Socius: Jurnal Penelitian Ilmu-Ilmu Sosial
Volume 3, Issue 10, May 2026, P 529-540
E-ISSN: 3025-6704
DOI: https://doi.org/10.5281/zenodo.21899580

Penetapan Tersangka dalam Perkara Pidana Digital Marketing: Analisis Praperadilan dan Kecukupan Dua Alat Bukti

Determination of Suspects in Digital Marketing Criminal Cases: An Analysis of Pretrial Proceedings and the Sufficiency of Two Pieces of Evidence

Muhamad Jamalih[1], Sarip Hidayat[2], Rahayudin[3]
[1-3]Universitas Sehati Indonesia, Indonesia

ARTICLE INFO
Riwayat artikel:
Received 20 May 2026
Revised 25 May 2026
Accepted 30 May 2026
Available online 15 June 2026

Keywords
Pretrial Hearings
Electronic Evidence
Digital Marketing
Chain of Custody
Due Process of Law

ABSTRACT
The evolution of the global economy toward algorithmic commercial ecosystems has facilitated the mutation of white-collar crime into the cyber dimension, particularly in highly volatile and borderless digital marketing sectors. Within the Indonesian criminal justice system, this technological reality triggers severe normative friction during pretrial hearings (praperadilan), where law enforcement agencies and judges often impose conventional paradigms by validating uncertified screenshots or physical printouts to satisfy the quantitative requirement of "two pieces of evidence" for designating a suspect. Existing legal scholarship predominantly focuses on the technical efficacy of digital forensics at the final adjudication stage, leaving a systemic dogmatic void regarding the intersection of formal criminal procedure and digital evidence governance during the critical phase of suspect determination. This research aims to critically analyze the ratio decidendi of pretrial judges in validating electronic evidence and to construct a framework for integrating global forensic standards into domestic judicial parameters. The doctrinal analysis reveals that reducing electronic evidence to physical printouts without a forensic audit trail constitutes an acute dogmatic flaw that fundamentally violates the due process of law and the mandate of Constitutional Court Decision Number 21/PUU-XII/2014. The novelty of this study manifests in the conceptualization of a hybrid evidentiary parameter that operationally marries the formal requirements of the Criminal Procedure Code (KUHAP) with global material forensic standards, specifically the ISO/IEC 27037 guidelines

ABSTRAK
Evolusi ekonomi global menuju ekosistem komersial berbasis algoritma telah memfasilitasi mutasi kejahatan kerah putih ke dimensi siber, khususnya pada sektor pemasaran digital (*digital marketing*) yang bersifat *volatile* dan nirbatas. Dalam sistem peradilan pidana Indonesia, realitas teknologis ini memicu ketegangan norma yang ekstrem pada fase praperadilan, di mana aparat penegak hukum dan hakim kerap memaksakan paradigma konvensional dengan mengesahkan penetapan tersangka hanya bermodalkan tangkapan layar (*print-out*) tak tersertifikasi guna memenuhi syarat kuantitatif "dua alat bukti". Literatur terdahulu mayoritas terfokus pada efikasi teknis forensik di tahap ajudikasi akhir, sehingga menyisakan kekosongan kajian sistematis mengenai irisan dogmatik antara hukum acara formil dan standar tata kelola pembuktian digital pada fase paling krusial, yakni penetapan tersangka. Penelitian ini bertujuan untuk menganalisis secara kritis *rasio decidendi* hakim praperadilan dalam memvalidasi alat bukti elektronik dan mengonstruksikan integrasi standar forensik global ke dalam parameter yudisial domestik. Hasil analisis menunjukkan bahwa reduksi pembuktian elektronik ke dalam selembar kertas tanpa jejak audit forensik merupakan kecacatan dogmatik yang secara fundamental melanggar prinsip *due process of law* dan Putusan Mahkamah Konstitusi Nomor 21/PUU-XII/2014. Kebaruan penelitian ini termanifestasi dalam konseptualisasi parameter pembuktian hibrida yang secara operasional mengawinkan syarat formil KUHAP dengan standar materiil forensik digital global (pedoman ISO/IEC 27037).

PENDAHULUAN

Evolusi arsitektur ekonomi global pada dekade ketiga abad ke-21 telah didominasi oleh penetrasi teknologi digital yang mendisrupsi model transaksi konvensional menuju ekosistem komersial berbasis algoritma. Transformasi ini melahirkan fenomena *digital marketing* (pemasaran digital) sebagai tulang punggung ekonomi modern yang beroperasi melalui

*Corresponding Author e-mail: muhammad.jamalih@gmail.com

manipulasi mahadata (*big data*), penargetan perilaku (*behavioral targeting*), dan otomatisasi kecerdasan buatan (*Artificial Intelligence*). Bersamaan dengan efisiensi pasar yang ditawarkan, ekosistem ini secara inheren memfasilitasi mutasi kejahatan kerah putih (*white-collar crime*) ke dalam dimensi siber. Tindak pidana yang bertaut dengan pemasaran digital seperti penipuan terafiliasi (*affiliate fraud*), rekayasa lalu lintas data melalui *click farm*, penyalahgunaan kredensial konsumen untuk manipulasi pasar, hingga pencurian kekayaan intelektual algoritmik memiliki karakteristik yang nirbatas (*borderless*), anonim, dan sepenuhnya bergantung pada jejak elektronik yang bersifat volatile (Franssen & Tosza, 2025). Pergeseran tipologi kejahatan ini memicu ketegangan norma (*clash of norms*) yang esensial di dalam sistem peradilan pidana, khususnya pada fase pra-ajudikasi. Aparatur penegak hukum yang masih beroperasi di bawah paradigma hukum acara pidana peninggalan abad ke-20 dihadapkan pada realitas teknologis abad ke-21, di mana bukti fisik (*tangible evidence*) telah disubstitusi secara absolut oleh metadata, log server, dan kode biner komputasi awan (*cloud computing*) (Abdullah et al., 2025).

