Jejakdigital
JURNAL ILMIAH MULTIDISIPLIN
Available online at https://indojurnal.com/index.php/jejakdigital

eISSN 3089-7734; pISSN 3089-7742
Vol. 2, No. 4, Tahun 2026
doi.org/10.63822/r9j9e578
Hal. 8324-8333

Kepastian Hukum Penggunaan Bukti Digital Berbasis *Cloud Storage* dalam Pembuktian Perkara Pidana

Ahmad Parhan[1], Aturkian Laia[2]
Ilmu Hukum, Hukum, Universitas Dirgantara Marsekal Suryadarma, Jakarta Timur, Indonesia[1]
Ilmu Hukum, Hukum, Universitas Dirgantara Marsekal Suryadarma, Jakarta Timur, Indonesia[2]

*Email Korespodensi: ahmadparhan9595@gmail.com

Sejarah Artikel:

Diterima 10-07-2026
Disetujui 15-07-2026
Diterbitkan 17-07-2026

ABSTRACT

The rapid development of cloud storage technology has transformed electronic data storage while creating new challenges for criminal evidence in Indonesia. This study analyzes the legal status of cloud storage-based digital evidence, legal certainty regarding its admissibility and evidentiary value, and the challenges associated with its use in criminal proceedings. The research employs a normative legal method using statutory and conceptual approaches based on the Indonesian Criminal Procedure Code, the Electronic Information and Transactions Law, the Personal Data Protection Law, and other relevant regulations. The findings indicate that cloud storage-based digital evidence has been legally recognized as an extension of admissible evidence. However, legal certainty remains limited due to the absence of specific rules governing evidence acquisition, authentication, chain of custody, and cloud forensics. Therefore, strengthening technical regulations, harmonizing legal frameworks, and enhancing international legal cooperation are essential to ensure legal certainty in criminal proceedings involving cloud-based digital evidence.

Keywords: *digital evidence; cloud storage; legal certainty; criminal evidence; criminal procedural law.*

ABSTRAK

Perkembangan teknologi *cloud storage* mengubah sistem penyimpanan informasi elektronik sekaligus menghadirkan tantangan dalam pembuktian perkara pidana di Indonesia. Penelitian ini bertujuan menganalisis kedudukan hukum bukti digital berbasis *cloud storage*, kepastian hukum atas keabsahan dan kekuatan pembuktiannya, serta tantangan penggunaannya dalam sistem peradilan pidana. Penelitian menggunakan metode yuridis normatif dengan pendekatan perundang-undangan dan konseptual berdasarkan Kitab Undang-Undang Hukum Acara Pidana, Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Pelindungan Data Pribadi, serta peraturan terkait. Hasil penelitian menunjukkan bahwa bukti digital berbasis *cloud storage* telah diakui sebagai perluasan alat bukti yang sah, tetapi kepastian hukumnya masih terbatas akibat belum adanya pengaturan mengenai akuisisi, otentikasi, *chain of custody*, dan *cloud forensics*. Oleh karena itu, diperlukan penguatan regulasi teknis, harmonisasi peraturan, serta kerja sama hukum internasional untuk menjamin kepastian hukum dalam pembuktian pidana.

Katakunci: bukti digital; *cloud storage*; kepastian hukum; pembuktian pidana; hukum acara pidana.

PENDAHULUAN

Transformasi digital telah mengubah cara masyarakat menyimpan dan mengelola informasi. Data yang semula tersimpan pada media fisik seperti kertas, kaset, atau *hard disk* lokal, kini semakin banyak berpindah ke ruang penyimpanan berbasis awan (*cloud storage*), baik yang bersifat publik seperti layanan penyimpanan komersial maupun privat yang dikelola institusi tertentu. Pergeseran ini membawa konsekuensi signifikan terhadap hukum pembuktian pidana, sebab sebagian besar aktivitas manusia termasuk aktivitas yang berpotensi menjadi tindak pidana kini meninggalkan jejak digital yang tersimpan bukan lagi pada perangkat milik pelaku atau korban, melainkan pada server milik penyelenggara sistem elektronik yang dapat berlokasi di berbagai negara.

Karakteristik *cloud storage* yang bersifat *virtualized*, terdistribusi, dan lintas yurisdiksi menimbulkan sejumlah persoalan hukum yang tidak sepenuhnya terjawab oleh kerangka hukum acara pidana konvensional. KUHAP disusun pada tahun 1981, jauh sebelum era internet dan komputasi awan berkembang, sehingga tidak memuat pengaturan eksplisit mengenai bukti elektronik, apalagi bukti yang tersimpan pada infrastruktur awan lintas negara. Pengakuan terhadap informasi dan dokumen elektronik sebagai alat bukti yang sah baru hadir melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang kemudian diubah dengan Undang-Undang Nomor 19 Tahun 2016, dan terakhir disesuaikan kembali melalui Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU ITE. Meskipun demikian, ketentuan tersebut masih bersifat umum dan belum menjawab kekhususan karakteristik data yang tersimpan pada *cloud storage*, seperti persoalan siapa yang menguasai secara hukum (*legal custody*) data tersebut, bagaimana proses akuisisi data dilakukan tanpa merusak integritasnya, serta bagaimana keotentikan data dapat dibuktikan ketika data tidak pernah "disentuh" secara fisik oleh penyidik.

