ISSN: 2338 4638

Volume 8 Nomor 7 (2024)

'ADALAH

Buletin Hukum & Keadilan

Kedudukan Bukti Digital dalam Sistem Peradilan Pidana Indonesia: Rekonsepsi Pengaturan dan Penguatan *Chain of Custody* di Era *Cyber-Enabled Crime*

Gilang Rizki Aji Putra*

Universitas Islam Negeri Syarif Hidayatullah Jakarta

10.15408/adalah.v8i7.51879

Abstract:

Digital transformation has reshaped criminal activity and positioned electronic evidence as a central element in criminal investigations. This article analyzes the juridical status of digital evidence within Indonesia's criminal justice system, focusing on its legal basis, evidentiary value, and challenges related to authentication and the preservation of chain of custody. Using normative legal research with statutory, conceptual, and case approaches, the study finds that the Electronic Information and Transactions Law (ITE Law) has expanded the closed system of evidentiary instruments under the Criminal Procedure Code (KUHAP) by formally recognizing electronic information and documents as admissible evidence. Nevertheless, significant issues remain, including unclear substantive requirements for admissibility, the absence of comprehensive chain of custody standards, and disparities in law enforcement capacity. Court decisions demonstrate that evidentiary strength often depends on proving integrity and authenticity rather than clear normative standards. The article concludes that procedural reform, standardized digital forensic protocols, and institutional capacity building are essential.

Keywords: Digital Evidence, Chain of Custody, Criminal Procedure Code (KUHAP), Electronic Information and Transactions Law (ITE Law), Digital Forensics.

* Peneliti pada Pusat Studi Konstitusi dan legislasi Nasional (Poskolegnas), Universitas Islam Negeri Syarif Hidayatullah Jakarta. Email: gilang.rizkiajiputra19@uinjkt.ac.id.

A. PENDAHULUAN

Revolusi digital telah mentransformasi hampir setiap aspek kehidupan manusia, termasuk cara kejahatan dilakukan dan diungkap. Kejahatan konvensional seperti pencurian, penipuan, hingga pembunuhan kini meninggalkan jejak digital yang tak terhapuskan: log panggilan telepon, pesan instan, data lokasi GPS, transaksi keuangan elektronik, hingga rekaman kamera pengawas. Sementara itu, kejahatan siber murni seperti peretasan dan penyebaran malware sepenuhnya terjadi di ranah digital dan tidak meninggalkan bukti fisik sama sekali. Dalam lanskap ini, bukti digital (*digital evidence*) menjelma menjadi "saksi bisu" yang seringkali lebih jujur daripada saksi manusia, namun juga lebih rapuh dan mudah dimanipulasi.

Sistem peradilan pidana Indonesia, yang fondasi proseduralnya dibangun oleh Kitab Undang-Undang Hukum Acara Pidana (KUHAP) pada tahun 1981, tidak dirancang untuk mengakomodasi bukti digital. KUHAP menganut sistem numerus clausus alat bukti yang tertutup: keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa. Ketika era digital tiba, pengadilan menghadapi dilema: haruskah chat WhatsApp dianggap sebagai surat? Apakah metadata server termasuk petunjuk? Kegamangan ini dijawab dengan lahirnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang melalui Pasal 5 ayat (1) dan (2) secara

revolusioner menyatakan bahwa informasi dan dokumen elektronik merupakan alat bukti hukum yang sah. Ketentuan ini menjadi terobosan penting karena secara de jure memperluas alat bukti yang diakui dalam hukum acara pidana.

Namun, pengakuan formil ini tidak serta-merta menyelesaikan seluruh persoalan. Pengakuan bahwa file rekaman CCTV adalah alat bukti yang sah tidak otomatis menjamin bahwa file tersebut akan diterima dan dipertimbangkan hakim sebagai bukti yang cukup. Kekuatan pembuktian bukti digital sangat bergantung pada kemampuannya untuk melewati uji keaslian, integritas, dan keterandalan, yang dalam praktiknya memerlukan prosedur *chain of custody* (rantai penguasaan) yang ketat. Sayangnya, Indonesia belum memiliki standar prosedur chain of custody yang baku dan mengikat secara nasional. Akibatnya, banyak bukti digital yang ditolak pengadilan bukan karena tidak relevan, melainkan karena cacat prosedur dalam pengumpulannya (Santoso, 2023). Rumusan masalah artikel ini adalah: Pertama, bagaimana kedudukan yuridis bukti digital dalam sistem hukum acara pidana Indonesia? Kedua, apa tantangan utama dalam penerapan bukti digital dan bagaimana solusi untuk memperkuat posisinya? Tujuannya adalah untuk menganalisis secara komprehensif kerangka hukum, mengidentifikasi celah implementasi, serta menawarkan langkah-langkah strategis untuk

memperkokoh integritas bukti digital dalam peradilan pidana.