Ketegangan norma hukum ini mencapai titik kulminasi diskursif ketika dihadapkan pada mandat konstitusional perlindungan hak asasi manusia melalui pranata praperadilan di Indonesia. Signifikansi diskursus ini dipicu oleh terbitnya Putusan Mahkamah Konstitusi (MK) Nomor 21/PUU-XII/2014, yang secara fundamental merombak lanskap hukum acara pidana dengan memperluas objek praperadilan untuk mencakup keabsahan "penetapan tersangka" (MKRI, 2014). Putusan yurisprudensial tersebut mewajibkan bahwa tindakan penetapan tersangka hanya sah apabila didasarkan pada minimal dua alat bukti yang sah sebagaimana diatur dalam Pasal 184 Kitab Undang-Undang Hukum Acara Pidana (KUHAP), diiringi dengan pemeriksaan calon tersangka. Namun, penerapan standar "dua alat bukti" ini menemui kebuntuan empiris dan teoretis ketika diterapkan secara spesifik pada perkara pidana *digital marketing*. Hakim praperadilan di tingkat Pengadilan Negeri dituntut untuk menilai kecukupan dan keabsahan alat bukti elektronik tanpa ditopang oleh parameter teknis-yuridis yang kohesif dalam regulasi hukum acara pidana nasional. Kekosongan hukum operasional mengenai tata cara pengujian keabsahan formil dan materiil atas alat bukti elektronik di fase praperadilan menyebabkan disparitas putusan hakim yang sangat tajam (Santosa & Kamali, 2022). Sebagian hakim mengambil posisi konservatif dengan menolak alat bukti berupa tangkapan layar (*screenshot*) atau log data yang tidak tersertifikasi, sementara sebagian lainnya terjebak pada bias "data fundamentalism" sebuah asumsi keliru yang menganggap seluruh luaran perangkat digital secara otomatis objektif dan sah, tanpa menilik integritas rantai pasok bukti (*chain of custody*) atau potensi manipulasi yang mendasarinya (Anggraeniko et al., 2026).

Untuk memetakan kompleksitas permasalahan ini secara utuh, kajian atas literatur terdahulu (*state of the art*) menunjukkan adanya polarisasi dan evolusi pandangan di antara para sarjana mengenai alat bukti digital dan pertanggungjawaban siber. Kelompok pemikiran pertama berfokus pada implikasi pertanggungjawaban teknologi otonom. Buiten et al. (2023) dan Ismaeel et al. (2026) menganalisis kewajiban hukum pada sistem kecerdasan buatan, menegaskan bahwa otonomi dan sifat *black-box* dari algoritma menyulitkan kerangka kausalitas tradisional, sehingga menuntut atribusi tanggung jawab yang didasarkan pada audit teknis yang presisi. Kelompok pemikiran kedua menitikberatkan pada validitas alat ukur forensik dalam hukum pembuktian. Ismail & Ariffin (2025) dan Abeysekera (2026) secara empiris memvalidasi penggunaan alat forensik sumber terbuka (*open-source*) dalam investigasi siber, menyimpulkan bahwa keabsahan hukum (*legal admissibility*) dari bukti digital sangat bergantung pada pemenuhan Standar Daubert khususnya kemampuan untuk mempertahankan nilai *hash* (seperti MD5 dan SHA1) guna membuktikan bahwa data tidak mengalami perusakan (*tampering*). Di ranah tata kelola investigasi global, kelompok pemikiran ketiga, yang direpresentasikan oleh Faizal & Luthfi (2024), mengonstruksikan kewajiban adopsi standar internasional ISO/IEC 27037 dalam mengidentifikasi, mengakuisisi, dan memelihara bukti digital oleh penanggap pertama (*first responders*) guna menjamin diterimanya bukti tersebut di muka pengadilan. Sementara itu, dalam konteks doktrin peradilan pidana, Westlund et al. (2025) memberikan peringatan kritis bahwa digitalisasi keadilan pidana tanpa pengawasan yudisial (*judicial oversight*) yang ketat akan mereduksi hak privasi dan memfasilitasi otoritarianisme teknologis. Pada lanskap domestik, kajian dari Jondong (2020) dan Siregar et al. (2026) secara konsisten mengeluhkan

ketertinggalan regulasi hukum acara dalam merespons volatilitas bukti elektronik, yang berujung pada disparitas dan inkonsistensi putusan praperadilan dalam menilai kecukupan bukti di tahap awal penyidikan.

Sintesis tematik atas literatur-literatur mutakhir tersebut mengidentifikasi sebuah kesenjangan penelitian (*gap analysis*) dan "titik buta" (*blind spot*) yang sangat fundamental. Mayoritas kajian terdahulu memusatkan lokus analisisnya pada pembuktian elektronik di fase ajudikasi (persidangan pokok perkara) atau murni berkutat pada perdebatan teknis efikasi perangkat lunak forensik digital, tanpa mendialogkannya dengan kerangka restriktif hukum acara pidana formil. Sangat minim literatur yang secara sistematis membedah irisan dogmatik antara hukum acara pidana, standar tata kelola forensik digital internasional, dan fenomena kejahatan algoritmik pemasaran digital pada fase yang paling krusial: fase penetapan tersangka di sidang praperadilan. Ketiadaan instrumen penguji (*testing mechanism*) yang terstandardisasi bagi hakim tunggal praperadilan dalam memvalidasi "dua alat bukti elektronik" memicu kekosongan hukum yang destruktif, di mana penetapan tersangka dapat dilegitimasi melalui perolehan bukti digital yang cacat secara melawan hukum (*unlawful legal evidence*), atau sebaliknya, penjahat siber terbebas dari jerat hukum akibat kelemahan literasi forensik aparat peradilan.

Berbeda dengan penelitian-penelitian sebelumnya yang mayoritas berfokus pada analisis teknis forensik di tingkat pembuktian pengadilan akhir atau kajian disparitas putusan pada tindak pidana konvensional semata, penelitian ini menawarkan pendekatan baru dengan mengintegrasikan standar tata kelola bukti digital internasional (khususnya pedoman ISO/IEC 27037 dan rantai pasok bukti atau *chain of custody*) sebagai pisau bedah hermeneutis bagi hakim praperadilan dalam mengukur dan menilai kecukupan konstitusional minimal dua alat bukti pada tindak pidana *digital marketing*. Kebaruan (*novelty*) dari naskah ini termanifestasi dalam konseptualisasi parameter *due process of law* yang bersifat hibrida yang secara operasional mengawinkan syarat formil pembuktian dalam KUHAP dan UU ITE dengan standar materiil-teknis forensik digital global sebagai filter yudisial independen di dalam institusi praperadilan.

Melalui konstruksi analisis yang holistik, dunia akademis dan praktisi penegak hukum didesak untuk mendekonstruksi dan merekonseptualisasi doktrin pembuktian pra-ajudikasi di era digital. Argumen utama (*thesis statement*) yang dipertahankan dalam artikel ini adalah bahwa kecukupan dan keabsahan "dua alat bukti" dalam penetapan tersangka perkara *digital marketing* tidak dapat dan tidak boleh diukur murni secara kuantitatif berdasarkan definisi konvensional Pasal 244 dan 245 KUHAP, melainkan mutlak harus diuji secara kualitatif berdasarkan jaminan integritas (*integrity*), keaslian (*authenticity*), dan prosedur perolehan yang sah melalui protokol forensik digital yang berstandar internasional. Temuan ini secara mendasar membedakan dirinya dari diskursus hukum pidana tradisional dengan meletakkan beban pembuktian otentikasi data di tahap pra-ajudikasi. Sebagai penutup dari pilar konseptual ini, solusi yang ditawarkan adalah pelembagaan doktrin *Exclusionary Rule* di dalam sidang praperadilan, di mana hakim berwenang secara mutlak untuk membatalkan penetapan tersangka apabila alat bukti elektronik yang diajukan oleh penyidik terbukti tidak dilampiri dengan dokumentasi log *chain of custody* dan validasi nilai *hash* forensik yang memadai, sehingga memastikan perlindungan hak asasi manusia terbebas dari kriminalisasi yang prematur dan artifisial.

