
**TRANSFORMASI SISTEM PEMBUKTIAN PIDANA INDONESIA
MENUJU ERA DIGITAL FORENSIK KEABSAHAN INFORMASI
ELEKTRONIK SEBAGAI ALAT BUKTI HUKUM MATERIIL DAN
FORMIL**

**Naufal Qushoyyi, Naufal Aziiz, Decky hermawan, M Ariel Anggara P, Ria Anggraeni
Utami**

Universitas Bengkulu

nqushoyyi@gmail.com, naufalaziizz00@gmail.com, deki120818@gmail.com,
arielanggara04@gmail.com, riaanggraeniutami@unib.ac.id

ABSTRAK

Penelitian ini menganalisis secara normatif transformasi fundamental dalam sistem hukum pembuktian pidana Indonesia, khususnya melalui adopsi informasi dan/atau dokumen elektronik sebagai alat bukti sah di samping lima alat bukti tradisional dalam Kitab Undang-Undang Hukum Acara Pidana (KUHP). Fokus utama adalah telaah terhadap Pasal 184 KUHP yang menjadi landasan sistem pembuktian terbatas, serta analisis pasal terhadap Pasal 5 Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagai sumber perluasan hukum pembuktian pidana. Metode penelitian hukum normatif digunakan untuk mengkaji harmonisasi antara asas *lex specialis derogat legi generali* dan prinsip legalitas dalam konteks teknologi digital. Hasil penelitian menunjukkan adanya dualisme sistem pembuktian yang memerlukan standarisasi prosedur Digital Evidence First Responder (DEFRR) dan Chain of Custody (CoC) guna menjamin integritas, autentisitas, dan ketersediaan bukti digital. Penelitian ini menyimpulkan bahwa keabsahan bukti elektronik sangat bergantung pada ketaatan formil prosedur forensik, bukan hanya substansi materilnya, dan merekomendasikan revisi regulasi teknis untuk menciptakan kepastian hukum.

Kata Kunci: Pembuktian Pidana, Bukti Elektronik, KUHP, UU ITE, Forensik Digital.

PENDAHULUAN

Sistem hukum acara pidana merupakan pilar utama dalam penegakan hukum yang adil dan beradab, menentukan prosedur formal untuk mencari serta menemukan kebenaran materil di pengadilan. Pasal 184 Kitab Undang-Undang Hukum Acara Pidana (KUHP) telah lama menjadi pedoman fundamental dengan membatasi alat bukti yang sah secara limitatif. Pembatasan ini mencakup keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa, menciptakan sistem pembuktian yang dikenal sebagai sistem negatif-legal. KUHP

menetapkan bahwa vonis bersalah hanya dapat dijatuhkan apabila didukung minimal dua alat bukti yang sah ditambah keyakinan hakim, menggarisbawahi pentingnya keabsahan formil dan materiil alat bukti. Namun, seiring dengan evolusi masyarakat dan perkembangan teknologi informasi, limitasi tersebut mulai menghadapi tantangan serius yang tak terhindarkan.

Era revolusi digital telah melahirkan modus operandi kejahatan yang semakin canggih dan terdigitalisasi, meninggalkan jejak yang tidak selalu berbentuk fisik layaknya tindak pidana konvensional. Data dan informasi kini menjadi aset sekaligus potensi barang bukti krusial dalam mengungkap tindak pidana modern, mulai dari kejahatan siber hingga kejahatan konvensional yang dimediasi oleh teknologi. Perubahan lanskap kejahatan ini menuntut adanya adaptasi proaktif dari instrumen hukum positif agar tetap relevan dan efektif dalam mencapai tujuan penegakan hukum. Oleh karena itu, hukum pembuktian pidana tidak bisa lagi hanya terpaku pada kerangka klasik yang diwarisi dari KUHAP, tetapi harus diperluas cakupannya.

Pemerintah merespons kebutuhan mendesak ini dengan mengundang Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang kemudian diubah dengan Undang-Undang Nomor 19 Tahun 2016. Secara eksplisit, UU ITE mengakui Informasi Elektronik dan/atau Dokumen Elektronik, termasuk hasil cetaknya, sebagai alat bukti hukum yang sah. Ketentuan ini secara yuridis-normatif telah memperluas cakupan alat bukti yang diakui dalam persidangan pidana, menciptakan apa yang dapat disebut sebagai sistem pembuktian terbuka parsial dalam konteks digital. Kehadiran bukti elektronik ini membuka jalan baru bagi penyidik dan penuntut umum untuk membuktikan fakta hukum yang sebelumnya sulit dijangkau melalui alat bukti konvensional.