B. TEORI PEMBUKTIAN, DIGITAL EVIDENCE, DAN PRINSIP *CHAIN OF CUSTODY*

Sistem pembuktian yang dianut di Indonesia adalah *negatief wettelijk bewijsstelsel* atau sistem pembuktian berdasar undang-undang secara negatif. Untuk menyatakan seseorang bersalah, diperlukan sekurang-kurangnya dua alat bukti yang sah yang meyakinkan hakim (Pasal 183 KUHAP). Sistem ini menekankan bahwa keyakinan hakim harus lahir dari alat bukti yang diatur oleh undang-undang, bukan dari intuisi semata. Dengan demikian, sah atau tidaknya suatu alat bukti secara formil menjadi gerbang pertama yang menentukan apakah ia dapat masuk ke ruang pertimbangan hakim.

UU ITE telah melakukan ekstensifikasi makna alat bukti. Pasal 5 ayat (1) menyatakan bahwa informasi elektronik dan/atau dokumen elektronik serta hasil cetaknya merupakan alat bukti hukum yang sah. Ayat (2) menegaskan bahwa hal tersebut merupakan perluasan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia. Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016 semakin mempertegas kedudukan ini dengan menyatakan bahwa bukti elektronik dapat berdiri sendiri sebagai alat bukti, tetapi dalam konteks pidana harus tetap memenuhi syarat formil dan materiil.

Dalam literatur internasional, bukti digital didefinisikan sebagai setiap informasi yang disimpan atau ditransmisikan dalam bentuk digital yang memiliki nilai pembuktian (*probative value*) dalam suatu perkara (Casey, 2011). Karakteristik utamanya adalah volatilitas (mudah berubah atau hilang), replikabilitas (mudah diperbanyak tanpa kehilangan kualitas), dan ketergantungan pada medium. Karena karakter tersebut, doktrin best evidence rule mengharuskan diajukannya bukti orisinal. Namun, untuk bukti digital, konsep "orisinal" menjadi problematik karena salinan digital seringkali identik secara *bit-by-bit* dengan aslinya. Oleh karena itu, fokusnya bergeser ke *chain of custody*: serangkaian prosedur yang mendokumentasikan siapa yang mengakses bukti, kapan, di mana, dan untuk tujuan apa, sejak bukti ditemukan hingga diajukan di pengadilan. *Chain of custody* yang putus atau tidak terdokumentasi dengan baik akan menghancurkan integritas bukti dan membuatnya tidak dapat diterima (*inadmissible*) (Brenner, 2022). Kerangka ini akan digunakan untuk mengukur sejauh mana sistem Indonesia mengakomodasi kekhususan bukti digital.

C. KEDUDUKAN YURIDIS DAN KEKUATAN PEMBUKTIAN BUKTI DIGITAL

1. Landasan Hukum dan Perluasan Alat Bukti dalam Hukum Acara Pidana

Sebelum UU ITE, pengadilan pidana di Indonesia seringkali mengalami kesulitan untuk menerima bukti digital. KUHAP hanya mengenal "surat" sebagaimana diatur dalam Pasal 184 ayat (1) huruf c dan dielaborasi dalam Pasal 187. Surat dalam arti KUHAP adalah kertas yang bertuliskan, dibuat oleh pejabat resmi, atau memiliki hubungan hukum dengan isi surat lainnya. Definisi ini jelas tidak menjangkau surel, pesan instan, atau database digital. Celah ini ditutup oleh Pasal 5 UU ITE yang secara revolusioner menyatakan bahwa informasi dan dokumen elektronik adalah alat bukti yang sah. Lebih lanjut, Pasal 44 UU ITE menegaskan bahwa alat bukti dalam penyidikan, penuntutan, dan pemeriksaan di sidang pengadilan menurut undang-undang ini meliputi alat bukti sebagaimana dimaksud dalam KUHAP dan juga informasi serta dokumen elektronik.