Berdasarkan latar belakang dan kerangka pemikiran yang telah diuraikan, diskursus yuridis dalam naskah ini akan dikonstruksikan dan dianalisis secara komprehensif melalui dua rumusan masalah berikut: (1) Bagaimana analisis kritis terhadap rasio decidendi hakim praperadilan dalam mengkonstruksikan, memvalidasi, dan menilai kecukupan minimal dua alat bukti elektronik pada fase penetapan tersangka tindak pidana *digital marketing* ditinjau dari prinsip *due process of law*. (2) Bagaimana standar keandalan forensik digital global (khususnya kerangka ISO/IEC 27037 dan mekanisme dokumentasi *chain of custody*) dapat diintegrasikan dan dielevasi menjadi parameter yudisial normatif yang mengikat dalam pengujian keabsahan perolehan alat bukti di lembaga praperadilan Indonesia.

METODE PENELITIAN

Desain penelitian ini mengimplementasikan metode penelitian hukum normatif (doktrinal) murni yang diformulasikan secara analitis dan operasional untuk memecahkan problematika kekosongan aturan dan ketegangan norma pembuktian elektronik. Pemilihan metode normatif ini didasarkan pada justifikasi bahwa akar persoalan utama yang dikaji tidak terletak pada seberapa sering kejahatan *digital marketing* terjadi secara empiris, melainkan pada kelemahan konstruksi yuridis, ambiguitas penafsiran teks undang-undang, serta kegagalan harmonisasi antara norma hukum acara pidana nasional dengan standar prosedural pembuktian saintifik global (Hutchinson, 2025).

Terdapat empat pendekatan utama yang dioperasionalkan secara sinergis dalam penelitian ini. *Pertama*, pendekatan perundang-undangan (*statute approach*) yang digunakan untuk membedah anatomi regulasi pembuktian dalam KUHAP, UU Nomor 11 Tahun 2008 jo. UU Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (ITE), dan regulasi pendukung lainnya. *Kedua*, pendekatan konseptual (*conceptual approach*) yang dioperasikan untuk menelusuri doktrin-doktrin hukum seperti *due process of law*, *exclusionary rule*, dan epistemologi bukti digital. *Ketiga*, pendekatan kasus (*case approach*) yang diterapkan melalui analisis kritis terhadap rasio decidendi dalam Putusan Mahkamah Konstitusi (khususnya Putusan Nomor 21/PUU-XII/2014 dan Putusan Nomor 20/PUU-XIV/2016) serta putusan-putusan pengadilan negeri pada tingkat praperadilan yang mengadili keabsahan penetapan tersangka. *Keempat*, pendekatan perbandingan proporsional (*comparative approach*) yang difungsikan untuk membenturkan standar hukum acara domestik dengan kerangka tata kelola global, termasuk regulasi *E-Evidence* Uni Eropa, parameter Federal Rules of Evidence (FRE) Amerika Serikat, dan standar ISO/IEC.

Sumber bahan hukum bertumpu pada kualifikasi primer dan sekunder yang diseleksi berdasarkan relevansi dan otoritasnya. Bahan hukum primer terdiri atas peraturan perundang-undangan yang bersifat otoritatif mengikat, yurisprudensi Mahkamah Konstitusi, putusan hakim praperadilan, serta standar teknis internasional yang telah diratifikasi atau diakui sebagai *best practices*, seperti ISO/IEC 27037:2012 mengenai pedoman penanganan bukti digital. Bahan hukum sekunder diekstraksi dari literatur primer berkualitas tinggi, meliputi artikel jurnal internasional bereputasi, risalah akademik, dan doktrin para sarjana hukum terkemuka yang terbit dalam lima tahun terakhir untuk menjaga kebaruan analisis.

Teknik pengumpulan bahan hukum dilaksanakan melalui metode studi kepustakaan (*library research*) yang mendalam, didukung oleh penelusuran digital pada pangkalan data hukum (*legal database*) dan *digital library* terindeks. Teknik analisis hukum dioperasionalkan menggunakan silogisme deduktif dan hermeneutika hukum. Teori pembuktian, prinsip perlindungan HAM, dan standar forensik ditempatkan sebagai premis mayor (aturan umum), sedangkan fakta hukum mengenai tata cara penyidik dalam menetapkan tersangka berbekal bukti elektronik tak tersertifikasi diletakkan sebagai premis minor. Keduanya kemudian didialogkan melalui metode penafsiran hukum (interpretasi gramatikal, sistematis, dan teleologis/sosiologis) untuk mengidentifikasi kesalahan logika penalaran penegak hukum dan merumuskan argumentasi preskriptif yang menjamin kepastian hukum serta keadilan substansial di ranah praperadilan pidana siber.

HASIL DAN PEMBAHASAN

Karakteristik Kejahatan *Digital Marketing* dan Dekonstruksi Paradigma Kuantifikasi Alat Bukti

Untuk dapat menguraikan akar permasalahan disparitas peradilan terkait bukti digital, fondasi analisis harus dimulai dengan mendekonstruksi anatomi tindak pidana *digital marketing* itu sendiri, serta mengapa karakteristiknya berbenturan keras dengan paradigma pembuktian klasik peninggalan abad ke-20. Praktik pemasaran digital modern mengandalkan interaksi yang sangat cepat antara peladen (*server*), antarmuka pemrograman aplikasi (API), dan perangkat pengguna akhir (*end-user*). Kejahatan di ekosistem ini seperti manipulasi *click-through rate* (CTR) secara massal oleh *bot* komputer untuk merugikan kompetitor bisnis, penipuan pembagian hasil afiliasi pemasaran melalui pemalsuan *IP address*, atau penipuan iklan algoritmik (*programmatic*

ad fraud) beroperasi pada level struktur kode yang tidak terlihat oleh mata telanjang. Karakteristik utama dari modus operandi ini adalah lokusnya yang berada dalam komputasi awan (*cloud storage*), sifat anonimitasnya, dan wujud alat buktinya yang imateriel serta rentan terhadap perubahan mendadak (*volatility*) (Franssen & Tosza, 2025). Temuan atas volatilitas ini secara langsung memvalidasi sekaligus mengonfirmasi kegelisahan akademik dalam lanskap domestik yang sebelumnya telah disuarakan oleh Jondong (2020) dan Siregar et al. (2026), di mana ketertinggalan regulasi hukum acara nasional dalam merespons sifat *volatile* dari bukti elektronik telah menjadi episentrum dari disparitas putusan praperadilan. Hal ini terjadi karena bukti digital pada hakikatnya tidak sekadar memuat data isi (*content data*), melainkan secara imperatif mengandung metadata yakni data mengenai data, seperti stempel waktu (*timestamp*), geolokasi, log akses pengguna, dan riwayat revisi sistem yang justru menjadi kunci utama otentikasi (Miller, 2023).