Persoalan ini menjadi semakin kompleks ketika dikaitkan dengan penyedia layanan *cloud storage* yang berkedudukan di luar negeri, sehingga permintaan data oleh aparat penegak hukum Indonesia harus melalui mekanisme kerja sama hukum timbal balik (*mutual legal assistance*) yang memakan waktu, sementara sifat data digital yang mudah berubah dan mudah dihapus menuntut kecepatan penanganan. Di sisi lain, berlakunya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) turut memunculkan ketegangan normatif antara kebutuhan penegakan hukum untuk mengakses data pribadi yang tersimpan di awan dan hak subjek data atas pelindungan data pribadinya. Kondisi inilah yang melatarbelakangi urgensi untuk mengkaji secara mendalam sejauh mana kepastian hukum atas penggunaan bukti digital berbasis *cloud storage* dalam sistem pembuktian perkara pidana di Indonesia.

Sejumlah penelitian terdahulu telah mengkaji isu bukti digital dan pembuktian pidana di Indonesia, meskipun belum banyak yang secara spesifik menyasar karakteristik *cloud storage*. Marsilindo dkk. dalam kajiannya tentang penggunaan alat bukti digital dalam pembuktian tindak pidana siber menyimpulkan bahwa alat bukti digital telah memperoleh legitimasi normatif sebagai perluasan alat bukti yang sah, tetapi dalam praktiknya masih ditempatkan secara tidak konsisten dalam kategori alat bukti yang telah diatur KUHAP, sehingga penilaiannya sangat bergantung pada pemahaman teknologi informasi oleh hakim (Marsilindo dkk., 2024). Penelitian tersebut juga menyoroti pentingnya interaksi antara substansi hukum, struktur hukum, dan budaya hukum dalam menentukan efektivitas penggunaan bukti digital, merujuk pada teori sistem hukum Lawrence M. Friedman.

Adnan (2021) mengkaji kekuatan pembuktian bukti elektronik dalam sistem peradilan pidana Indonesia dan menemukan bahwa meskipun Pasal 5 UU ITE menegaskan informasi dan dokumen elektronik sebagai alat bukti yang sah, kekuatan pembuktiannya di persidangan masih sangat tergantung

pada keyakinan hakim karena belum ada parameter baku untuk menilai keaslian data elektronik. Sejalan dengan itu, Dewantoro (2024) menyoroti pentingnya autentikasi alat bukti elektronik dalam mempercepat proses pembuktian pada era disrupsi teknologi, dengan menekankan bahwa autentikasi menjadi titik krusial yang menentukan apakah data elektronik dapat diterima sebagai bukti yang meyakinkan.

Penelitian yang membahas dimensi lintas yurisdiksi juga mulai berkembang. Prayoga (2022) mengkaji tantangan hukum pembuktian lintas yurisdiksi dalam kasus *cyber-terrorism* dan menekankan bahwa perbedaan sistem hukum antarnegara serta lambannya mekanisme bantuan hukum timbal balik menjadi hambatan utama dalam memperoleh bukti digital yang berada di server luar negeri. Penelitian lain yang dilakukan pada perkara kejahatan siber juga menegaskan bahwa isu yurisdiksi merupakan salah satu tantangan utama pembuktian, di samping keterbatasan sumber daya dan kapasitas penegak hukum dalam melakukan forensik digital (Aini dkk., 2024).

Di ranah hukum perdata, penelitian tentang validitas bukti digital dalam sengketa perdata turut memberikan kontribusi konseptual yang relevan. Kajian mengenai validitas kekuatan hukum bukti digital dalam sengketa perdata menemukan bahwa validitas bukti digital ditentukan oleh integritas data, autentikasi sumber, dan keamanan penyimpanan, dengan menawarkan model penilaian yang mengadaptasi standar internasional forensik digital ke dalam kerangka hukum nasional (Greenpub, 2026). Penelitian mengenai pembuktian digital dalam sengketa perdata lain juga menyimpulkan perlunya amandemen menyeluruh terhadap hukum acara guna mengakomodasi validitas formil dan materiil dokumen elektronik (Ilham dkk., 2025).

Pada ranah forensik digital, Ashari dkk. (2025) memaparkan prinsip dan teknik digital forensik dalam era siber modern, sementara kajian mengenai penerapan prinsip *best practices* digital forensik menegaskan bahwa keabsahan alat bukti elektronik sangat ditentukan oleh kepatuhan terhadap prosedur forensik standar sejak tahap identifikasi, akuisisi, hingga presentasi bukti di persidangan (Fitria dkk., 2025).