Dengan demikian, bukti digital tidak menggantikan alat bukti konvensional, melainkan berdiri di sampingnya sebagai lex specialis yang memperluas alat bukti. Secara formil, kedudukannya sudah kuat. Namun, persoalannya adalah UU ITE tidak mengatur secara rinci bagaimana bukti digital harus diperoleh, disimpan, dan diajukan. UU ITE merujuk pada prinsip "data yang dapat dilihat, dibaca, atau didengar" dan menekankan bahwa hasil cetak atau salinan digital adalah sah sepanjang dapat diakses dan dijamin integritasnya (Pasal 6 dan Pasal 15). Permasalahan muncul ketika integritas itu

dipertanyakan: siapa yang berwenang menyatakan integritas suatu bukti digital terjaga? Apakah cukup dengan keterangan penyidik, atau harus melalui ahli forensik? Ketidakjelasan inilah sumber masalah utama.

2. Syarat Formil dan Materiil Bukti Digital: Ketegangan antara Orisinalitas dan Integritas

Agar dapat digunakan dalam pembuktian pidana, bukti digital harus memenuhi syarat formil dan syarat materiil. Syarat formil meliputi: (a) cara memperolehnya sah (tidak melalui penyadapan ilegal atau akses tanpa hak); (b) disimpan dan diajukan sesuai dengan prosedur chain of custody; dan (c) dihadirkan oleh pihak yang berwenang. Syarat materiil meliputi: (a) relevan dengan perkara; (b) isinya benar dan tidak dimanipulasi; serta (c) tidak bertentangan dengan hukum dan kesusilaan.

Salah satu isu paling krusial adalah bagaimana membuktikan bahwa bukti digital yang diajukan adalah "asli". Dalam kasus di mana bukti berupa salinan tangkapan layar (screenshot), pembela seringkali membantah dengan berargumen bahwa screenshot mudah direkayasa menggunakan perangkat lunak pengedit gambar. Mahkamah Agung dalam sejumlah putusannya, seperti Putusan Nomor 661 K/Pid.Sus/2019, menekankan bahwa untuk menilai keaslian bukti digital, hakim harus mempertimbangkan alat bukti lain yang mendukung, termasuk keterangan saksi ahli digital

forensik. Artinya, bukti digital yang diajukan tanpa dukungan ahli sangat rapuh terhadap bantahan.

Praktik di pengadilan juga menunjukkan adanya ketidakkonsistenan. Ada hakim yang menerima print out rekening koran sebagai alat bukti surat biasa tanpa mempersoalkan keasliannya, ada pula yang menolak hasil unduhan konten media sosial karena tidak disertai berita acara penyitaan digital. Ketidakpastian ini sangat merugikan baik bagi penuntut umum yang ingin membuktikan dakwaan, maupun bagi terdakwa yang haknya untuk diadili secara adil terancam oleh bukti yang tidak valid (Prasetyo, 2024).

3. *Chain of Custody*: Elemen Kunci yang Sering Terabaikan

Chain of custody dalam konteks bukti digital adalah serangkaian kronologis yang mendokumentasikan pengumpulan, pengamanan, pengiriman, analisis, dan penyimpanan bukti. Setiap aktivitas harus dicatat: siapa yang melakukannya, kapan, di perangkat apa, dengan tools apa, dan siapa yang menyaksikan. Di Indonesia, pemahaman tentang *chain of custody* digital baru berkembang di segelintir laboratorium forensik seperti Pusat Laboratorium Forensik Polri (Puslabfor) dan BSSN. Di tingkat Kepolisian Resor atau Kejaksaan Negeri, peralatan dan keahlian untuk mempertahankan *chain of custody* masih sangat terbatas.

Akibatnya, banyak perkara yang seharusnya dapat dibuktikan dengan bukti digital yang kuat justru berakhir dengan pembebasan karena bukti tersebut "tercemar". Contoh paling sederhana adalah ketika penyidik menyita telepon genggam tersangka dan dengan santainya menggunakan password yang diberikan tersangka untuk membuka dan membaca sendiri isinya tanpa disaksikan oleh ahli, tanpa merekam prosesnya, dan tanpa melakukan imaging forensik. Tindakan ini, selain melanggar privasi, juga merusak integritas metadata: kapan pesan itu pertama kali diakses, apakah ada perubahan, semuanya menjadi tidak dapat diverifikasi. Di persidangan, pembela dapat dengan mudah membantah bahwa isi ponsel tersebut telah dimanipulasi oleh penyidik. Di sinilah chain of custody menjadi benteng terakhir yang menentukan diterima atau tidaknya bukti digital (Santoso, 2023).

