik berfungsi sebagai jembatan antara data elektronik yang bersifat teknis dengan kebutuhan pembuktian dalam hukum acara pidana (Suci Ramadani).

Selain pengaturan nasional, pembuktian digital juga dipengaruhi oleh perkembangan standar internasional. United Nations Office on Drugs and Crime menekankan pentingnya standardisasi penanganan barang bukti digital, pelatihan aparat penegak hukum, dan kerja sama lintas negara untuk menghadapi karakter transnasional cybercrime. Standar internasional tersebut memberikan pedoman bagi negara-negara, termasuk Indonesia, dalam menyusun kebijakan dan prosedur penanganan alat bukti elektronik yang efektif dan akuntabel (United Nations Office on Drugs and Crime, 2013).

Dari perspektif doktrin hukum, Andi Hamzah menyatakan bahwa hukum pembuktian harus berkembang seiring perubahan masyarakat dan kemajuan teknologi agar tetap mampu menjamin keadilan. Pandangan ini menegaskan bahwa pengakuan terhadap alat bukti elektronik merupakan konsekuensi logis dari transformasi digital yang telah mengubah cara manusia berkomunikasi dan bertransaksi. Oleh karena itu, pembaruan hukum acara pidana melalui KUHAP baru merupakan langkah penting untuk memastikan bahwa sistem peradilan tetap relevan terhadap perkembangan zaman (Andi Hamzah, 2019).

Dalam hubungan dengan tindak pidana siber, pengaturan pembuktian digital juga berkaitan dengan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Undang-undang ini memberikan kerangka hukum yang menegaskan pentingnya perlindungan terhadap data pribadi sekaligus menetapkan konsekuensi hukum terhadap penyalahgunaan data. Dalam perkara cybercrime yang berkaitan dengan pencurian atau kebocoran data, alat bukti elektronik memiliki peran yang sangat penting untuk membuktikan adanya akses ilegal, transfer data, dan dampak yang ditimbulkan (Undang-Undang Nomor 27 Tahun 2022).

Secara sistematis, pengaturan hukum mengenai pembuktian digital di Indonesia menunjukkan adanya integrasi antara hukum materiil, hukum acara, dan kebijakan keamanan siber. Undang-Undang ITE memberikan legitimasi terhadap alat bukti elektronik, KUHAP baru menyediakan kerangka prosedural, Undang-Undang Perlindungan Data Pribadi memperkuat aspek perlindungan hak, dan praktik digital forensik menyediakan metode ilmiah untuk menguji keabsahan bukti. Integrasi ini membentuk fondasi normatif yang cukup kuat untuk mendukung penegakan hukum terhadap tindak pidana siber (Rahmayanti). Dengan demikian, dapat disimpulkan bahwa pengaturan hukum mengenai pembuktian digital dalam penegakan

hukum tindak pidana siber di Indonesia telah berkembang secara signifikan. Melalui Undang-Undang Nomor 20 Tahun 2025 tentang KUHAP, Undang-Undang Nomor 1 Tahun 2024 tentang ITE, dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Indonesia telah memiliki dasar hukum yang memadai untuk mengakui, mengatur, dan memanfaatkan alat bukti elektronik dalam proses peradilan pidana. Tantangan selanjutnya terletak pada konsistensi implementasi, peningkatan kapasitas aparat, dan penyempurnaan standar teknis agar pembuktian digital dapat memberikan kepastian hukum, keadilan, dan efektivitas dalam penegakan hukum cybercrime.

Problematika yang Dihadapi Aparat Penegak Hukum serta Upaya Optimalisasi Pembuktian Digital dalam Penegakan Hukum Tindak Pidana Siber di Indonesia

Meskipun Indonesia telah memiliki landasan normatif yang cukup kuat melalui Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana, Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik, dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, praktik pembuktian digital dalam penanganan tindak pidana siber masih menghadapi berbagai kendala yang kompleks. Tantangan tersebut tidak hanya bersifat yuridis, tetapi juga mencakup aspek teknis, kelembagaan, sumber daya manusia, dan kerja sama internasional. Kompleksitas tersebut menyebabkan proses pembuktian sering kali tidak berjalan secara optimal, sehingga memengaruhi efektivitas penegakan hukum terhadap cybercrime (Barda Nawawi Arief, 2016).