Meskipun perluasan alat bukti telah diatur, integrasi bukti elektronik ke dalam praktik peradilan pidana tidaklah tanpa hambatan, mengingat karakteristiknya yang unik. Bukti digital sangat rapuh, mudah dimanipulasi, dan tidak memiliki bentuk fisik yang tetap, sehingga menuntut prosedur penanganan yang sangat ketat dan spesifik. Isu krusial muncul terkait dengan aspek formil pembuktian, termasuk bagaimana memastikan autentisitas, integritas, dan orisinalitas dari bukti elektronik yang diajukan di persidangan. Pengawasan terhadap proses pengumpulan, penyitaan, analisis, hingga presentasi bukti digital, yang dikenal sebagai *Chain of Custody* (CoC), menjadi penentu utama keabsahan bukti tersebut di hadapan hakim.

Oleh karena itu, diperlukan kajian hukum normatif yang mendalam untuk menganalisis bagaimana harmonisasi antara ketentuan limitatif KUHAP dan ketentuan ekstensif UU ITE

dapat ditegakkan secara konsisten. Telaah hukum ini harus berfokus pada interpretasi pasal-pasal kunci serta implikasinya terhadap doktrin pembuktian yang telah mapan di Indonesia. Penting pula untuk mengidentifikasi standar prosedur teknis yang wajib dipatuhi oleh aparat penegak hukum, seperti penerapan prinsip *Digital Evidence First Responder* (DEFRR) dan kebutuhan akan infrastruktur forensik digital yang tersertifikasi internasional. Tanpa panduan teknis yang baku dan mengikat, potensi sengketa hukum mengenai keabsahan bukti elektronik akan terus menjadi ancaman serius bagi kepastian hukum.

Penelitian ini bertujuan untuk memberikan landasan teoritis-normatif yang kuat mengenai status hukum bukti elektronik dalam kerangka hukum pembuktian pidana Indonesia, serta menawarkan solusi regulatif yang tepat. Melalui analisis hukum murni, artikel ini akan mengupas dualisme sistem pembuktian, menelaah putusan-putusan pengadilan yang relevan, dan merumuskan langkah-langkah strategis untuk memperkuat keabsahan bukti digital. Dengan demikian, diharapkan artikel ini dapat berkontribusi pada pengembangan doktrin hukum acara pidana yang adaptif dan responsif terhadap tuntutan zaman digital, memastikan bahwa kebenaran materiil dapat dicapai melalui alat bukti yang valid dan autentik.

RUMUSAN MASALAH

- A. Bagaimana konstruksi hukum perluasan alat bukti pidana melalui Pasal 5 Undang-Undang ITE harmonisasi dengan asas limitatif Pasal 184 KUHAP dalam mencapai kebenaran materiil?
- B. Apa saja tantangan prosedural dan standarisasi yang harus dipenuhi dalam proses penanganan *Chain of Custody* (CoC) dan forensik digital untuk menjamin keabsahan bukti elektronik di pengadilan?

METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif (*normative legal research*) yang berfokus pada kajian terhadap norma-norma hukum positif yang berlaku, yakni Kitab Undang-Undang Hukum Acara Pidana (KUHAP) dan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Pendekatan yang digunakan adalah pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan analitis (*analytical approach*). Bahan hukum primer yang dianalisis meliputi teks-teks undang-undang tersebut beserta peraturan pelaksana terkait, sedangkan bahan hukum sekunder mencakup literatur hukum, jurnal ilmiah, dan pandangan-pandangan doktrinal para ahli hukum.

Pengumpulan bahan hukum dilakukan melalui studi kepustakaan yang sistematis, diikuti dengan identifikasi isu hukum yang relevan dengan topik transformasi pembuktian pidana di era digital. Analisis bahan hukum dilakukan secara deskriptif-kualitatif dengan teknik interpretasi hukum, yaitu interpretasi gramatikal, sistematis, dan teleologis, untuk menemukan makna dan rasio di balik norma-norma yang ada. Selain itu, dilakukan pula telaah kritis terhadap doktrin-doktrin hukum acara pidana tradisional versus perkembangan hukum pembuktian kontemporer. Tujuan akhir dari metode ini adalah membangun argumentasi normatif yang kokoh mengenai kedudukan hukum, syarat formil, dan syarat materiil keabsahan bukti elektronik dalam sistem peradilan pidana.