Berbeda dari penelitian-penelitian terdahulu yang secara umum membahas bukti digital atau bukti elektronik dalam kerangka besar tindak pidana siber maupun sengketa perdata, penelitian ini secara khusus memfokuskan analisis pada karakteristik unik data yang tersimpan pada *cloud storage* yakni sifatnya yang tervirtualisasi, terdistribusi lintas server, dikuasai oleh penyelenggara sistem elektronik pihak ketiga, dan berpotensi lintas yurisdiksi. Kebaruan penelitian ini terletak pada tiga hal. Pertama, penelitian ini mengintegrasikan analisis atas tiga rezim hukum sekaligus, yaitu hukum acara pidana (KUHAP), hukum informasi dan transaksi elektronik (UU ITE beserta perubahannya, termasuk perubahan terbaru tahun 2024), dan hukum pelindungan data pribadi (UU PDP), untuk melihat titik temu maupun ketegangan normatif di antara ketiganya dalam konteks bukti digital berbasis awan. Kedua, penelitian ini menyoroti secara spesifik problem akuisisi dan otentikasi bukti dalam lingkungan awan yang belum banyak dikaji dalam literatur hukum Indonesia, berbeda dengan penelitian terdahulu yang umumnya membahas bukti elektronik secara generik tanpa membedakan lokasi penyimpanan data. Ketiga, penelitian ini memberikan analisis atas tantangan pembuktian lintas yurisdiksi yang dikaitkan langsung dengan praktik penyimpanan data di server luar negeri oleh penyedia layanan *cloud storage* global, sekaligus menawarkan arah penguatan regulasi yang lebih konkret.

Berdasarkan uraian latar belakang tersebut, penelitian ini berfokus pada tiga permasalahan utama, yaitu bagaimana kedudukan hukum bukti digital berbasis *cloud storage* dalam sistem pembuktian perkara pidana di Indonesia, bagaimana kepastian hukum mengenai keabsahan dan kekuatan pembuktian bukti digital yang disimpan pada *cloud storage*, serta apa saja tantangan yuridis dan praktis dalam penggunaan bukti digital berbasis *cloud storage* dalam pembuktian perkara pidana di Indonesia. Sejalan dengan

permasalahan tersebut, penelitian ini bertujuan untuk menganalisis kedudukan hukum bukti digital berbasis *cloud storage* dalam sistem pembuktian perkara pidana berdasarkan Kitab Undang-Undang Hukum Acara Pidana dan peraturan perundang-undangan terkait, mengkaji tingkat kepastian hukum atas keabsahan dan kekuatan pembuktian bukti digital yang tersimpan pada *cloud storage* ditinjau dari prinsip autentikasi dan integritas data, serta mengidentifikasi tantangan yuridis dan praktis dalam penggunaannya, termasuk persoalan yurisdiksi lintas negara, sekaligus merumuskan arah penguatan regulasi yang diperlukan.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif (*normative legal research*), yaitu penelitian yang mengkaji hukum sebagai norma tertulis (*law in books*) dengan menelaah asas-asas hukum, sistematika hukum, taraf sinkronisasi vertikal dan horizontal peraturan perundang-undangan, serta perbandingan hukum (Marzuki, 2021). Penelitian ini tidak dimaksudkan untuk menguji data lapangan (*law in action*), melainkan untuk menganalisis konsistensi dan kecukupan norma hukum positif dalam mengatur bukti digital berbasis *cloud storage* sebagai alat bukti dalam perkara pidana.

Pendekatan yang digunakan meliputi tiga jenis. Pertama, pendekatan perundang-undangan (*statute approach*), yaitu menelaah seluruh peraturan perundang-undangan yang berkaitan dengan pembuktian pidana dan informasi elektronik, meliputi Kitab Undang-Undang Hukum Acara Pidana (KUHAP), Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 dan Undang-Undang Nomor 1 Tahun 2024, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta peraturan pelaksana lain yang relevan. Kedua, pendekatan konseptual (*conceptual approach*), yang digunakan untuk mengkaji konsep bukti digital, integritas data, autentikasi, dan *chain of custody* sebagaimana berkembang dalam doktrin hukum pembuktian dan digital forensik. Ketiga, pendekatan kasus (*case approach*) secara terbatas, yang digunakan untuk melihat kecenderungan pertimbangan hukum pengadilan dalam menilai bukti elektronik pada perkara-perkara pidana yang telah dipublikasikan.

Bahan hukum yang digunakan terdiri atas tiga jenis. Bahan hukum primer berupa peraturan perundang-undangan sebagaimana disebutkan di atas. Bahan hukum sekunder berupa buku, jurnal ilmiah, dan hasil penelitian terdahulu yang membahas bukti digital, digital forensik, dan cyberlaw, baik yang diterbitkan di dalam maupun luar negeri. Bahan hukum tersier berupa kamus hukum dan bahan pendukung lain yang membantu memahami istilah teknis. Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*), dengan menelusuri peraturan perundang-undangan, jurnal hukum terakreditasi, dan literatur digital forensik yang relevan dalam kurun sepuluh tahun terakhir. Analisis dilakukan secara deskriptif-kualitatif dengan sifat preskriptif, yaitu tidak hanya menggambarkan norma yang berlaku, tetapi juga memberikan penilaian dan rekomendasi mengenai bagaimana seharusnya norma tersebut diatur untuk menjamin kepastian hukum.

