

PENGAKSESAN AKUN CLOUD COMPUTING OLEH APARAT PENEGAK HUKUM: ANALISIS TERHADAP KEABSAHAN ALAT BUKTI ELEKTRONIK

Access to Cloud Computing Accounts by Law Enforcement Officials: An Analysis of the Admissibility of Electronic Evidence

Asaad Ahmad

UIN Sunan Gunung Djati,
Indonesia

*email: asaad36@gmail.com

Lisensi:CC-BY 

Abstrak

Perkembangan teknologi *cloud computing* memicu transformasi radikal dalam modus operandi kejahatan siber (*cybercrime*), yang menuntut kesiapan aparat penegak hukum dalam pengumpulan alat bukti digital. Namun, karakteristik data *cloud* yang bersifat virtual dan lintas batas yurisdiksi sering kali melahirkan benturan hukum. Penelitian ini bertujuan untuk menganalisis aspek hukum pengaksesan akun *cloud computing* oleh aparat penegak hukum berdasarkan regulasi di Indonesia (UU ITE dan UU PDP) dibandingkan dengan sistem *common law* (ECPA dan CLOUD Act), serta menguji validitas dokumen elektronik yang diperoleh di luar prosedur hukum acara formal. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan deskriptif analitis, menggunakan data sekunder yang bersumber dari bahan kepustakaan. Hasil penelitian menunjukkan bahwa pengaksesan akun *cloud computing* oleh penyidik di Indonesia tunduk pada pembatasan ketat Pasal 30 jo. Pasal 43 UU ITE (Undang-Undang Nomor 1 Tahun 2024) serta rezim perlindungan privasi dalam UU Perlindungan Data Pribadi (Undang-Undang Nomor 27 Tahun 2022) yang mewajibkan adanya izin atau penetapan pengadilan (*due process of law*). Sementara dalam sistem *common law* di Amerika Serikat, kakunya aturan *Electronic Communications Privacy Act* (ECPA) kini telah dijembatani oleh CLOUD Act melalui skema perjanjian bilateral internasional. Konsekuensi yuridis terhadap dokumen elektronik hasil pengaksesan akun *cloud* yang dilakukan tidak sesuai prosedur (*unlawful search and seizure*) adalah cacat hukum. Berdasarkan doktrin *fruit of the poisonous tree* (*the exclusionary rule*), alat bukti tersebut kehilangan kekuatan pembuktian (*bewijs kracht*) dan dinyatakan tidak sah atau tidak dapat diterima (*inadmissible evidence*) demi hukum di persidangan.

Kata Kunci:

Cloud Computing, Alat Bukti Elektronik, Penegakan Hukum, Keabsahan Pembuktian

Keywords:

Cloud Computing, Electronic Evidence, Law Enforcement, Admissibility.

Abstract

The development of cloud computing technology has triggered a radical transformation in the modus operandi of cybercrime, demanding the readiness of law enforcement agencies in collecting digital evidence. However, the virtual and cross-border nature of cloud data frequently leads to legal conflicts. This study aims to analyze the legal aspects of accessing cloud computing accounts by law enforcement officers under Indonesian regulations (UU ITE and UU PDP) compared to the common law system (ECPA and CLOUD Act), as well as to evaluate the validity of electronic documents obtained outside formal procedural law. The research method applied is normative legal research with a descriptive-analytical approach, utilizing secondary data sourced from literature studies. The results indicate that accessing cloud computing accounts by investigators in Indonesia is strictly limited by Article 30 jo. Article 43 of the ITE Law (Law No. 1 of 2024) and the privacy protection regime under the Personal Data Protection Law (Law No. 27 of 2022), which mandate judicial authorization or warrants (*due process of law*). Meanwhile, in the United States common law system, the rigid restrictions of the Electronic Communications Privacy Act (ECPA) have now been bridged by the CLOUD Act through international bilateral agreement frameworks. The juridical consequence of electronic documents obtained from cloud account access that violates formal procedures (*unlawful search and seizure*) is that they are legally flawed. Based on the fruit of the poisonous tree doctrine (*the exclusionary rule*), such evidence loses its probative value (*bewijs kracht*) and must be declared legally invalid or inadmissible in court.