D. IMPLEMENTASI BUKTI DIGITAL DALAM PRAKTIK PERADILAN PIDANA

Putusan Mahkamah Agung Nomor 1089 K/Pid.Sus/2018 (Kasus Ujaran Kebencian)

Dalam kasus ini, terdakwa didakwa menyebarkan ujaran kebencian melalui akun Facebook. Alat bukti utama yang diajukan adalah tangkapan layar akun Facebook atas nama terdakwa yang berisi unggahan bernada kebencian, serta berita acara penyitaan digital. Di tingkat pertama, terdakwa divonis bersalah. Namun, di tingkat kasasi,

pembela mengajukan keberatan tentang keaslian bukti: akun Facebook sangat mudah diretas atau dikloning, dan tangkapan layar bukanlah bukti orisinal karena tidak ada pemeriksaan forensik terhadap server Facebook. Mahkamah Agung dalam putusannya membatalkan vonis dan membebaskan terdakwa karena jaksa tidak mampu membuktikan keaslian akun secara meyakinkan. Kasus ini menjadi preseden penting tentang betapa krusialnya peran ahli forensik dalam mengautentikasi bukti digital. Tanpa digital forensic imaging dan verifikasi dari penyelenggara platform, bukti digital berupa unggahan media sosial sangatlah rapuh.

Pembuktian Korupsi dengan Bukti Transfer Elektronik (Putusan MA No. 161 K/Pid.Sus/2019)

Berbeda dengan kasus sebelumnya, dalam sebuah kasus korupsi dana desa, jaksa berhasil meyakinkan hakim menggunakan bukti transfer elektronik. Bukti yang diajukan tidak hanya tangkapan layar, tetapi juga rekaman log transaksi asli yang diperoleh dari bank berdasarkan permintaan resmi penyidik, disertai berita acara pemeriksaan data elektronik oleh auditor forensik. *Chain of custody* dijaga ketat: data diterima dalam bentuk harddisk tersegel, dibuka bersama di hadapan saksi, dan diperiksa menggunakan perangkat lunak forensik berlisensi. Hakim menerima bukti tersebut sebagai alat bukti surat elektronik yang sah dan menjatuhkan vonis bersalah. Kasus ini menunjukkan bahwa jika prosedur chain

of custody dipatuhi, bukti digital memiliki kekuatan pembuktian yang sangat kuat, bahkan lebih sulit dibantah dibandingkan bukti fisik.

CCTV dan Pengungkapan Pembunuhan Berencana (Kasus Mirna Salihin, 2016)

Kasus pembunuhan Wayan Mirna Salihin dengan kopi beracun pada tahun 2016 mungkin adalah kasus paling populer yang melibatkan bukti digital secara masif. Bukti utama penuntut umum adalah rekaman CCTV di kafe yang menunjukkan terdakwa, Jessica Wongso, meletakkan sesuatu ke dalam gelas Mirna. Tidak ada saksi mata langsung yang melihat tindakan peracunan. Pembuktian didasarkan pada rekaman CCTV yang telah diambil dari hard disk perekam, diperiksa ahli forensik video, dan disaksikan oleh banyak pihak. Proses *chain of custody*-nya menjadi sorotan karena rekaman tersebut hanya memperlihatkan gerakan, bukan wajah jelas. Ahli forensik menjelaskan bahwa pixelasi tertentu tidak menunjukkan manipulasi, melainkan keterbatasan resolusi. Meskipun penuh kontroversi, kekuatan pembuktian bukti video digital mampu mengarahkan keyakinan hakim untuk menjatuhkan vonis bersalah. Kasus ini menunjukkan bahwa bukti digital dapat menjadi tulang punggung pembuktian, tetapi sekaligus menunjukkan betapa pentingnya transparansi dan validasi ahli dalam mempertahankannya.

E. REFORMULASI NORMA DAN PENINGKATAN KAPASITAS

Untuk memperkuat kedudukan bukti digital, diperlukan langkah-langkah reformatif yang sistematis. Pertama, revisi KUHAP harus segera dilakukan untuk mengintegrasikan secara eksplisit alat bukti elektronik ke dalam Pasal 184 KUHAP, tidak hanya bergantung pada UU ITE sebagai lex specialis. Revisi ini harus juga mengatur prinsip-prinsip pengumpulan, penyimpanan, dan penyajian bukti digital yang memenuhi standar hak asasi manusia, termasuk larangan penyadapan tanpa izin pengadilan.