HASIL DAN PEMBAHASAN

A. Konsep Bukti Digital dan *Cloud Storage* dalam Perkembangan Teknologi Informasi

Secara konseptual, bukti digital (*digital evidence*) dipahami sebagai informasi yang disimpan atau ditransmisikan dalam bentuk digital, yang memiliki nilai pembuktian karena dapat menunjukkan hubungan

antara suatu tindakan dengan akibat hukum tertentu (Al-Azhar, 2012). Berbeda dengan bukti fisik konvensional, bukti digital memiliki karakteristik yang khas: mudah digandakan tanpa kehilangan kualitas (*duplicable*), mudah diubah tanpa meninggalkan jejak kasatmata apabila tidak ditangani secara forensik (*volatile* dan *alterable*), serta dapat tersebar pada berbagai lokasi penyimpanan yang terpisah dari perangkat penggunanya. Karakteristik inilah yang membedakan pendekatan hukum terhadap bukti digital dari bukti konvensional yang diatur dalam Pasal 184 KUHAP.

Cloud storage merupakan salah satu bentuk layanan komputasi awan yang memungkinkan pengguna menyimpan data pada infrastruktur server yang dikelola oleh penyelenggara sistem elektronik, dan dapat diakses kapan saja melalui jaringan internet tanpa pengguna perlu mengetahui secara pasti lokasi fisik penyimpanan data tersebut. Karakteristik teknis ini yang dikenal dengan istilah *resource pooling*, *multi-tenancy*, dan *data replication* menyebabkan satu berkas data dapat disalin dan disimpan secara simultan pada beberapa server yang berlokasi di negara berbeda demi alasan efisiensi dan keandalan sistem. Implikasinya, ketika data tersebut hendak dijadikan alat bukti dalam perkara pidana, penyidik tidak lagi berhadapan dengan satu perangkat fisik yang dapat disita, melainkan berhadapan dengan data yang "tidak bertempat tinggal tetap" (Marsilindo dkk., 2024).

Dalam konteks hukum pidana, pergeseran ini memunculkan setidaknya tiga persoalan mendasar. Pertama, persoalan penguasaan hukum atas data (*legal control*), yaitu siapa pihak yang secara hukum dianggap menguasai data yang tersimpan di *cloud storage* apakah pengguna layanan (*data subject/controller*), ataukah penyelenggara sistem elektronik (*cloud service provider*) yang secara teknis mengendalikan infrastruktur penyimpanan. Kedua, persoalan akuisisi data tanpa merusak integritasnya, mengingat proses pengambilan data dari server awan berbeda secara teknis dari penyitaan barang bukti fisik yang diatur dalam Pasal 38–46 KUHAP. Ketiga, persoalan pembuktian keaslian (*authenticity*) data, karena data yang diperoleh dari *cloud storage* pada umumnya berupa salinan (*copy*) dan bukan data asli (*original*) sebagaimana lazim dipahami dalam hukum pembuktian konvensional.

B. Kedudukan Hukum Bukti Digital Berbasis *Cloud Storage* dalam Sistem Pembuktian Pidana di Indonesia

Sistem pembuktian pidana Indonesia menganut asas *numerus clausus*, yaitu alat bukti yang sah dibatasi secara limitatif sebagaimana diatur dalam Pasal 184 ayat (1) KUHAP, yang meliputi keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa. Ketentuan ini disusun pada masa ketika teknologi informasi belum berkembang, sehingga tidak secara eksplisit mengakomodasi data elektronik sebagai kategori alat bukti tersendiri. Kekosongan ini kemudian diisi oleh Pasal 5 UU ITE, yang menegaskan bahwa informasi elektronik dan/atau dokumen elektronik serta hasil cetaknya merupakan alat bukti hukum yang sah dan merupakan perluasan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia. Ketentuan ini diperkuat lagi dengan pengaturan dalam Pasal 5 ayat (4) UU ITE yang mengecualikan surat yang menurut undang-undang harus dibuat dalam bentuk tertulis dan surat beserta dokumennya yang menurut undang-undang harus dibuat dalam bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta.