Submit Tgl.: 19-Juli-2026

Diterima Tgl.: 23-Juli-2026

Diterbitkan Tgl.: 25-Juli-2026

PENDAHULUAN

Cloud computing menandai era baru dalam industri telekomunikasi. Konsep ini telah diperkenalkan sejak tahun 1960-an oleh John McCarthy yang memprediksi bahwa komputasi akan menjadi infrastruktur publik seperti listrik dan telepon (Anggerian et al., n.d.). Pada tahun 1995, Larry Ellison, pendiri Oracle, memperkenalkan konsep network computing sebagai alternatif terhadap dominasi desktop computing. Konsep ini menekankan bahwa pengguna tidak perlu menginstal berbagai perangkat lunak pada komputer karena layanan komputasi dapat disediakan melalui jaringan (Anggerian et al., n.d.).

Cloud computing merupakan teknologi komputasi yang memanfaatkan internet untuk menyediakan perangkat lunak dan infrastruktur sebagai layanan (Afrianto, 2011). Cloud computing merupakan model layanan teknologi informasi yang memanfaatkan internet untuk menyediakan sumber daya komputasi secara fleksibel dan efisien.

Di samping berbagai manfaatnya, penggunaan cloud computing juga berpotensi menimbulkan penyalahgunaan yang memicu meningkatnya kejahatan siber (cybercrime). Peraturan perundang-undangan konvensional pada dasarnya mengatur tindak pidana seperti penipuan, pencurian, dan perusakan yang dilakukan secara langsung, sehingga belum sepenuhnya mengakomodasi karakteristik kejahatan siber (Soepratomo, 2001).

Perkembangan teknologi internet telah mendorong munculnya kejahatan siber melalui penggunaan komputer dan sistem telekomunikasi. Dalam konteks ini, internet menjadi infrastruktur utama yang memungkinkan penyelenggaraan cloud computing (Afrianto, 2011). Penggunaan cloud computing menimbulkan persoalan hukum terkait perlindungan privasi, mengingat data pengguna berada dalam penguasaan penyedia layanan yang berkewajiban menjamin keamanannya (Santoso, n.d.).

Menurut Shinta Dewi, informasi pribadi merupakan informasi yang berada di bawah kendali individu, sehingga setiap orang berhak membatasi akses dan penyebarannya kepada pihak lain (Dewi, 2009). Penyedia layanan cloud computing berkewajiban menjamin keamanan dan kerahasiaan informasi pribadi pengguna.

Dalam konteks hukum pidana, pembuktian merupakan fase krusial di persidangan. Pasal 191 ayat (1) Kitab Undang-Undang Hukum Acara Pidana (KUHAP) menegaskan bahwa apabila kesalahan terdakwa tidak terbukti secara sah dan meyakinkan, maka ia harus dibebaskan. Sebaliknya, kesalahan terdakwa harus didasarkan pada alat-alat bukti yang sah menurut ketentuan Pasal 184 KUHAP agar hakim dapat menjatuhkan pidana sesuai Pasal 193 ayat (1) KUHAP. Oleh karena itu, hakim dituntut untuk sangat cermat dan hati-hati dalam menilai batas minimum kekuatan pembuktian (bewijskracht) dari setiap alat bukti (Alfitra, 2011).

Eksistensi alat bukti elektronik atau digital sendiri telah diakui keabsahannya dalam hukum acara Indonesia melalui perluasan Pasal 184 KUHAP oleh Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 (UU ITE). Namun, tantangan nyata muncul ketika aparat penegak hukum berusaha mendapatkan dokumen elektronik yang tersimpan di dalam akun cloud computing. Tindakan mengakses sistem komputer atau akun cloud diatur dalam Pasal 30 UU ITE. Masalahnya, mayoritas penyedia layanan cloud raksasa (seperti Google, AWS, atau Microsoft) merupakan korporasi asing yang berdomisili di Amerika Serikat dan tunduk pada Electronic Communication Privacy Act (ECPA). Berdasarkan ECPA, penyedia layanan dilarang keras memberikan akses data pengguna kepada siapapun, termasuk penegak hukum asing, demi alasan privasi. Meskipun kini terdapat mekanisme Clarifying Lawful Overseas Use of Data Act (CLOUD Act) di AS yang

membuka ruang kerja sama lintas batas, benturan yurisdiksi dan prosedur birokrasi penegakan hukum antarnegara kerap kali masih menemui jalan buntu.