Kedua, diperlukan Standar Prosedur Operasional (SOP) nasional tentang *chain of custody* bukti digital yang ditetapkan oleh institusi penegak hukum bersama (Polri, Kejaksaan, Mahkamah Agung). SOP ini harus mengadaptasi standar internasional seperti ISO/IEC 27037 tentang petunjuk identifikasi, pengumpulan, dan akuisisi bukti digital, disesuaikan dengan kondisi Indonesia. SOP ini akan menjadi rujukan bagi hakim untuk menilai apakah chain of custody telah terpenuhi atau tidak.

Ketiga, peningkatan kapasitas SDM dan infrastruktur forensik digital tidak dapat ditawar. Setiap Polda dan Kejaksaan Tinggi idealnya memiliki laboratorium forensik digital dasar yang mampu menangani akuisisi dan analisis bukti digital sederhana. Pelatihan tentang digital evidence handling harus menjadi bagian dari kurikulum wajib

bagi penyidik, jaksa, dan hakim. Keempat, pembentukan *Digital Evidence Review Board* atau panel independen yang dapat diakses oleh terdakwa untuk memverifikasi keabsahan bukti digital dapat menjadi solusi untuk menjamin *fair trial* dan menghindari digital *evidence fabrication* (Kusumawardhani, 2024).

F. KESIMPULAN

Kedudukan bukti digital dalam sistem peradilan pidana Indonesia telah diakui secara formil melalui Pasal 5 UU ITE sebagai perluasan dari alat bukti yang sah dalam KUHAP. Ini adalah lompatan besar yang memungkinkan penegakan hukum menjangkau kejahatan di era digital. Namun, kekuatan pembuktian bukti digital masih sangat bergantung pada pemenuhan syarat materiil, khususnya integritas dan keaslian, yang diukur melalui standar *chain of custody* yang ketat. Menjawab rumusan masalah, tantangan utama terletak pada ketiadaan standar nasional yang baku, keterbatasan SDM dan peralatan forensik, serta masih lemahnya pemahaman aparat penegak hukum tentang karakter unik bukti digital. Akibatnya, terjadi disparitas penerimaan bukti digital di pengadilan, yang menimbulkan ketidakpastian hukum dan ketidakadilan. Studi kasus menegaskan bahwa keberhasilan atau kegagalan pembuktian sangat ditentukan oleh profesionalisme dalam menjaga *chain of custody*.

Rekomendasi yang diajukan adalah: pertama, segera melakukan revisi KUHAP untuk mengintegrasikan bukti digital secara definitif; kedua, menetapkan SOP nasional *chain of custody* bukti digital oleh lembaga terkait; ketiga, membangun laboratorium forensik digital terakreditasi di setiap provinsi dan meningkatkan kapasitas penegak hukum secara berkelanjutan; keempat, memberikan akses bagi pihak terdakwa untuk menguji keabsahan bukti digital melalui panel ahli independen. Hanya dengan fondasi prosedural yang kokoh, bukti digital dapat menjadi pilar keadilan yang andal, bukan sekadar fragmen digital yang rentan dipatahkan.

REFERENSI:

Brenner, S. W. (2022). Cybercrime: Criminal Threats from Cyberspace (2nd ed.). Praeger.

Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd ed.). Academic Press.

Kusumawardhani, A. (2024). Rekonsepsi Chain of Custody dalam Bukti Digital di Indonesia. Jurnal Hukum Siber, 6(1), 15–32.

Prasetyo, B. (2024). Bukti Digital dan Hak atas Fair Trial. Jurnal Hukum dan Masyarakat, 16(1), 88–107.

Putusan Mahkamah Agung Nomor 661 K/Pid.Sus/2019.

Putusan Mahkamah Agung Nomor 1089 K/Pid.Sus/2018.

Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016.

Santoso, L. (2023). Chain of Custody Bukti Digital dalam Sistem Peradilan Pidana Indonesia. Jurnal Yudisial, 16(3), 301–322. https://doi.org/10.29123/jy.v16i3.542

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang

Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Tahun 2024 Nomor 1, Tambahan Lembaran Negara Nomor 6905).

Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (Lembaran Negara Tahun 1981 Nomor 76, Tambahan Lembaran Negara Nomor 3209).