Dengan demikian, secara normatif, bukti digital termasuk yang tersimpan pada *cloud storage* dapat dikategorikan sebagai perluasan alat bukti yang sah, sepanjang memenuhi syarat formil dan materiil yang ditentukan undang-undang. Dalam praktik peradilan, bukti digital yang berasal dari *cloud storage* biasanya dihadirkan bukan sebagai kategori mandiri, melainkan "ditarik" ke dalam salah satu kategori alat bukti dalam Pasal 184 KUHAP: sebagai alat bukti surat apabila berbentuk dokumen elektronik yang dicetak,

sebagai petunjuk apabila digunakan untuk membangun keyakinan hakim atas keterkaitan antarfakta, atau melalui keterangan ahli forensik digital yang menjelaskan proses dan hasil analisis data (Marsilindo dkk., 2024). Pola penempatan yang tidak seragam ini menunjukkan bahwa kedudukan bukti digital berbasis *cloud storage* dalam sistem hukum acara pidana masih bersifat adaptif dan bergantung pada penafsiran hakim kasus demi kasus, bukan hasil dari norma yang secara khusus dan tuntas mengatur karakteristik data awan.

Persoalan menjadi lebih kompleks ketika dikaitkan dengan tahap penyidikan. Pasal 38–41 KUHAP mengatur penggeledahan dan penyitaan yang berorientasi pada objek fisik yang dapat "digenggam" oleh penyidik, sementara data pada *cloud storage* tidak dapat disita secara fisik melainkan harus diakses secara jarak jauh (*remote access*) atau dimintakan kepada penyelenggara sistem elektronik yang menguasainya. UU ITE dan peraturan pelaksananya, termasuk Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, memang mengatur kewajiban penyelenggara sistem elektronik untuk memberikan akses guna kepentingan penegakan hukum, namun pengaturan tersebut masih bersifat umum dan belum merinci prosedur teknis akuisisi data awan secara forensik yang menjamin data tidak berubah selama proses pengambilan. Kekosongan pengaturan teknis inilah yang menjadi titik lemah kedudukan hukum bukti digital berbasis *cloud storage*, sebab keabsahan proses perolehan bukti (*lawfully obtained evidence*) merupakan prasyarat mutlak sebelum menilai kekuatan pembuktian substansinya.

C. Keabsahan, Autentikasi, Integritas, dan Kepastian Hukum Nilai Pembuktian Data pada *Cloud Storage*

Kepastian hukum, sebagaimana dikemukakan Gustav Radbruch, merupakan salah satu tujuan hukum di samping keadilan dan kemanfaatan, yang menuntut agar norma hukum dirumuskan secara jelas sehingga dapat diterapkan secara konsisten dan dapat diprediksi. Dalam konteks bukti digital berbasis *cloud storage*, kepastian hukum menuntut adanya parameter yang jelas mengenai tiga unsur utama: keabsahan cara memperoleh bukti, keaslian (*authenticity*) data, dan integritas data sejak diperoleh hingga dihadirkan di persidangan.

Pertama, dari aspek keabsahan cara memperoleh bukti, hukum acara pidana Indonesia menganut asas bahwa alat bukti yang diperoleh secara melawan hukum tidak dapat digunakan (*fruit of the poisonous tree doctrine*), meskipun asas ini tidak diatur secara eksplisit dalam KUHAP dan lebih banyak berkembang melalui doktrin dan yurisprudensi. Untuk bukti digital berbasis *cloud storage*, keabsahan cara memperoleh menjadi rumit karena proses akuisisi data pada umumnya dilakukan melalui permintaan kepada penyelenggara sistem elektronik atau melalui akses jarak jauh dengan bantuan ahli forensik digital, bukan melalui penggeledahan fisik sebagaimana diatur KUHAP. Ketiadaan pengaturan spesifik mengenai prosedur permintaan data awan termasuk siapa yang berwenang mengeluarkan perintah, bentuk dokumen permintaan, dan batas kewenangan akses menyebabkan praktik antarinstansi penegak hukum tidak seragam, sehingga rentan menimbulkan perdebatan mengenai keabsahannya di persidangan (Adnan, 2021).

Kedua, dari aspek keaslian (*authenticity*), data yang diperoleh dari *cloud storage* pada umumnya berbentuk salinan digital (*forensic image* atau *copy*), bukan data "asli" dalam pengertian fisik konvensional. Autentikasi data digital lazimnya dilakukan melalui teknik *hashing* (misalnya menggunakan algoritma MD5 atau SHA-256) untuk menghasilkan nilai unik yang dapat membuktikan bahwa salinan data identik dengan data sumber pada saat pengambilan dilakukan. Namun, hukum acara pidana Indonesia belum mengatur secara eksplisit kewajiban penggunaan metode autentikasi tertentu sebagai syarat formil keabsahan bukti digital, sehingga penerimaan hasil autentikasi forensik sepenuhnya bergantung pada keterangan ahli dan penilaian hakim (Dewantoro, 2024). Kekosongan ini menjadi krusial dalam konteks

cloud storage, mengingat data yang sama dapat disalin dan tersebar di berbagai server, sehingga pembuktian bahwa data yang dihadirkan di persidangan identik dengan data yang tersimpan pada akun tersangka/terdakwa pada waktu tertentu memerlukan metodologi forensik yang teruji, bukan semata keyakinan subjektif.