Secara normatif, paradigma pembuktian hukum acara pidana Indonesia sejatinya kini sedang bertransformasi secara fundamental melalui KUHAP Baru (UU No. 20 Tahun 2025). Sistem pembuktian berpindah dari model tertutup yang kaku menjadi sistem pembuktian modern yang terbuka dan fleksibel (*vrije bewijsstelsels*). Ketentuan dasar pemidanaan yang dikodifikasikan dalam Pasal 244 ayat (1) KUHAP Baru tetap melarang hakim menjatuhkan pidana tanpa adanya keyakinan yang didukung oleh minimal dua alat bukti sah. Akan tetapi, Pasal 235 ayat (1) KUHAP Baru telah mendobrak batasan fisik dan lisan masa lalu dengan memperluas kategori alat bukti secara non-limitatif menjadi delapan jenis. Selain mengakomodasi dimensi klasik seperti keterangan saksi, ahli, surat, dan keterangan terdakwa, KUHAP Baru secara otonom mengesahkan barang bukti, bukti elektronik, pengamatan hakim, hingga kategori terbuka berupa "segala sesuatu yang dapat digunakan untuk kepentingan pembuktian" sepanjang diperoleh secara sah (KUHAP, 2025). Ekspansi normatif ini juga didelegasikan melalui Pasal 5 UU ITE (2024), yang melegitimasi Informasi dan Dokumen Elektronik beserta hasil cetaknya (ITE, 2024). Namun, alih-alih diiringi dengan peningkatan kapasitas saintifik sebagaimana direkomendasikan oleh Faizal & Luthfi (2024) terkait adopsi standar internasional ISO/IEC 27037 bagi *first responders*, penyidik dan sistem peradilan justru merespons perluasan ini dengan reduksi logika yang sangat problematis. Penegak hukum sering kali memperlakukan ekstensi bukti elektronik ini semata-mata sebagai "peralihan medium" fisik belaka dari kertas konvensional menjadi layar monitor.

Praktik di lapangan menunjukkan bahwa aparat penegak hukum sering kali mengekstraksi data log *digital marketing* yang kompleks hanya dengan mengambil tangkapan layar (*screenshot*) kemudian mencetaknya ke dalam kertas berita acara (*print-out*), lalu secara serampangan mengkategorikannya sebagai alat bukti "Surat" atau "Petunjuk" guna menggenapi syarat "dua alat bukti". Analisis tajam terhadap fenomena ini mengungkap sebuah anomali peradilan yang serius: paradigma kuantifikasi alat bukti (menghitung jumlah bukti agar genap menjadi dua) telah mengalahkan kualifikasi alat bukti (menguji substansi dan integritas forensik bukti). Praktik ini secara diametral bertentangan dengan temuan Ismail & Ariffin (2025) serta Abeysekera (2026), yang menegaskan bahwa keabsahan hukum (*legal admissibility*) alat bukti siber mutlak bergantung pada pemenuhan Standar Daubert, khususnya ketersediaan nilai *hash* (MD5/SHA1) untuk membuktikan ketiadaan perusakan (*tampering*). Dengan sekadar mencetak bukti digital, keseluruhan struktur metadata yang memverifikasi integritas algoritma dan keaslian penanda waktu otomatis terputus dari sumber aslinya. Akibatnya, bukti tersebut terdegradasi menjadi informasi sepihak (*hearsay*) yang kehilangan objektivitas forensiknya (Tejerizo, 2023). Jika dibiarkan tanpa pengawasan yudisial (*judicial oversight*) yang ketat pada fase praperadilan, praktik penetapan tersangka berbasis tangkapan layar ini akan membenarkan peringatan kritis Westlund et al. (2025), di mana digitalisasi peradilan justru memfasilitasi otoritarianisme teknologis dan mereduksi kebebasan fundamental akibat prosedur hukum yang serampangan.

Di sinilah letak akar permasalahan doktrinal yang menyelimuti peradilan pidana siber Indonesia. Paradigma kuantifikasi yang dijalankan oleh aparat penegak hukum tidak mampu menahan laju kerentanan teknologis (*technological vulnerability*) bukti elektronik, mengingat dokumen digital dapat dimodifikasi dengan sangat mudah tanpa meninggalkan jejak kasat mata.

Realitas empiris ini beresonansi kuat dengan postulat Buiten et al. (2023) dan didukung oleh analisis Ismaeel et al. (2026), yang memperingatkan bahwa sistem teknologi otonom dan algoritmik memiliki struktur internal berupa *black-box* (kotak hitam). Sifat *black-box* ini mustahil dan tidak boleh diverifikasi hanya dengan pendekatan observasi konvensional berbasis indra penglihatan (seperti sekadar melihat *print-out*). Hal ini menuntut adanya atribusi tanggung jawab yang didasarkan pada audit teknis yang spesifik, terkontrol, dan presisi. Ketika logika pembuktian konvensional KUHAP dipaksakan untuk menafsirkan realitas *black-box digital marketing* tanpa dijembatani oleh disiplin sains forensik, maka kuantifikasi "dua alat bukti" pada tahap praperadilan hanya akan menghasilkan kepastian hukum semu yang mencederai keadilan substantif.

Analisis *Rasio Decidendi* Hakim Praperadilan: Ketegangan antara Formalitas Prosedural dan *Due Process of Law*

Keterasingan instrumen pembuktian konvensional terhadap realitas bukti siber memicu perdebatan hukum yang ekstrem ketika diuji dalam ruang sidang praperadilan. Pranata praperadilan pada hakikatnya merupakan sarana peradilan konstitusional yang didesain secara spesifik untuk menguji legalitas tindakan paksa aparatur negara terhadap warga negaranya. Ekstensifikasi kewenangan praperadilan melalui Putusan Mahkamah Konstitusi (MK) Nomor 21/PUU-XII/2014 yang memasukkan pengujian sah atau tidaknya "penetapan tersangka" sebagai objek praperadilan dilandasi oleh rasionalitas bahwa pembatasan hak asasi manusia sejak tahap dini penyelidikan dan penyidikan tidak boleh dilakukan secara serampangan. Pembatasan tersebut wajib merujuk pada standar minimal pembuktian serta jaminan perlindungan HAM yang diatur ketat dalam Pasal 235 KUHAP Baru. Melalui penguatan prinsip *due process of law*, penetapan status hukum maupun tindakan upaya paksa oleh aparat harus didasarkan pada kecukupan alat bukti sah, guna mencegah penyalahgunaan wewenang sejak awal proses peradilan. Signifikansi filosofis dari yurisprudensi ini terletak pada pergeseran rezim peradilan pidana dari kekuasaan mutlak penyidik (*executive heavy*) menuju pengetatan mekanisme uji peradilan awal (*judicial scrutiny*). Transisi ini mengonfirmasi peringatan kritis dari Westlund et al. (2025), yang menegaskan bahwa digitalisasi sistem peradilan pidana mutlak membutuhkan pengawasan yudisial (*judicial oversight*) yang ketat; ketiadaan pengawasan ini hanya akan mereduksi hak-hak privasi sipil dan memfasilitasi lahirnya otoritarianisme teknologis di tangan aparat penegak hukum.