Kondisi tersebut seringkali mendorong penyidik di lapangan melakukan tindakan pengaksesan akun cloud computing secara langsung tanpa persetujuan tertulis (consent) dari pemilik akun atau tanpa melalui prosedur kerja sama internasional resmi (Mutual Legal Assistance). Jika pengaksesan akun tersebut dilakukan dengan melangkahi prosedur hukum formal (due process of law), tindakan tersebut berpotensi dikategorikan sebagai pengaksesan ilegal (illegal access). Konsekuensinya, keabsahan (admissibility) dokumen elektronik yang diperoleh sebagai alat bukti di persidangan akan dipertanyakan dan rentan dinyatakan tidak sah (inadmissible evidence) berdasarkan doktrin hukum fruit of the poisonous tree.

Oleh karena itu, diperlukan penelitian mendalam untuk mengevaluasi validitas tindakan pengaksesan akun komputasi awan oleh penegak hukum. Berdasarkan latar belakang di atas, rumusan masalah dalam penelitian ini adalah:

Pertama, bagaimanakah aspek hukum pengaksesan akun cloud computing oleh aparat penegak hukum berdasarkan peraturan perundang-undangan di Indonesia (UU ITE dan UU PDP) dibandingkan dengan sistem hukum common law (ECPA dan CLOUD Act)? Kedua, apakah dokumen elektronik hasil pengaksesan akun cloud computing dalam proses penyidikan yang tidak sesuai prosedur dapat digunakan sebagai alat bukti yang sah untuk pembuktian di pengadilan?

Sejalan dengan rumusan masalah tersebut, tujuan penelitian ini adalah: pertama, untuk menganalisis aspek hukum pengaksesan akun cloud computing dalam koridor hukum Indonesia dan common law system. Kedua, untuk menguji dan mengevaluasi keabsahan hasil pengaksesan akun cloud computing dalam proses pembuktian pidana.

Penelitian ini diharapkan dapat memberikan kontribusi teoretis bagi perkembangan ilmu hukum, khususnya hukum norma siber (cyber law) dan hukum pembuktian elektronik. Secara praktis, tulisan ini diharapkan dapat menjadi panduan akurat bagi aparat penegak hukum, praktisi, akademisi, serta pemerintah dalam merumuskan standarisasi regulasi mengenai tata cara penggeledahan dan penyitaan aset digital berbasis cloud.

Kajian Teori

Menurut Mochtar Kusumaatmadja, ketertiban adalah tujuan pokok dan pertama dari hukum, yang disusul oleh tercapainya keadilan yang ukurannya dinamis mengikuti masyarakat dan zamannya (Salman & Damian, 2011). Untuk mewujudkan ketertiban dan kepastian hukum sebagai syarat mutlak organisasi hidup manusia, dibentuklah lembaga-lembaga hukum (Salman & Damian, 2011). Hukum itu sendiri diartikan sebagai keseluruhan kaidah, asas, lembaga, dan proses yang mengatur serta memelihara ketertiban dalam pergaulan hidup masyarakat (Indah et al., 2005).