Ketiga, dari aspek integritas data, prinsip *chain of custody* menjadi elemen sentral untuk menjamin bahwa data tidak mengalami perubahan sejak diakuisisi hingga dihadirkan sebagai bukti. Pada bukti fisik, *chain of custody* relatif mudah didokumentasikan melalui berita acara penyitaan dan penyimpanan barang bukti. Namun pada data *cloud storage*, rantai penguasaan menjadi lebih panjang dan melibatkan lebih banyak pihak: penyelenggara sistem elektronik yang mengelola server, petugas forensik digital yang melakukan akuisisi, hingga penyidik yang menerima hasil akuisisi tersebut. Setiap titik peralihan penguasaan data berpotensi menimbulkan celah manipulasi apabila tidak didokumentasikan secara ketat. Penelitian mengenai penerapan prinsip *best practices* digital forensik menegaskan bahwa keabsahan alat bukti elektronik sangat ditentukan oleh kepatuhan terhadap standar forensik baku sejak tahap identifikasi, pengumpulan, akuisisi, hingga presentasi bukti (Fitria dkk., 2025), namun standar tersebut hingga kini masih berupa praktik baik (*best practices*) yang tidak dikodifikasi secara mengikat dalam peraturan perundang-undangan Indonesia.

Ketiadaan norma teknis yang mengikat atas ketiga unsur di atas menyebabkan kepastian hukum atas nilai pembuktian data *cloud storage* menjadi rentan. Nilai pembuktian suatu alat bukti pada akhirnya bergantung pada penilaian hakim berdasarkan keyakinannya (Pasal 183 KUHAP), namun tanpa parameter normatif yang jelas mengenai autentikasi dan integritas data awan, penilaian tersebut berpotensi tidak konsisten antara satu perkara dengan perkara lain, bahkan antara satu majelis hakim dengan majelis lainnya. Kondisi ini bertentangan dengan tujuan kepastian hukum yang menuntut prediktabilitas penerapan norma.

Persoalan lain yang memengaruhi kepastian hukum adalah ketegangan normatif antara kebutuhan penegakan hukum untuk mengakses data pada *cloud storage* dan hak pelindungan data pribadi sebagaimana diatur dalam UU PDP. UU PDP mengatur bahwa pemrosesan data pribadi harus didasarkan pada dasar pemrosesan yang sah, termasuk untuk pelaksanaan kewajiban hukum dan kepentingan penegakan hukum, namun tetap mensyaratkan prinsip pembatasan tujuan dan keamanan data. Ketika penyidik meminta akses data dari *cloud storage* yang di dalamnya turut tersimpan data pribadi pihak lain yang tidak terkait dengan perkara, UU PDP menuntut agar akses tersebut dibatasi secara proporsional. Namun, mekanisme teknis untuk memastikan proporsionalitas tersebut misalnya melalui prosedur *minimisasi data* dalam proses akuisisi forensik digital belum diatur secara rinci dalam hukum acara pidana maupun peraturan pelaksana UU ITE, sehingga berpotensi menimbulkan tumpang tindih norma antara kepentingan pembuktian pidana dan hak atas pelindungan data pribadi.

4. Tantangan Yuridis dan Praktis: Yurisdiksi Lintas Batas dan Kebutuhan Penguatan Regulasi

Tantangan paling signifikan dalam penggunaan bukti digital berbasis *cloud storage* adalah persoalan yurisdiksi. Banyak penyedia layanan *cloud storage* besar berkedudukan hukum atau menempatkan server utamanya di luar negeri, sehingga permintaan akses data oleh penegak hukum Indonesia terhadap data yang berkaitan dengan perkara pidana domestik seringkali harus melalui mekanisme bantuan hukum timbal balik (*Mutual Legal Assistance*/MLA) yang diatur dalam Undang-Undang Nomor 1 Tahun 2006 tentang Bantuan Timbal Balik dalam Masalah Pidana. Mekanisme MLA yang formal dan berjenjang ini pada praktiknya memakan waktu yang tidak sebanding dengan sifat data digital yang mudah berubah atau dihapus, sehingga berisiko kehilangan bukti sebelum permintaan MLA

diproses secara tuntas. Prayoga (2022) menegaskan bahwa perbedaan sistem hukum antarnegara serta lambannya mekanisme kerja sama hukum menjadi hambatan struktural utama dalam memperoleh bukti digital lintas yurisdiksi, khususnya dalam perkara-perkara yang menuntut kecepatan penanganan seperti kejahatan siber transnasional dan terorisme berbasis dunia maya.