Namun, analisis kritis atas berbagai *rasio decidendi* (pertimbangan hukum) hakim tunggal praperadilan dalam perkara kejahatan siber justru memperlihatkan sebuah labirin disparitas putusan yang sangat mengkhawatirkan. Fenomena ini secara presisi menjawab dan memvalidasi keluhan akademis pada lanskap domestik yang sebelumnya dikemukakan oleh Jondong (2020) serta Siregar et al. (2026), di mana ketertinggalan regulasi hukum acara dalam merespons sifat volatilitas bukti elektronik telah berujung pada inkonsistensi yang akut di tahap awal penyidikan. Dalam banyak kasus, hakim mengambil posisi formalistik sempit dengan berlindung di balik premis bahwa "praperadilan hanya berwenang menilai aspek formil, bukan masuk ke dalam materi pokok perkara". Berdasarkan *rasio decidendi* formalistik ini, selama penyidik dapat menunjukkan selembar Berita Acara Pemeriksaan (BAP) Saksi dan selembar hasil cetak (*print-out*) dokumen elektronik dari aktivitas *digital marketing* yang dipersengketakan, maka syarat minimal kuantitatif "dua alat bukti" dianggap telah paripurna. Hakim penganut mazhab ini secara sadar menutup mata dan menolak untuk memeriksa bagaimana *print-out* tersebut diperoleh. Mereka mengabaikan pentingnya memvalidasi apakah data peladen telah diubah sebelum tangkapan layar diambil, atau apakah data diekstraksi secara ilegal. Pengabaian ini merupakan penolakan langsung terhadap Standar Daubert yang diajukan oleh Ismail & Ariffin (2025) dan Abeysekera (2026), di mana keabsahan hukum (*legal admissibility*) dari sebuah bukti digital seharusnya dinilai dari kemampuannya mempertahankan nilai *hash* (seperti MD5 dan SHA1) untuk membuktikan secara empiris bahwa data tersebut tidak mengalami perusakan (*tampering*).

Pendekatan yudisial yang sempit ini berbenturan langsung secara diametral dengan substansi *due process of law* yang diamanatkan konstitusi, serta secara benderang melanggar roh

Putusan MK Nomor 20/PUU-XIV/2016. Putusan MK tersebut secara fundamental memberikan preskripsi bahwa alat bukti elektronik tidak hanya dinilai dari wujud keberadaannya semata, tetapi secara imperatif mensyaratkan perolehan yang sah (*lawful interception/acquisition*) sesuai asas kepatutan hukum (MKRI, 2016). Parameter perolehan yang sah ini, sebagaimana dikonstruksikan oleh Faizal & Luthfi (2024), seharusnya mengadopsi kerangka standar tata kelola global seperti ISO/IEC 27037 dalam hal identifikasi dan akuisisi oleh penanggap pertama (*first responders*). Jika sebuah perolehan data digital melanggar hukum prosedur forensik, maka bukti tersebut berubah statusnya menjadi alat bukti tidak sah (*unlawful legal evidence*) dan otomatis tunduk pada doktrin *fruit of the poisonous tree* (buah dari pohon yang beracun). Konsekuensinya, bukti tersebut kehilangan kekuatan pembuktian dan harus dibatalkan demi hukum (*exclusionary rule*) guna mencegah kriminalisasi prematur (Thuyen, 2025).

Kegagalan mayoritas hakim praperadilan dalam memahami garis demarkasi antara "syarat formil kemunculan bukti digital" dengan "pengujian materi pokok perkara" telah menciptakan kekacauan penegakan hukum tersendiri. Pertanyaan mengenai *"apakah dokumen digital marketing ini benar milik tersangka dan berisi unsur penipuan"* memang merupakan domain pengujian materi pokok perkara di sidang akhir. Namun, pertanyaan mengenai *"apakah dokumen digital ini diekstraksi menggunakan metode penyitaan yang mempertahankan keaslian data (integritas forensik) sehingga sah secara prosedur untuk dijadikan pijakan penetapan tersangka"* adalah secara mutlak merupakan ranah pengujian formil praperadilan. Mengingat ekosistem *digital marketing* ditopang oleh algoritma otonom yang bersifat *black-box*, kewajiban menghadirkan jejak audit teknis forensik bukanlah sebuah opsi, melainkan syarat keabsahan yang esensial (Buiten et al., 2023; Ismaeel et al., 2026). Oleh karena itu, *rasio decidendi* yang melegitimasi alat bukti digital semata-mata karena telah dicetak di atas kertas dan dilampiri stempel penyidik tanpa disertai laporan log forensik atau audit teknis yang presisi merupakan bentuk distorsi yang fatal terhadap tujuan keadilan praperadilan. Dialog akademis ini membantah keras pandangan konvensional yang menyatakan bahwa ruang lingkup praperadilan dilarang menguji metodologi pengumpulan bukti. Praperadilan memang tidak berwenang menguji kebenaran isi dari bukti elektronik, tetapi lembaga ini secara imperatif dan konstitusional diwajibkan untuk menguji keabsahan proses formil di balik kemunculan bukti tersebut.

Operasionalisasi Teori Bukti Digital: Standar Forensik dan Rantai Pasok Bukti (*Chain of Custody*) sebagai Instrumen Validasi Yudisial

Menyikapi krisis *rasio decidendi* dan disparitas putusan praperadilan yang secara konsisten dikeluhkan dalam lanskap domestik oleh Jondong (2020) serta Siregar et al. (2026), norma hukum acara pidana wajib meminjam infrastruktur teoretis dari sains forensik komputer (*computer forensics*) untuk melahirkan kepastian hukum. Teori bukti digital mensyaratkan bahwa untuk dapat diterima secara hukum (*admissible*), suatu data elektronik harus memenuhi parameter kelengkapan (*completeness*), keandalan (*reliability*), keaslian (*authenticity*), dan bebas dari kontaminasi (*integrity*). Parameter ketat ini mustahil dibuktikan melalui sumpah saksi penyidik semata; ia secara imperatif menuntut instrumen validasi prosedural bernama *chain of custody* (rantai pasok bukti). Tanpa instrumen ini, proses peradilan digital membenarkan peringatan kritis Westlund et al. (2025), di mana ketiadaan pengawasan yudisial (*judicial oversight*) yang berbasis standar saintifik akan mereduksi hak privasi dan menjerumuskan penegakan hukum ke dalam praktik otoritarianisme teknologis.