HASIL DAN PEMBAHASAN

A. Konstruksi Hukum Perluasan Alat Bukti Pidana melalui Pasal 5 UU ITE dan Harmonisasi dengan Asas Limitatif Pasal 184 KUHAP

Pasal 184 ayat (1) KUHAP secara eksplisit memuat lima jenis alat bukti yang sah dalam hukum acara pidana, menetapkan suatu sistem pembuktian yang bercorak limitatif atau tertutup. Sistem ini bertujuan memberikan kepastian hukum dan perlindungan terhadap hak asasi terdakwa, memastikan bahwa hakim tidak menggunakan alat bukti di luar yang telah ditentukan oleh undang-undang. Namun, sifat kaku dan tertutup dari Pasal 184 ini menjadi problematik ketika berhadapan dengan evolusi kejahatan di ranah digital yang melahirkan bentuk-bentuk bukti baru. Keterbatasan ini mengharuskan adanya intervensi legislatif yang bersifat spesifik untuk mengakomodasi realitas hukum yang berkembang.

Intervensi krusial tersebut diwujudkan melalui Pasal 5 ayat (1) Undang-Undang ITE, yang secara tegas menyatakan bahwa Informasi Elektronik dan/atau Dokumen Elektronik serta hasil cetaknya merupakan alat bukti hukum yang sah. Perumusan pasal ini secara fundamental memperluas daftar alat bukti dalam hukum acara pidana, menciptakan dualisme sistem pembuktian antara KUHAP sebagai *lex generalis* dan UU ITE sebagai *lex specialis*. Secara doktrinal, asas *lex specialis derogat legi generali* memberikan keutamaan penerapan UU ITE untuk tindak pidana yang terkait dengan informasi dan dokumen elektronik, termasuk ketika bukti digital menjadi elemen kunci dalam tindak pidana konvensional.

Telaah terhadap Pasal 5 UU ITE mengungkapkan bahwa legislator tidak bermaksud menggantikan sistem pembuktian KUHAP, melainkan melengkapinya dengan bukti yang setara secara kedudukan hukum. Bukti elektronik diakui sebagai alat bukti yang sah, namun penggunaannya tetap harus memperhatikan ketentuan pidana yang berlaku, termasuk prinsip

minimal dua alat bukti yang sah dan keyakinan hakim. Dengan demikian, bukti elektronik tidak berdiri sendiri melainkan berfungsi sebagai pelengkap atau penguat alat bukti lain, meskipun dalam praktiknya seringkali menjadi alat bukti utama (*prime evidence*) dalam kasus-kasus siber.

Analisis pasal-pasal kunci menunjukkan bahwa harmonisasi terletak pada interpretasi yang progresif dan sistematis. Bukti elektronik dapat dikategorikan sebagai salah satu dari lima alat bukti KUHAP, terutama sebagai 'surat' atau 'petunjuk', tetapi dengan syarat dan prosedur formil tambahan yang diatur oleh UU ITE. Sebagai contoh, bukti digital yang dicetak dapat diperlakukan sebagai 'surat' jika memenuhi syarat formil tertentu, sementara data digital yang memerlukan interpretasi ahli (*expert analysis*) dapat dikategorikan sebagai 'keterangan ahli' atau *petunjuk* yang diperoleh melalui sarana elektronik.

Dalam konteks hukum materiil, keabsahan informasi elektronik sebagai alat bukti bergantung pada kemampuannya untuk memberikan keterangan yang utuh, otentik, dan tidak dapat disangkal mengenai perbuatan pidana. Ini adalah aspek materiil yang harus diuji di persidangan. Keberadaan bukti digital harus mampu merepresentasikan fakta hukum secara akurat, menjawab unsur-unsur tindak pidana yang didakwakan oleh Penuntut Umum.

Namun, tantangan terbesar dalam harmonisasi ini adalah menghindari *l'arbitraire du juge* atau kesewenang-wenangan hakim dalam menilai bukti. Meskipun UU ITE memperluas cakupan, UU ini tidak merinci secara memadai bagaimana prosedur formal KUHAP (penyitaan, penggeledahan) harus diadaptasi untuk ranah digital. Kekosongan regulasi teknis ini seringkali menjadi celah yang dieksploitasi oleh pihak-pihak yang berkepentingan untuk mempersoalkan keabsahan bukti.