Problematika pertama terletak pada keterbatasan sumber daya manusia yang memiliki kompetensi di bidang digital forensik. Tidak semua penyidik, penuntut umum, maupun hakim memiliki pemahaman yang memadai mengenai karakteristik alat bukti elektronik, metode ekstraksi data, analisis metadata, serta teknik menjaga integritas barang bukti digital. Akibatnya, terdapat potensi kesalahan dalam proses penyitaan, pemeriksaan, dan penyajian alat bukti di persidangan. Dalam konteks ini, kemampuan teknis aparat penegak hukum menjadi faktor penentu dalam memastikan bahwa alat bukti elektronik dapat diterima dan memiliki kekuatan pembuktian yang optimal (Suci Ramadani). Permasalahan kedua adalah keterbatasan sarana dan prasarana, khususnya laboratorium digital forensik dan perangkat lunak analisis data elektronik. Di beberapa daerah, aparat penegak hukum masih harus mengandalkan fasilitas terbatas atau mengirim perangkat ke laboratorium tertentu, yang menyebabkan proses penyidikan memerlukan waktu lebih lama. Padahal, bukti digital bersifat sangat dinamis dan rentan mengalami perubahan. Keterlambatan dalam proses analisis dapat berakibat pada hilangnya data penting yang seharusnya dapat digunakan untuk mengungkap tindak pidana (Eoghan Casey, 2011).

Problematika ketiga berkaitan dengan belum seragamnya standar operasional prosedur (SOP) dalam penanganan barang bukti elektronik. Setiap tahapan, mulai dari penyitaan perangkat, pembuatan salinan forensik, penyimpanan data, hingga penyajian hasil analisis, harus dilakukan sesuai prinsip chain of custody. Apabila prosedur tersebut tidak dijalankan secara konsisten, maka keaslian dan integritas alat bukti dapat dipersoalkan oleh pihak terdakwa. Oleh karena itu, standardisasi prosedur merupakan syarat utama untuk menjamin validitas alat bukti digital (Rahmayanti).

Tantangan keempat adalah sifat transnasional dari tindak pidana siber. Banyak data yang dibutuhkan untuk proses pembuktian tersimpan pada server di luar negeri dan berada di bawah kendali perusahaan teknologi global. Untuk memperoleh data tersebut, aparat penegak hukum harus menempuh mekanisme mutual legal assistance atau kerja sama internasional lainnya. Proses tersebut sering memerlukan waktu yang panjang dan menghadapi hambatan birokrasi maupun perbedaan sistem hukum antarnegara. Kondisi ini menjadi salah satu kendala utama dalam pembuktian cybercrime yang melibatkan lintas yurisdiksi (United Nations Office on Drugs and Crime, 2013).

Permasalahan kelima adalah penggunaan teknologi yang semakin canggih oleh pelaku, seperti enkripsi, virtual private network (VPN), jaringan anonim, dan aplikasi komunikasi dengan end-to-end encryption. Teknologi tersebut mempersulit pelacakan aktivitas pelaku dan menyulitkan aparat untuk memperoleh data yang relevan. Bahkan ketika perangkat telah disita, isi data sering kali tidak dapat diakses tanpa keahlian dan alat khusus. Situasi ini menunjukkan bahwa perkembangan teknologi menciptakan perlombaan kemampuan antara pelaku kejahatan dan aparat penegak hukum (Sigid Suseno, 2020).

Problematika keenam adalah belum seragamnya pemahaman mengenai kekuatan pembuktian alat bukti elektronik di antara aparat penegak hukum. Dalam praktik, masih terdapat perbedaan pandangan mengenai validitas tangkapan layar, percakapan digital, rekaman suara, maupun metadata. Perbedaan interpretasi tersebut dapat menimbulkan inkonsistensi dalam proses penyidikan, penuntutan, dan pemeriksaan di persidangan. Akibatnya, kepastian hukum dan konsistensi putusan pengadilan dapat terganggu (Eddy O.S. Hiariej, 2021).

Permasalahan ketujuh berkaitan dengan perlindungan hak asasi manusia dan privasi. Pengumpulan dan pemeriksaan data elektronik harus dilakukan secara proporsional dan berdasarkan kewenangan yang sah. Penyitaan perangkat elektronik tanpa prosedur yang benar dapat menimbulkan pelanggaran terhadap hak privasi dan hak atas perlindungan data pribadi. Oleh karena itu, aparat penegak hukum harus menyeimbangkan kebutuhan pembuktian dengan