Tantangan yurisdiksi ini diperparah oleh belum adanya keikutsertaan Indonesia dalam kerangka kerja sama internasional yang secara spesifik mengatur akses lintas batas terhadap bukti elektronik, seperti Konvensi Budapest tentang Kejahatan Siber (*Budapest Convention on Cybercrime*) yang telah diratifikasi banyak negara namun belum diikuti Indonesia. Tanpa kerangka kerja sama multilateral yang mengikat, permintaan data lintas negara sangat bergantung pada itikad baik penyedia layanan dan kesediaan otoritas negara tempat server berada untuk bekerja sama, yang pada gilirannya menimbulkan ketidakpastian mengenai berapa lama proses tersebut akan berlangsung dan apakah data akan tetap tersedia hingga proses tersebut selesai (Casey, 2021).

Tantangan berikutnya bersifat praktis-institusional, yaitu kesenjangan kapasitas sumber daya manusia dan infrastruktur forensik digital di lingkungan penegak hukum. Studi mengenai eksaminasi bukti digital dalam kasus kejahatan siber menunjukkan bahwa meskipun secara normatif bukti digital telah diakui melalui UU ITE, implementasinya masih menghadapi kendala keterbatasan sumber daya manusia yang terlatih dalam forensik digital, keterbatasan infrastruktur laboratorium forensik, serta belum harmonisnya regulasi lintas batas (Joecy, 2024). Keterbatasan ini menyebabkan proses akuisisi data *cloud storage* seringkali dilakukan tanpa mengikuti standar forensik yang memadai, sehingga meningkatkan risiko bukti ditolak atau dipertanyakan keabsahannya di persidangan.

Tantangan lain yang bersifat yuridis murni adalah belum adanya pengaturan yang jelas mengenai kewenangan penyidik untuk melakukan *remote forensic access* terhadap data yang tersimpan di server yang berada di luar wilayah hukum Indonesia, termasuk batasan-batasan yang harus dipatuhi agar tindakan tersebut tidak melanggar kedaulatan hukum negara lain. Praktik akses data lintas batas tanpa kerangka hukum yang jelas berpotensi menimbulkan persoalan legalitas alat bukti itu sendiri, sebab cara memperoleh bukti yang melanggar hukum negara lain berpotensi dikualifikasi sebagai cara memperoleh bukti yang melawan hukum, meskipun tujuannya untuk kepentingan penegakan hukum domestik.

Menghadapi berbagai tantangan tersebut, penguatan regulasi menjadi kebutuhan mendesak. Pertama, diperlukan pengaturan teknis yang lebih rinci mengenai prosedur akuisisi bukti digital dari *cloud storage*, termasuk standar minimal metode *hashing* dan dokumentasi *chain of custody* digital, yang dapat dituangkan dalam peraturan pelaksana UU ITE maupun pedoman teknis internal Kepolisian dan Kejaksaan. Kedua, diperlukan harmonisasi antara hukum acara pidana dan UU PDP melalui pengaturan mekanisme akses data pribadi untuk kepentingan penegakan hukum yang tetap menghormati prinsip proporsionalitas dan minimisasi data. Ketiga, diperlukan penguatan kerja sama hukum internasional, baik melalui perjanjian bilateral maupun melalui pertimbangan aksesi terhadap kerangka kerja sama multilateral mengenai bukti elektronik lintas batas, guna mempercepat proses permintaan data kepada penyedia layanan *cloud storage* asing. Keempat, diperlukan peningkatan kapasitas kelembagaan, baik dari sisi sumber daya manusia forensik digital maupun infrastruktur laboratorium forensik, sebagai prasyarat teknis bagi terwujudnya kepastian hukum yang bukan hanya bersifat normatif di atas kertas, tetapi juga dapat diimplementasikan secara konsisten dalam praktik peradilan.

KESIMPULAN

Berdasarkan analisis di atas, dapat disimpulkan tiga hal pokok. Pertama, kedudukan hukum bukti digital berbasis *cloud storage* dalam sistem pembuktian pidana Indonesia pada dasarnya telah memperoleh pengakuan normatif melalui Pasal 5 UU ITE sebagai perluasan alat bukti yang sah, namun penempatannya ke dalam kategori alat bukti Pasal 184 KUHAP masih bersifat adaptif dan tidak seragam, sebagai akibat dari KUHAP yang belum mengatur secara khusus karakteristik data yang tersimpan pada infrastruktur awan. Kedua, kepastian hukum atas keabsahan dan kekuatan pembuktian bukti digital berbasis *cloud storage* masih rapuh karena hukum acara pidana belum mengatur secara rinci prosedur akuisisi data, standar autentikasi (termasuk metode *hashing*), maupun mekanisme *chain of custody* digital yang mengikat, sehingga penilaian keabsahan dan kekuatan pembuktian sangat bergantung pada keterangan ahli dan keyakinan hakim kasus demi kasus, belum pada parameter normatif yang pasti dan dapat diprediksi. Ketiga, tantangan yuridis dan praktis yang dihadapi meliputi persoalan yurisdiksi lintas batas akibat lokasi server penyedia layanan *cloud storage* yang umumnya berada di luar negeri, lambannya mekanisme bantuan hukum timbal balik, ketiadaan keikutsertaan Indonesia dalam kerangka kerja sama internasional mengenai bukti elektronik lintas batas, ketegangan normatif dengan UU PDP, serta keterbatasan kapasitas sumber daya manusia dan infrastruktur forensik digital di lingkungan penegak hukum.