Chain of custody pada dasarnya adalah dokumentasi historis dan logis tanpa putus yang mencatat perjalanan dan pemeliharaan alat bukti dari titik pengamanan awal (identifikasi) di tempat kejadian, proses ekstraksi data, kloning forensik (*forensic imaging*), penyimpanan, hingga presentasi di muka peradilan (Nath et al., 2024). Dalam konteks kejahatan *digital marketing*, bukti yang disita oleh penyidik bukan berupa objek fisik statis (meskipun tersimpan di dalam perangkat keras/komputer), melainkan susunan elektromagnetik (kode biner) yang sangat rentan hancur apabila perangkat dioperasikan dengan cara yang keliru, di-*reboot* secara acak, atau terkoneksi dengan internet terbuka. Merespons kerentanan fatal ini, konstruksi kewajiban adopsi standar internasional ISO/IEC 27037 oleh *first responders* (penanggap pertama)

sebagaimana diajukan oleh Faizal & Luthfi (2024) menjadi sangat krusial, guna menjamin identifikasi dan akuisisi bukti digital dilakukan tanpa merusak integritas data aslinya.

Memvalidasi urgensi tata kelola tersebut, Ismail & Ariffin (2025) yang analisis empirisnya sejalan dengan Abeysekera (2026) mengenai validitas alat ukur forensik mengoperasionalkan pentingnya jaminan integritas ini melalui validasi hasil forensik menggunakan alat investigasi digital (baik komersial maupun sumber terbuka). Keabsahan instrumen hukum dalam investigasi ini diukur secara saintifik dari parameter algoritma kriptografi yang dikenal dengan istilah nilai *hash* (seperti *Message-Digest algorithm 5*/MD5 atau *Secure Hash Algorithm 1*/SHA1). Nilai *hash* bertindak sebagai sidik jari digital tak terbantahkan (*digital fingerprint*) dari sebuah arsip data. Jika data *log server digital marketing* digandakan dengan benar secara forensik (*bit-stream image*), duplikat data tersebut harus menghasilkan kalkulasi algoritma *hash* yang seratus persen identik dengan data asli (Franssen & Tosza, 2025). Sekecil apapun modifikasi yang terjadi bahkan pengubahan satu karakter pun pada arsip data pemasaran akan secara instan dan dramatis mengubah nilai *hash*-nya, menandakan bahwa alat bukti telah tercemar atau direkayasa (*tampering*). Kebutuhan akan presisi kriptografis inilah yang secara langsung merespons dilema *black-box* algoritma yang dianalisis oleh Buiten et al. (2023) dan Ismaeel et al. (2026), di mana otonomi teknologi menyulitkan kausalitas tradisional sehingga menuntut atribusi tanggung jawab yang didasarkan murni pada audit teknis yang presisi.

Operasionalisasi konsep sains ini ke dalam pisau analisis hukum deduktif menghasilkan suatu konklusi yang tegas bagi hakim praperadilan. Syarat minimal "dua alat bukti" elektronik yang sah tidak dapat dan tidak boleh ditafsirkan telah terpenuhi apabila penyidik gagal menunjukkan dokumentasi *chain of custody* dan nilai *hash* di sidang praperadilan. Ketiadaan bukti otentikasi algoritmik ini mengindikasikan ketiadaan jaminan keaslian formil. Oleh karena itu, langkah penyidik yang secara sepihak merampas akses komputasi perusahaan pemasaran digital dan mencetak isi basis datanya secara acak tanpa metode *forensic imaging* harus diputus tidak sah. Menegakkan prinsip ini berarti menghalangi praktik manipulasi peradilan pidana melalui pemalsuan atau modifikasi data digital (*tampering*), sekaligus menempatkan hukum acara Indonesia sejajar dengan pemenuhan *Daubert Standard* yang digunakan secara universal dalam tata kelola peradilan modern (Kurtz & Pintarelli, 2024).

Komparasi Proporsional Standar Global ISO/IEC 27037 dan Transformasi Kelembagaan Praperadilan

Mendiskusikan legalitas alat bukti elektronik semata-mata pada ranah lokal regulasi KUHAP terbukti memicu kebuntuan dan stagnasi penalaran hukum. Oleh karena itu, diskursus pembuktian ini mutlak harus dielevasi dengan membedah konstelasi perundang-undangan domestik yang kemudian dibenturkan dan didialogkan dengan standar tata kelola ketatanegaraan universal serta studi komparasi internasional. Dalam hal ini, temuan penelitian ini mengafirmasi dan memperluas analisis Faizal & Luthfi (2024), yang secara rigid mengelaborasi urgensi kepatuhan terhadap regulasi internasional ISO/IEC 27037:2012 mengenai pedoman identifikasi, pengumpulan, akuisisi, dan preservasi bukti digital. Standar ISO ini tidak dikonstruksikan untuk mendisrupsi atau menggantikan hukum acara pidana nasional (*national laws*), melainkan secara spesifik berfungsi memfasilitasi keseragaman metodologis. Melalui pedoman ini, penyidik atau penanggap pertama (*Digital Evidence First Responders*/DEFR) diwajibkan untuk mengidentifikasi dan memproteksi data komputasi tanpa sedikit pun mengotak-atik keasliannya guna menghindari kontaminasi atau *tampering*.

Dalam ruang komparasi peradilan tata negara Barat, persoalan kekosongan hukum ini telah lama dijembatani melalui doktrin hukum pembuktian yang jauh lebih presisi dan maju. Di yurisdiksi Amerika Serikat, syarat validitas perolehan data elektronik secara ketat tunduk pada parameter *Federal Rules of Evidence* (FRE). Khususnya pada *Rule 901* mengenai otentikasi data, regulasi tersebut secara imperatif mensyaratkan pembuktian keaslian sumber data tanpa adanya intervensi pihak mana pun (Legal Information Institute, 2011). Lebih lanjut, yurisdiksi Eropa telah melangkah lebih jauh dengan menginisiasi kerangka kerja *E-Evidence* (*Directive & Regulation on European Production and Preservation Orders for electronic evidence*). Kerangka kerja regional ini mensyaratkan bahwa penyitaan dan pemeliharaan alat bukti digital lintas batas

negara wajib tunduk pada instrumen pengawasan pengadilan (*judicial oversight*) yang independen. Pengawasan ini didesain guna menjaga titik keseimbangan yang rasional antara agenda pemberantasan kejahatan dan proteksi hak privasi warga negara. Kegagalan penyidik dalam mematuhi protokol penjaminan privasi dan otentikasi forensik ini berimplikasi fatal, yang dapat menyebabkan hakim menolak penerimaan bukti tersebut secara mutlak (Ramos, 2025).