Dalam ranah hukum publik, ketentuan hukum pidana material (tentang delik, pelaku, dan sanksi) memerlukan hukum pidana formal (hukum acara) agar dapat diterapkan secara nyata; tanpa hukum acara, hukum material kehilangan kemanfaatannya (Sunaryo & Dianawati, 2009). Pintu gerbang penegakan hukum ini dimulai dari penyelidikan, yaitu tindakan mencari dan menemukan peristiwa pidana (Harahap, 2008; Ramelan, 2006) sekaligus persiapan penindakan (Ramelan, 2006) serta penyidikan, yakni tindakan pejabat berwenang (Polri dan PPNS) (Hamzah, 2008) mencari dan mengumpulkan bukti guna membuat terang tindak pidana dan menemukan tersangkanya (Harahap, 2008). Ketentuan prosedural di dalam KUHAP ini secara *mutatis mutandis* juga berlaku penuh terhadap penanganan perkara pidana siber dalam rezim UU ITE.

Fase paling esensial dalam menentukan nasib terdakwa demi mencari kebenaran materiil di persidangan adalah hukum pembuktian (Alfitra, 2011; Makarim, 2003). Sudikno Mertokusumo membagi pengertian membuktikan ke dalam tiga arti: Pertama, logis yakni memberikan kepastian mutlak tanpa bukti lawan. Kedua, konvensional yakni memberikan kepastian nisbi berdasarkan perasaan (*conviction intime*) maupun akal (*conviction raisonnée*). Ketiga, yuridis yakni memberikan dasar cukup bagi hakim untuk memperoleh kepastian tentang kebenaran peristiwa (Mertokusumo, 2006).

Dalam sistem peradilan siber, UU ITE telah memperluas ketentuan Pasal 184 KUHAP dengan melegitimasi Informasi dan/atau Dokumen Elektronik sebagai alat bukti yang sah (Pasal 5 dan 6 UU ITE), sepanjang pemanfaatannya memenuhi persyaratan formil dan materiil perundang-undangan (Pasal 7 UU ITE). Secara praktis, alat bukti elektronik diakomodasi ke dalam dua bentuk, yaitu: Bukti surat apabila informasi/dokumen elektronik tersebut telah dialihwujudkan ke dalam bentuk cetak (*print-out*). Atau bukti petunjuk apabila informasi/dokumen elektronik tersebut memiliki keterkaitan linier dengan alat bukti sah lainnya berdasarkan penilaian dan keyakinan hakim.

Cloud computing pada dasarnya merupakan sebuah Sistem Elektronik yakni serangkaian perangkat dan prosedur elektronik yang mengolah hingga menyebarkan informasi elektronik (Budhijanto, 2010). Sebagai media penyimpanan data, cloud computing memanfaatkan virtualisasi server pada pihak ketiga secara dinamis lintas batas (*cross border*), sehingga lokasi fisiknya dapat berubah sewaktu-waktu meskipun secara virtual terlihat statis oleh pengguna.

Untuk memperoleh dokumen elektronik di dalam cloud sebagai alat bukti, penegak hukum wajib memiliki akses legal ke akun tersebut. Namun, Pasal 30 UU ITE secara tegas melarang tindakan pengaksesan komputer atau sistem elektronik tanpa hak (*illegal access*), yang dikategorikan sebagai kejahatan penyusupan kode akses (Widodo, 2013; Rahardjo, 2002).

Lebih lanjut, kewenangan penegakan hukum dipagari oleh kewajiban melindungi hak privasi (Pasal 43 ayat (2) UU ITE). Perlindungan privasi atas data yang tersimpan di dalam cloud saat ini diperketat secara rigid oleh Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) (Undang-Undang Nomor 27 Tahun 2022), yang menempatkan data pribadi dalam cloud sebagai objek terlindung yang pengaksesannya oleh penegak hukum harus tunduk pada asas *due process of law* agar validitas alat bukti yang dihasilkan tidak gugur di pengadilan.

Metode Penelitian

Penelitian ini menggunakan metode yuridis normatif dengan pendekatan deskriptif analitis. Data yang digunakan berupa data sekunder yang diperoleh melalui studi kepustakaan terhadap peraturan perundang-undangan, literatur, dan hasil penelitian yang relevan. Seluruh data dianalisis secara kualitatif untuk memperoleh kesimpulan mengenai permasalahan hukum yang diteliti.