Oleh karena itu, diperlukan pedoman interpretasi yang baku yang menegaskan bahwa *lex specialis* UU ITE tidak meniadakan prosedur formil KUHAP. Sebaliknya, ia menambahkan lapisan persyaratan prosedural, terutama yang berkaitan dengan ilmu forensik digital, untuk memastikan bahwa data yang dikumpulkan benar-benar merefleksikan kebenaran. Standar minimum formil ini harus ditekankan untuk menjaga integritas proses peradilan.

Para ahli hukum sepakat bahwa meskipun terjadi perluasan, ruh dari sistem pembuktian negatif-legal harus tetap dipertahankan. Artinya, pengakuan bukti elektronik tidak boleh mengarah pada sistem pembuktian bebas (*vrij bewijs*). Kekuatan pembuktian bukti elektronik harus setara dengan alat bukti KUHAP lainnya, yakni memerlukan dukungan alat bukti lain

dan keyakinan hakim.

Telaah lebih lanjut menunjukkan bahwa putusan pengadilan modern cenderung menerima bukti elektronik asalkan diiringi dengan keterangan ahli forensik yang memadai. Keterangan ahli ini berfungsi sebagai jembatan yang menghubungkan data mentah digital dengan fakta hukum yang relevan, mengubah bukti elektronik menjadi 'keterangan ahli' yang valid menurut Pasal 184 huruf b KUHAP.

Penting untuk dicatat bahwa Pasal 5 ayat (2) UU ITE memberikan pengecualian terhadap bukti elektronik yang diperoleh secara melawan hukum, yang secara implisit mengadopsi prinsip *exclusionary rule* dalam hukum pembuktian. Ini semakin menekankan pentingnya ketaatan pada prosedur formil yang sah dalam pengumpulan bukti digital.

Dengan demikian, konstruksi hukum yang ideal adalah memperlakukan UU ITE sebagai ketentuan prosedural tambahan yang mengatur syarat formil dan materiil spesifik untuk Bukti Elektronik. Harmonisasi ini berhasil menciptakan suatu sistem pembuktian yang adaptif tanpa meninggalkan prinsip-prinsip dasar perlindungan hak terdakwa yang terkandung dalam KUHAP.

Secara teoritis, bukti elektronik dapat dikategorikan sebagai 'perluasan' sekaligus 'penafsiran' atas alat bukti petunjuk dalam KUHAP, terutama mengingat sifatnya yang memerlukan penalaran dari hakim. Namun, pengakuan eksplisit dalam UU ITE menjadikannya kategori bukti tersendiri yang memerlukan perlakuan hukum yang unik. Dualisme ini akan terus ada sampai adanya revisi KUHAP yang secara eksplisit memasukkan bukti elektronik sebagai alat bukti keenam yang sah.

B. Tantangan Prosedural dan Standarisasi *Chain of Custody* (CoC) dan Forensik Digital untuk Menjamin Keabsahan Bukti Elektronik di Pengadilan

Tantangan terbesar dalam penerapan bukti elektronik tidak lagi terletak pada pengakuan substansialnya, tetapi pada pemenuhan persyaratan prosedural formil yang menjamin integritas dan autentisitasnya. Sifat digital yang rapuh, mudah dimodifikasi, dan tidak meninggalkan jejak fisik yang nyata menuntut protokol penanganan yang sangat ketat. Tanpa prosedur yang baku dan terstandarisasi, bukti elektronik, sekokoh apa pun isinya, berisiko dianggap tidak sah atau tidak memiliki kekuatan pembuktian di pengadilan.

Kepatuhan terhadap prinsip *Chain of Custody* (CoC) merupakan prasyarat mutlak untuk

keabsahan bukti digital, berfungsi sebagai rantai dokumentasi yang tidak terputus dari waktu penemuan hingga presentasi di persidangan. CoC mendokumentasikan siapa yang mengumpulkan, kapan, di mana, bagaimana bukti itu disimpan, siapa yang mengaksesnya, dan mengapa. Setiap transfer, analisis, atau penyimpanan harus dicatat secara rinci untuk membuktikan bahwa bukti tersebut tidak mengalami perubahan atau manipulasi yang dapat merusak integritasnya.