Jika parameter komparatif internasional ini ditranslasikan dan disuntikkan ke dalam kerangka pembuktian peradilan pidana Indonesia, maka integrasi standar ISO/IEC 27037 dapat dipetakan secara presisi sebagai instrumen uji peradilan formil (*judicial review*) yang mengikat pada pranata praperadilan. Pemetaan integratif dan dialog antar-sistem ini dapat dikonseptualisasikan secara komprehensif melalui tabel perbandingan prosedural berikut:

Tabel 1. Korelasi KUHAP, ISO/IEC 27037, dan Hukum Konstitusional

Mekanisme KUHAP Tradisional	Translasi Forensik Berdasarkan ISO/IEC 27037	Signifikansi Hukum Konstitusional (Due Process of Law)
Penyitaan Benda Berwujud (Pasal 118 sampai Pasal 135 KUHAP)	**Identifikasi & Pengumpulan:** (*Identification & Collection*) terhadap bukti volatil (RAM komputer, lalu lintas web) dan non-volatil.	Mencegah kerusakan bukti kritis yang berujung pada penetapan tersangka prematur. Melindungi dari penyitaan data yang tidak relevan dengan objek pidana (proteksi privasi).
Penjagaan Keaslian Bukti Fisik (Penyegelan)	**Akuisisi & Preservasi:** (*Acquisition & Preservation*). Wajib memakai metode *bit-by-bit copy* tanpa memanipulasi *file* asli pada perangkat asal pelaku.	Menjamin kedudukan bukti elektronik identik mutlak dengan perangkat asli, mematikan narasi pembelaan tersangka bahwa data telah dimanipulasi oleh kepolisian.
Berita Acara Pemeriksaan (BAP) Penyitaan Benda	**Dokumentasi Rantai Pasok Bukti:** (*Chain of Custody*). Log lengkap mencatat nilai *hash* (MD5/SHA1), perangkat lunak ekstraksi yang dipakai, tanggal, dan akses riwayat.	Memberikan alat uji akuntabilitas (*auditability*) bagi Hakim Praperadilan untuk mengeksekusi *Exclusionary Rule* apabila terindikasi cacat formil perolehan bukti.

Tabel komparasi konseptual di atas merepresentasikan formulasi argumentasi penyelesaian yang holistik dan komprehensif atas kebuntuan disparitas putusan praperadilan. Menjadikan parameter ISO/IEC 27037 sebagai panduan *de facto* untuk menafsirkan keabsahan "dua alat bukti" sama sekali bukan berarti melampaui teks undang-undang KUHAP, melainkan merupakan upaya untuk mengisi kekosongan hukum operasional melalui interpretasi sistematis dan teleologis yang berorientasi kuat pada terwujudnya peradilan yang jujur dan adil (*fair trial*). Pendekatan ini secara langsung mengamini sekaligus menjawab ketakutan akademik yang disuarakan secara lantang oleh Westlund et al. (2025). Apabila institusi praperadilan membiarkan kewenangan tak terbatas dari aparat negara dalam mengekstraksi dan menafsirkan data digital secara serampangan, sistem peradilan pidana dipastikan tidak lagi bekerja untuk mengadili kejahatan. Sebaliknya, instrumen peradilan justru akan bertransformasi menjadi sarana "kediktatoran teknologis" yang memberangus hak-hak kebebasan fundamental warga negaranya. Hakim praperadilan, dengan demikian, dituntut untuk keluar dari belenggu positivisme sempit dan tidak hanya pasif memegang palu. Mereka dituntut untuk berevolusi menjadi moderator saintifik yang kritis, yang senantiasa mewajibkan keadilan matematis (forensik) agar berjalan seirama dan sejalan dengan keadilan sosiologis (konstitusi).

Mengakhiri diskursus yang mendalam mengenai persimpangan rumit antara hukum acara pidana, teknologi forensik, dan fenomena kejahatan pemasaran digital algoritmik, analisis kritis dari penelitian ini secara tegas mematahkan dan mendekonstruksi ortodoksi praktik peradilan konvensional. Penyelidikan dan penyidikan terhadap tindak pidana *digital marketing*

mutlak tidak dapat lagi diukur, dibaca, maupun diadili melalui kacamata paradigma fisikal warisan abad lampau. Reduksi esensi pembuktian elektronik ke dalam format selembar hasil cetak *screenshot* dan BAP saksi pelapor semata yang kemudian disahkan secara sepihak sebagai pemenuhan syarat kuantitatif "dua alat bukti" oleh hakim praperadilan merupakan sebuah kecacatan dogmatik akut. Praktik yang keliru ini secara sistematis akan menghancurkan fondasi *due process of law* di Indonesia.

Oleh karenanya, penetapan status tersangka yang beranjak dari alat bukti pembuktian digital menuntut pemenuhan parameter kualitatif secara ketat, bukan sekadar kalkulasi kuantitatif. Pemenuhan ini diwujudkan dengan mendialogkan syarat keabsahan dalam UU ITE dan KUHAP (berdasarkan Putusan MK No. 21/PUU-XII/2014) secara integratif bersama dengan prinsip validasi internasional. Hakim tunggal praperadilan secara konstitusional diwajibkan untuk merekonstruksi *rasio decidendi*-nya dengan mengadopsi standar tata kelola ISO/IEC 27037. Selain itu, hakim harus menuntut secara imperatif eksistensi dokumentasi *chain of custody* berserta otentikasi *hash value* sebagai syarat sah formil mutlak berdirinya suatu alat bukti elektronik. Ketiadaan instrumen forensik fundamental ini secara absolut mengkonversi kedudukan bukti digital menjadi perolehan yang merusak dan melanggar hukum prosedur (*unlawful legal evidence*). Kondisi cacat formil ini memerintahkan hakim secara hukum untuk mengeksekusi kewenangannya dan membatalkan status penetapan tersangka dengan bersandar pada doktrin buah dari pohon beracun (*fruit of the poisonous tree*). Pada akhirnya, integrasi hibrida antara norma perundang-undangan dan forensik digital ini bukan sekadar tawaran metodologi alternatif yang opsional. Integrasi ini merupakan keharusan sistemik dan urgensi peradilan demi memulihkan muruah keadilan pidana Indonesia, memastikan setiap penetapan tersangka dilakukan di atas pijakan saintifik yang objektif dan tak terbantahkan, serta menjaga kemurnian perisai konstitusional hak asasi manusia dari arogansi maupun kebodohan teknologis dalam arena investigasi pidana siber.