penghormatan terhadap hak-hak konstitusional warga negara (Undang-Undang Nomor 27 Tahun 2022). Untuk mengatasi berbagai problematika tersebut, langkah pertama yang perlu dilakukan adalah peningkatan kapasitas sumber daya manusia melalui pendidikan dan pelatihan yang berkelanjutan. Penyidik, penuntut umum, hakim, dan advokat perlu dibekali dengan pengetahuan mengenai digital forensik, alat bukti elektronik, dan perkembangan teknologi informasi. Dengan demikian, setiap aparat penegak hukum memiliki pemahaman yang seragam mengenai prosedur dan standar pembuktian digital (Andi Hamzah, 2019). Langkah kedua adalah penguatan sarana dan prasarana, termasuk pembangunan laboratorium digital forensik yang terakreditasi di berbagai wilayah Indonesia. Ketersediaan perangkat keras dan perangkat lunak yang memadai akan mempercepat proses analisis data elektronik dan meningkatkan kualitas hasil pemeriksaan. Selain itu, standardisasi peralatan dan metode pemeriksaan penting untuk menjamin konsistensi dan akurasi hasil digital forensik (Badan Siber dan Sandi Negara, 2022).

Langkah ketiga adalah penyusunan dan penerapan standar operasional prosedur nasional mengenai penanganan barang bukti elektronik. SOP tersebut harus mengatur secara rinci tata cara penyitaan, pembuatan forensic image, dokumentasi chain of custody, analisis, dan penyajian alat bukti di persidangan. Dengan adanya SOP yang seragam, validitas alat bukti digital dapat lebih terjamin dan risiko sengketa mengenai keaslian data dapat diminimalkan (Eoghan Casey, 2011).

Langkah keempat adalah penguatan kerja sama antarlembaga dan kerja sama internasional. Sinergi antara Kepolisian, Kejaksaan, Pengadilan, Badan Siber dan Sandi Negara, dan kementerian terkait sangat diperlukan untuk mempercepat pertukaran informasi dan koordinasi teknis. Di tingkat internasional, optimalisasi mutual legal assistance, perjanjian bilateral, dan partisipasi dalam forum global menjadi sangat penting untuk memperoleh data yang berada di luar yurisdiksi Indonesia (United Nations Office on Drugs and Crime, 2013). Dengan demikian, problematika pembuktian digital dalam penegakan hukum tindak pidana siber di Indonesia merupakan tantangan multidimensional yang memerlukan solusi yang terintegrasi. Keberhasilan penegakan hukum tidak hanya ditentukan oleh kelengkapan regulasi, tetapi juga oleh kompetensi aparat, kesiapan infrastruktur, keseragaman prosedur, dan efektivitas kerja sama lintas negara. Apabila langkah-langkah optimalisasi tersebut dilaksanakan secara konsisten, pembuktian digital akan menjadi instrumen yang semakin efektif dalam mewujudkan penegakan hukum yang adil, modern, dan responsif terhadap perkembangan teknologi.

5. KESIMPULAN DAN SARAN

Kesimpulan

Pengaturan hukum mengenai pembuktian digital dalam penegakan hukum tindak pidana siber di Indonesia telah memiliki landasan normatif yang kuat dan semakin komprehensif. Pengakuan terhadap informasi elektronik dan/atau dokumen elektronik sebagai alat bukti yang sah diatur dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Selanjutnya, Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana memperkuat sistem pembuktian modern dengan memberikan dasar prosedural yang lebih jelas mengenai penggunaan alat bukti elektronik, pemeriksaan digital, dan perlindungan hak para pihak. Selain itu, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi melengkapi kerangka hukum tersebut, khususnya dalam perkara yang berkaitan dengan penyalahgunaan data pribadi. Dengan demikian, secara normatif Indonesia telah memiliki perangkat hukum yang memadai untuk mendukung pembuktian digital dalam penegakan hukum tindak pidana siber. Problematika utama dalam pembuktian digital terletak pada aspek sumber daya manusia, sarana prasarana, standardisasi prosedur, tantangan yurisdiksi lintas negara, serta perkembangan teknologi yang digunakan pelaku kejahatan. Keterbatasan kompetensi aparat penegak hukum, minimnya laboratorium digital forensik, belum seragamnya penerapan chain of custody, dan kesulitan memperoleh data yang berada di luar negeri menjadi hambatan signifikan dalam proses pembuktian. Untuk mengatasi kendala tersebut, diperlukan langkah-langkah optimalisasi berupa peningkatan kapasitas aparat melalui pendidikan dan pelatihan, penguatan infrastruktur digital forensik, penyusunan standar operasional prosedur nasional, serta peningkatan kerja sama antarlembaga dan kerja sama internasional. Apabila langkah-langkah tersebut dilaksanakan secara konsisten, pembuktian digital akan mampu menjadi instrumen yang efektif dalam mewujudkan penegakan hukum yang modern, adil, dan responsif terhadap perkembangan teknologi.