Prosedur CoC harus dimulai dengan penerapan prinsip *Digital Evidence First Responder* (DEFER) di lokasi kejadian. DEFER adalah protokol awal yang memastikan bahwa bukti digital, yang seringkali bersifat volatil (seperti data RAM), ditangani secara tepat untuk mencegah kerusakan atau penghilangan. Protokol ini harus mencakup langkah-langkah seperti isolasi perangkat, dokumentasi mendetail, dan pengamanan lingkungan digital untuk menghindari penulisan data baru.

Sayangnya, implementasi DEFER dan CoC dalam praktik penegakan hukum seringkali masih bervariasi karena ketiadaan regulasi teknis yang seragam dan mengikat secara nasional. Kesenjangan ini menciptakan apa yang disebut sebagai 'lubang prosedural' (*procedural gap*) yang dapat dimanfaatkan oleh Terdakwa untuk mengajukan keberatan terhadap admisibilitas bukti. Penuntut umum harus mampu membuktikan CoC tanpa cacat sedikit pun, dari tingkat penyidik hingga ke meja ahli forensik.

Standarisasi forensik digital, terutama yang mengacu pada standar internasional seperti ISO/IEC 27037 dan ISO/IEC 17025, sangat mendesak. ISO/IEC 27037 memberikan panduan mengenai penanganan bukti digital, sementara ISO/IEC 17025 mengatur kompetensi laboratorium forensik. Sertifikasi laboratorium forensik adalah jaminan ilmiah bahwa hasil analisis bukti digital dilakukan oleh pihak yang kompeten dengan metode yang diakui dan dapat dipertanggungjawabkan.

Keterbatasan kapasitas sumber daya manusia (SDM) penyidik juga menjadi hambatan signifikan dalam menjaga CoC yang sempurna. Banyak penyidik masih kurang teredukasi mengenai teknik pengamanan bukti digital yang memerlukan keahlian spesifik yang berbeda dengan penyitaan barang bukti fisik. Pelatihan berkelanjutan dan sertifikasi adalah solusi untuk mengatasi kesenjangan kapasitas ini.

Di tingkat peradilan, hakim dituntut memiliki pemahaman yang memadai mengenai aspek teknis forensik untuk menilai kredibilitas CoC yang disajikan. Proses eksaminasi ahli di

persidangan menjadi sangat vital, di mana ahli harus mampu menjelaskan secara ilmiah dan logis metodologi yang digunakan dan bagaimana integritas bukti dijaga. Keraguan hakim terhadap proses forensik secara langsung akan menggugurkan nilai pembuktian bukti elektronik.

Tantangan lain adalah masalah yurisdiksi dan kewenangan penyitaan data lintas batas, yang semakin umum dalam kejahatan siber transnasional. Hukum acara pidana harus segera diperkuat dengan ketentuan yang mengatur kerja sama internasional dalam konteks penyitaan data, karena CoC dapat terputus hanya karena masalah kewenangan antarnegara. Ketentuan domestik harus mampu mengikat prosedur CoC global.

Untuk memperkuat argumentasi normatif dan prosedural, berikut adalah tabel konseptual yang merangkum *Hierarki Persyaratan Admisibilitas Bukti Elektronik* yang ideal di Indonesia, menggabungkan KUHAP dan UU ITE:

Kriteria Admisibilitas	Landasan Hukum	Standar Prosedural	Kekuatan Pembuktian Ideal
Keleluasaan (Legalitas)	Pasal 184 KUHAP <i>jo.</i> Pasal 5 UU ITE	Penyitaan/Penggeledahan sesuai KUHAP	Bukti Sah, Memiliki Kekuatan Hukum
Integritas (Keutuhan)	Pasal 5 ayat (1) UU ITE	Protokol DEFR (Akuisisi forensik/Hashing)	Tidak dimodifikasi, otentik dengan sumber
Autentisitas (Keaslian)	Pasal 6 UU ITE	Dokumentasi <i>Chain of Custody</i> (CoC)	Dapat diverifikasi dari asal-usulnya
Relevansi (Keterkaitan)	Pasal 183 & 184 KUHAP	Keterangan Ahli Forensik	Mendukung keyakinan hakim, relevan dengan unsur pidana
Kompetensi (Keahlian)	Pasal 184 huruf b KUHAP	Sertifikasi Ahli (ISO/IEC 17025)	Validitas metode ilmiah teruji

Tabel ini menunjukkan bahwa keabsahan bukti elektronik tidak dapat dipisahkan dari standar prosedural forensik yang ketat. Ketaatan terhadap DEFR dan CoC harus menjadi norma baku dalam setiap penanganan perkara yang melibatkan bukti digital, melampaui sekadar

kepatuhan terhadap prosedur penyitaan fisik. Kegagalan dalam salah satu elemen CoC, misalnya dokumentasi *hashing* (sidik jari digital) yang tidak memadai, harusnya dapat menggugurkan admisibilitas bukti tersebut.