SIMPULAN

Penegakan hukum terhadap tindak pidana *digital marketing* yang bersifat *volatile* mutlak menuntut pergeseran paradigma dari pembuktian fisikal konvensional menuju pendekatan saintifik guna menjamin keadilan substantif. Berdasarkan analisis kritis, *rasio decidendi* mayoritas hakim praperadilan yang mengesahkan status tersangka hanya dengan bersandar pada kuantifikasi alat bukti seperti cetakan tangkapan layar (*print-out*) tanpa audit forensik merupakan sebuah kecacatan dogmatik yang secara fundamental melanggar prinsip perlindungan hak asasi manusia dan *due process of law*. Sebagai solusi sistemik atas kekosongan tersebut, standar keandalan forensik digital global, khususnya kerangka ISO/IEC 27037, wajib diintegrasikan sebagai parameter yudisial normatif yang mengikat di lembaga praperadilan dengan mensyaratkan eksistensi dokumentasi *chain of custody* beserta otentikasi *hash value* pada setiap pengujian keabsahan bukti elektronik. Ketiadaan pemenuhan instrumen validasi internasional tersebut secara absolut akan mengonversi kedudukan bukti digital menjadi perolehan ilegal (*unlawful legal evidence*), sehingga hakim berwenang secara imperatif membatalkan status tersangka untuk mencegah terjadinya kriminalisasi yang prematur dan artifisial.

REFERENSI

Abdullah, H. O., Maqsood, M., & Nadeem, A. (2025). Digital Evidence in Criminal Proceedings: Legal Standards, Chain of Custody, and Evidentiary Reliability in The Digital Era. *Research Journal for Social Affairs*, *3*(5), 795–805. https://doi.org/10.71317/RJSA.003.05.0375

Abeysekera, I. (2026). Open source tools: an evaluation for digital forensic investigations. *Frontiers in Research Metrics and Analytics*, *11*. https://doi.org/10.3389/frma.2026.1790333

Anggraeniko, L. S., Ambarwati, A., & Utami, F. R. (2026). Admissibility of digital evidence in Indonesia: Criminal–civil implications for the chain of custody and evidentiary validity. *Priviet Social Sciences Journal*, *6*(4), 483–494. https://doi.org/10.55942/pssj.v6i4.1566

Buiten, M., de Streel, A., & Peitz, M. (2023). The law and economics of AI liability. *Computer Law &*

Security Review, *48*, 105794. https://doi.org/10.1016/j.clsr.2023.105794

Faizal, A., & Luthfi, A. (2024). Comparison Study of NIST SP 800-86 and ISO/IEC 27037 Standards as A Framework for Digital Forensic Evidence Analysis. *Journal of Information Systems and Informatics*, *6*(2), 701–718. https://doi.org/10.51519/journalisi.v6i2.717

Franssen, V., & Tosza, S. (2025). Collecting Digital Evidence: Transversal Challenges and Solutions. In V. Franssen & S. Tosza (Eds.), *The Cambridge Handbook of Digital Evidence in Criminal Investigations* (pp. 11–40). Cambridge University Press. https://doi.org/10.1017/9781009049771

Hutchinson, T. (2025). Doctrinal research. In *Research Methods in Law* (pp. 8–38). Routledge. https://doi.org/10.4324/9781032710372-2

Ismaeel, S., Alammari, K., & Ghanim Younus, Z. (2026). Evidentiary Challenges in AI-Mediated E-Commerce Disputes. *Justicia Islamica*, *23*(1), 85–118. https://doi.org/10.21154/justicia.v23i1.11809

Ismail, I., & Ariffin, K. A. Z. (2025). The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance. *PLOS One*, *20*(9), e0331683. https://doi.org/10.1371/journal.pone.0331683

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

Jondong, Z. (2020). Kebijakan Hukum Pidana bagi Tindak Pidana Cyber Terrorism dalam Rangka Pembentukan Hukum Positif di Indonesia. *Jurnal Preferensi Hukum*, *1*(2), 21–27. https://doi.org/10.22225/jph.1.2.2337.21-27

KUHAP. (2025). *Undang-undang (UU) Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana*.

Kurtz, J. E., & Pintarelli, E. M. (2024). The Daubert Standards for Admissibility of Evidence Based on the Personality Assessment Inventory. *Psychological Injury and Law*, *17*(2), 105–116. https://doi.org/10.1007/s12207-024-09508-5

Legal Information Institute. (2011). *Rule 901. Authenticating or Identifying Evidence*. https://www.law.cornell.edu/rules/fre/rule_901

Miller, C. M. (2023). A survey of prosecutors and investigators using digital evidence: A starting point. *Forensic Science International: Synergy*, *6*, 100296. https://doi.org/10.1016/j.fsisyn.2022.100296

MKRI. (2014). *Mahkamah Konstitusi, Putusan Nomor 21/PUU-XII/2014 perihal Pengujian Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana terhadap Undang-Undang Dasar Negara Republik Indonesia Tahun 1945*.

MKRI. (2016). *Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016, Pengujian Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.

Nath, S., Summers, K., Baek, J., & Ahn, G.-J. (2024). Digital Evidence Chain of Custody: Navigating New Realities of Digital Forensics. *2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)*, 11–20. https://doi.org/10.1109/TPS-ISA62245.2024.00012

Ramos, J. A. E. (2025). European Preservation and Production Orders: A Non-Exclusive Approach to E-Evidence within the EU: Implications of the Union Legislator's Choice to Derogate from the Precedence of Union Law in the E-Evidence Regulation. *Eucrim – European Law Forum: Prevention, Investigation, Prosecution*, *20*(3), 216–220. https://doi.org/10.30709/eucrim-2025-018

Santosa, D. G. G., & Kamali, K. M. I. (2022). Acquisition and Presentation of Digital Evidence in Criminal Trial in Indonesia. *Jurnal Hukum Dan Peradilan*, *11*(2), 195. https://doi.org/10.25216/jhp.11.2.2022.195-218

Siregar, W., Ansyari Siregar, A., & Siahaan, N. (2026). The Position of Electronic Evidence in the Police Investigation Process Based on the Criminal Procedure Code and Law Number 1 of 2024 Concerning ITE. *International Journal of Science and Environment (IJSE)*, *6*(1), 603–609. https://doi.org/10.51601/ijse.v6i1.376

Tejerizo, M. de A. (2023). Digital evidence and fair trial rights at the International Criminal Court. *Leiden Journal of International Law*, *36*(3), 749–769.

https://doi.org/10.1017/S0922156523000031

Thuyen, T. D. (2025). Fruit of the Poison Tree Doctrine in U.S. Criminal Proceedings and Regulations on the Exclusion of Evidence in Vietnamese Criminal Proceedings. *International Journal for the Semiotics of Law - Revue Internationale de Sémiotique Juridique*, *38*(2), 443–461. https://doi.org/10.1007/s11196-024-10129-z

Westlund, O., Carlson, M., Hamada, B., Helberger, N., Lecheler, S., C. Lewis, S., Quandt, T., D. Reese, S., Salaverría, R., Saldaña, M., Thomson, T. J., Wahl-Jorgensen, K., & Wu, S. (2025). Public Knowledge and Expertise Under Authoritarian Siege: A Defense of Academic Freedom from Digital Journalism Studies. *Digital Journalism*, *13*(5), 869–892. https://doi.org/10.1080/21670811.2025.2527997