Untuk menjamin kepastian hukum yang lebih kokoh, penelitian ini merekomendasikan agar pembentuk undang-undang dan pemangku kepentingan terkait segera merumuskan pengaturan teknis yang lebih rinci mengenai akuisisi dan autentikasi bukti digital berbasis *cloud storage*, baik melalui revisi hukum acara pidana maupun peraturan pelaksana UU ITE, disertai harmonisasi dengan UU PDP dan penguatan kerja sama hukum internasional. Penelitian lanjutan diperlukan untuk mengkaji secara lebih mendalam model regulasi teknis akuisisi bukti awan yang paling sesuai dengan kondisi kelembagaan penegak hukum Indonesia, termasuk kemungkinan pembentukan pedoman teknis nasional mengenai forensik awan (*cloud forensics*) yang mengikat secara hukum.

DAFTAR PUSTAKA

Adnan, N. F. (2021). Kekuatan pembuktian bukti elektronik dalam sistem peradilan pidana Indonesia. *Jurnal Hukum Pidana dan Kriminologi, 4*(1).

Aini, N., et al. (2024). Tantangan pembuktian dalam kasus kejahatan siber di Indonesia. *Judge: Jurnal Hukum, 5*.

Al-Azhar, M. N. (2012). *Digital forensics: Panduan praktis investigasi komputer*. Elex Media Komputindo.

Ashari, I. F., et al. (2025). *Digital forensik: Prinsip, teknik, dan implementasi dalam era siber modern*. Yayasan Kita Menulis.

Budhijanto, D. (2024). *Revolusi cyberlaw Indonesia: Revisi UU ITE 2024*. Refika Aditama.

Casey, E. (2021). The challenge of cross-border access to electronic evidence. *Digital Investigation, 38*, Article 101186. https://doi.org/10.1016/j.diin.2021.101186

Chazawi, A. (2014). *Pelajaran hukum pidana: Bagian 1*. Rajawali Pers.

Dewantoro, D. (2024). Autentikasi alat bukti elektronik dalam memperlancar pembuktian di persidangan pada era disrupsi. *Jurnal Hukum Progresif, 12*(2), 135–151.

Fitria, S. D., et al. (2025). Analisis yuridis penerapan prinsip *best practices digital forensics* dalam menjamin keabsahan alat bukti elektronik di Indonesia. *Collegium Studiosum Journal, 8*(2).

Gulo, A. S., Lasmadi, S., & Nawawi, K. (2021). Cyber crime dalam bentuk phishing berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *PAMPAS: Journal of Criminal Law, 2*(1).

Hiariej, E. O. S. (2012). *Teori dan hukum pembuktian*. Erlangga.

Indonesia. (1981). *Undang-Undang Nomor 8 Tahun 1981 tentang Kitab Undang-Undang Hukum Acara Pidana*.

Indonesia. (2006). *Undang-Undang Nomor 1 Tahun 2006 tentang Bantuan Timbal Balik dalam Masalah Pidana*.

Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.

Indonesia. (2016). *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.

Indonesia. (2019). *Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik*.

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

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

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

Mansur, D. M. A., & Gultom, E. (2018). *Cyber law: Aspek hukum teknologi informasi*. Refika Aditama.

Marsilindo, et al. (2024). Penggunaan alat bukti digital dalam pembuktian tindak pidana siber di pengadilan Indonesia. *Judge: Jurnal Hukum, 6*(1).

Marzuki, P. M. (2021). *Penelitian hukum* (Edisi revisi). Kencana.

Pratama, B., & Sulistyanti, R. (2021). The admissibility of electronic evidence in Indonesian civil courts: Current issues and future perspectives. *Digital Evidence and Electronic Signature Law Review, 18*, 55–70.

Prayoga, A. S. (2022). Tantangan hukum pembuktian lintas yurisdiksi dalam kasus *cyber-terrorism*. *Jurnal Hukum Internasional, 15*(1).

Putri, A. R., & Santoso, S. (2021). Implementasi digital forensic dalam pembuktian tindak pidana siber di Indonesia. *Jurnal Teknologi dan Sistem Informasi, 7*(3), 241–258. https://doi.org/10.25077/teknosi.v7i3.2021.241-258

Rahmawati, et al. (2026). Validitas kekuatan hukum bukti digital dalam pembentukan sengketa perdata di era digital. *Jurnal Ilmu Multidisiplin, 4*(2).

Suhariyanto, B. (2013). *Tindak pidana teknologi informasi (Cybercrime): Urgensi pengaturan dan celah hukumnya*. Rajawali Pers.

Tim Peneliti. (2024). Eksaminasi terhadap bukti digital dalam kasus kejahatan siber. *Journal of Education and Cyber Law (JOECY), 3*(1).