Peran regulator, terutama Mahkamah Agung dan lembaga teknis terkait, menjadi krusial dalam menyusun Pedoman Standar Operasional Prosedur (SOP) yang rinci mengenai DEFR dan CoC, memastikan keseragaman praktik di seluruh yurisdiksi. Tanpa pedoman yang terperinci, prinsip *due process of law* terancam terlanggar, dan pengadilan akan terus dihadapkan pada perdebatan teknis yang menghambat proses penemuan kebenaran materiil. Pada akhirnya, jaminan keabsahan bukti elektronik terletak pada akuntabilitas dan transparansi seluruh rantai penanganan forensik digital.

Perbedaan mendasar antara bukti fisik dan bukti elektronik terletak pada *volatilitas* data digital, yang memerlukan *imaging* atau *hashing* segera untuk menjaga integritasnya. Prosedur *hashing* ini menghasilkan sidik jari digital yang unik, yang harus dicatat dalam berita acara penyitaan. Sidik jari digital ini adalah kunci formil untuk membuktikan bahwa data tidak mengalami perubahan sejak saat akuisisi. Proses ini secara teknis lebih rumit dibandingkan penyitaan barang bukti fisik, yang hanya memerlukan segel dan tanda tangan saksi. Oleh karena itu, *hashing* harus diatur secara eksplisit dalam regulasi setingkat Peraturan Kapolri atau Peraturan Jaksa Agung.

Telaah mendalam terhadap prinsip legalitas KUHAP menunjukkan bahwa setiap perluasan alat bukti harus tetap berbasis pada undang-undang. UU ITE memenuhi syarat ini sebagai *lex specialis*, namun kekosongan prosedur teknisnya harus diisi dengan peraturan di bawahnya. Ketentuan mengenai ahli forensik digital harus diperkuat, memastikan bahwa ahli yang memberikan keterangan adalah pihak yang benar-benar independen dan kompeten. Kompetensi ahli ini adalah pilar penting dalam mengubah data mentah menjadi fakta hukum yang dapat dipahami oleh majelis hakim yang non-teknis.

Aspek hak asasi manusia juga menjadi pertimbangan penting dalam harmonisasi ini, terutama terkait dengan hak privasi dan perlindungan data pribadi. Bukti elektronik seringkali mengandung data yang sangat sensitif, memerlukan batasan yang jelas mengenai lingkup penyitaan dan analisis. Batasan ini harus ditetapkan melalui perintah pengadilan yang spesifik dan terperinci, menghindari *fishing expeditions* atau penyitaan data yang tidak relevan. Perlindungan privasi harus diseimbangkan dengan kebutuhan untuk mengungkap kebenaran

materiil dalam perkara pidana.

Dalam konteks putusan pengadilan, telah banyak preseden yang menunjukkan penerimaan bukti elektronik, namun seringkali dengan pertimbangan hukum yang menekankan unsur 'petunjuk' dari bukti tersebut. Hakim menggunakan bukti elektronik untuk memperkuat bukti konvensional lainnya, seperti keterangan saksi, yang menunjukkan masih adanya kehati-hatian dalam menempatkan bukti digital sebagai alat bukti tunggal yang menentukan. Kecenderungan ini mengindikasikan bahwa keyakinan hakim masih sangat dipengaruhi oleh kelengkapan prosedur formil penyitaan dan analisis forensik.