Saran

Pemerintah dan pembentuk undang-undang perlu terus melakukan harmonisasi dan penyempurnaan regulasi yang berkaitan dengan pembuktian digital, termasuk penyusunan peraturan pelaksana yang lebih teknis mengenai tata cara penyitaan, pemeriksaan, dan penyajian alat bukti elektronik di persidangan agar tidak menimbulkan perbedaan penafsiran di antara aparat penegak hukum. Aparat penegak hukum, khususnya Kepolisian, Kejaksaan, dan Pengadilan, perlu meningkatkan kompetensi sumber daya manusia melalui pendidikan dan pelatihan yang berkelanjutan di bidang digital forensik, teknologi informasi, dan hukum siber,

serta memperluas pembangunan laboratorium digital forensik yang terstandarisasi dan terakreditasi di berbagai daerah. Kerja sama antarlembaga dan kerja sama internasional perlu diperkuat untuk mempercepat pertukaran data dan informasi yang berkaitan dengan tindak pidana siber, terutama dalam perkara yang melibatkan server dan penyedia layanan elektronik yang berada di luar wilayah Indonesia, sehingga proses pembuktian dapat berlangsung lebih efektif dan efisien.

DAFTAR REFERENSI

Arief, B. N. (2016). *Bunga rampai kebijakan hukum pidana*. Kencana Prenada Media Group.

Badan Siber dan Sandi Negara. (n.d.). *Laporan tahunan keamanan siber Indonesia*. https://www.bssn.go.id

Casey, E. (2011). *Digital evidence and computer crime* (3rd ed.). Academic Press.

Google Scholar. (n.d.). *Database referensi ilmiah tentang pembuktian digital dan tindak pidana siber*. https://scholar.google.com

Hamzah, A. (2019). *Hukum acara pidana Indonesia*. Sinar Grafika.

Harahap, M. Y. (2016). *Pembahasan permasalahan dan penerapan KUHAP: Pemeriksaan sidang pengadilan, banding, kasasi, dan peninjauan kembali*. Sinar Grafika.

Hiariej, E. O. S. (2021). *Hukum acara pidana*. Universitas Terbuka.

Jaringan Dokumentasi dan Informasi Hukum Badan Pemeriksa Keuangan Republik Indonesia. (n.d.). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*. https://peraturan.bpk.go.id

Jaringan Dokumentasi dan Informasi Hukum Dewan Perwakilan Rakyat Republik Indonesia. (n.d.). *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. https://www.dpr.go.id/jdih

Rahmayanti. (n.d.). *Analisis yuridis terhadap manipulasi data elektronik sebagai bentuk tindak pidana siber* [Artikel ilmiah, Fakultas Hukum Universitas Pembangunan Panca Budi].

Ramadani, S. (n.d.). *Peran digital forensik dalam pembuktian tindak pidana siber di Indonesia* [Artikel ilmiah, Fakultas Hukum Universitas Pembangunan Panca Budi].

Repository Universitas Pembangunan Panca Budi. (n.d.). *Kumpulan artikel ilmiah dan penelitian Fakultas Hukum Universitas Pembangunan Panca Budi*. https://repository.pancabudi.ac.id

Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*.

Republik Indonesia. (2023). *Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana*.

Republik Indonesia. (2024). *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.

Republik Indonesia. (2025). *Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana*.

Suseno, S. (2020). *Hukum siber Indonesia*. PT Refika Aditama.

Suseno, S. (n.d.). Kedudukan alat bukti elektronik dalam sistem pembuktian pidana Indonesia. *Jurnal Ilmu Hukum*.

United Nations Office on Drugs and Crime. (2013). *Comprehensive study on cybercrime*. United Nations.

United Nations Office on Drugs and Crime. (2013). *Comprehensive study on cybercrime*. https://www.unodc.org/unodc/en/organized-crime/comprehensive-study-on-cybercrime.html

Widodo. (2012). *Cybercrime dan cyberlaw dalam sistem hukum Indonesia*. PT RajaGrafindo Persada.

Widodo. (n.d.). Penegakan hukum pidana terhadap kejahatan siber di Indonesia. *Jurnal Hukum dan Peradilan*.