KESIMPULAN

Konstruksi hukum pembuktian pidana di Indonesia telah mengalami transformasi signifikan dengan diakuinya Informasi Elektronik dan/atau Dokumen Elektronik sebagai alat bukti yang sah melalui Pasal 5 UU ITE, melengkapi lima alat bukti limitatif Pasal 184 KUHAP. Harmonisasi antara kedua undang-undang ini menghasilkan dualisme sistem pembuktian, di mana UU ITE berfungsi sebagai *lex specialis* yang memperluas cakupan alat bukti tanpa meniadakan prinsip-prinsip dasar KUHAP. Keabsahan materiil bukti elektronik, yaitu kemampuannya merefleksikan fakta hukum, harus selalu didukung oleh keabsahan formil yang sempurna, terutama terkait prosedur pengumpulan dan analisis. Perluasan ini, meskipun progresif, menuntut pemahaman sistematis bahwa bukti elektronik harus diinterpretasikan dan diuji dengan standar yang lebih tinggi dibandingkan bukti fisik konvensional.

Tantangan terbesar dalam implementasi terletak pada ranah prosedural, khususnya dalam penegakan standar *Chain of Custody* (CoC) dan forensik digital yang baku, yang belum diatur secara memadai dalam regulasi teknis. Keutuhan (*integrity*) dan keaslian (*authenticity*) bukti elektronik hanya dapat dijamin melalui ketaatan ketat pada protokol *Digital Evidence First Responder* (DEFRR) dan sertifikasi laboratorium sesuai ISO/IEC 17025. Kegagalan dalam menjaga CoC dapat serta merta menggugurkan kekuatan pembuktian bukti digital, terlepas dari relevansi substansinya, karena melanggar prinsip *due process of law*. Oleh karena itu, diperlukan intervensi regulatif yang cepat untuk memastikan kepastian hukum dan mencegah *procedural gap* yang merugikan.

DAFTAR PUSTAKA

Anggraini, W., & Puspita, N. (2023). Integritas bukti elektronik dan urgensi SOP nasional forensik digital. *Jurnal Advokasi Hukum Indonesia*, 5(1), 301–320.

- Ariyanto, A. (2021). Urgensi pembaruan sistem pembuktian pidana di era digital. *Jurnal Hukum & Pembangunan*, 51(2), 325–342.
- Hasibuan, R. H. (2021). Kajian yuridis bukti digital dan penerapan exclusionary rule. *Jurnal Hukum dan Peradilan*, 10(2), 245–264.
- Hutagaol, T. (2023). Standarisasi forensik digital berbasis ISO/IEC 27037 di Indonesia. *Jurnal Forensik Digital Nusantara*, 2(1), 10–28.
- Kusumawardani, R. (2021). Perlindungan hak privasi dalam penyitaan data elektronik. *Jurnal HAM Indonesia*, 12(1), 65–82.
- Mahendra, Y. (2021). Problematika autentikasi data digital di peradilan pidana. *Jurnal Hukum dan Teknologi*, 6(2), 112–129.
- Nugroho, B., & Aprilianto, A. (2022). Digital Evidence First Responder (DEFRR) dalam praktik penyidikan di Indonesia. *Jurnal Kepolisian Republik Indonesia*, 8(1), 77–93.
- Pratama, M. R., & Yuliana, F. (2022). Keabsahan informasi elektronik sebagai alat bukti menurut KUHAP dan UU ITE. *Jurnal Rechts Vinding*, 11(1), 87–104.
- Putri, S., & Lestari, M. (2020). Tantangan pembuktian elektronik dalam perkara pidana konvensional. *Jurnal Yudisial*, 13(3), 456–474.
- Rachman, F., & Dewi, I. (2020). Analisis putusan pengadilan terkait bukti elektronik sebagai petunjuk. *Jurnal Putusan Pengadilan Indonesia*, 9(4), 500–518.
- Rahmatullah, I. (2022). Penerapan Chain of Custody (CoC) pada barang bukti digital oleh penyidik. *Jurnal Criminal Justice*, 5(1), 51–67.
- Sakti, D. A. (2022). Peran ahli forensik digital dalam pembuktian di persidangan. *Jurnal Peradilan Indonesia*, 3(2), 189–206.
- Setiawan, D. (2020). Analisis yuridis kedudukan bukti elektronik dalam peradilan pidana. *Jurnal Hukum Prioris*, 10(3), 201–215.
- Suryani, L., & Karim, A. (2021). Asas lex specialis dalam penerapan UU ITE terhadap KUHAP. *Jurnal Legislasi Indonesia*, 18(2), 233–248.
- Widodo, S., & Hamdani, R. (2023). Digital evidence dalam pembuktian tindak pidana siber. *Jurnal Penegakan Hukum Indonesia*, 4(2), 144–161.