HASIL DAN PEMBAHASAN

1. Aspek Hukum Pengaksesan Akun *Cloud Computing* oleh Aparat Penegak Hukum: Analisis Komparatif Regulasi Indonesia dan *Common Law System*

Cloud computing secara teknis merupakan sebuah sistem elektronik penyimpanan data berbasis server virtual yang dikelola oleh pihak ketiga. Untuk memperoleh barang bukti digital yang tersimpan di dalamnya, aparat penegak hukum lazimnya menggunakan dua metode pendekatan akses yaitu: Pertama, Akses Logikal (*Logical Access*) yakni pengaksesan

menggunakan identitas akun berupa *username* dan *password* melalui jaringan. Kedua, Akses Fisik (*Physical Access*) yakni pengaksesan infrastruktur keras penyimpanan data melalui kolaborasi langsung dengan administrator sistem penyedia layanan.

Dalam sistem hukum Indonesia, tindakan pengaksesan akun *cloud computing* oleh penyidik harus diletakkan dalam koridor hukum positif secara ketat agar tidak dikategorikan sebagai akses ilegal (*illegal access*). Secara umum, Pasal 30 UU ITE melarang setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun. UU ITE tidak memberikan pengecualian eksplisit terhadap larangan pengaksesan ini untuk kepentingan penegakan hukum (berbeda dengan tindakan penyadapan atau intersepsi yang dikecualikan untuk penegakan hukum berdasarkan perintah undang-undang).

Oleh karena itu, argumen praktis kepolisian bahwa pengaksesan data untuk tujuan penegakan hukum secara otomatis menggugurkan unsur "ilegal" harus dinilai secara hati-hati (**Widodo, 2013**). Demi menjamin legalitas tindakan tersebut, penyidik wajib memenuhi rambu-rambu Pasal 43 ayat (2) UU ITE (sebagaimana telah diubah dengan UU No. 1/2024), yang mengamanatkan bahwa proses penyidikan dan pengumpulan alat bukti elektronik wajib memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, dan integritas data (*chain of custody*). Rambu privasi ini kini diperkuat secara fundamental oleh Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Berdasarkan UU PDP, data pribadi yang tersimpan di dalam akun *cloud* merupakan objek terlindungi. Meskipun Pasal 50 UU PDP mengecualikan kewajiban pemrosesan data pribadi untuk kepentingan penegakan hukum, pengecualian tersebut tetap wajib dilaksanakan melalui prosedur hukum acara yang sah (*due process of law*) melalui penetapan penyitaan oleh pengadilan.

Perbandingan mendasar terlihat pada sistem *common law* di Amerika Serikat. Perlindungan privasi data *cloud* awalnya diproteksi secara kaku oleh *Electronic Communications Privacy Act* (ECPA). Hambatan yurisdiksi perlindungan ini terlihat jelas dalam kasus *Suzlon Energy Ltd. v. Microsoft Corp.*, di mana Pengadilan Federal AS menolak permohonan penyerahan data surel yang dikuasai Microsoft meskipun objek hukumnya berada di luar negeri (Australia), atas dasar bahwa ECPA melindungi data setiap pengguna terlepas dari status kewarganegaraannya (***Suzlon Energy Ltd. v. Microsoft Corp.*, 2011**).

Namun, guna menjembatani kebuntuan penegakan hukum transnasional di era *borderless* ini, sistem *common law* di AS kini mengadopsi *CLOUD Act* (*Clarifying Lawful Overseas Use of Data Act*). Melalui *CLOUD Act*, penyedia layanan komputasi awan yang berbasis di AS dapat diwajibkan untuk memberikan data pengguna kepada penegak hukum asing, asalkan terdapat perjanjian bilateral resmi (*Executive Agreement*) antar negara. Hambatan terbesar di Indonesia saat ini adalah belum adanya undang-undang spesifik setingkat UU yang mengatur mekanisme penggeledahan dan penyitaan digital terhadap data *cloud*, serta belum adanya perjanjian kerja sama di bawah kerangka *CLOUD Act* dengan negara-negara domisili *vendor* utama komputasi awan.

2. Validitas Dokumen Elektronik Hasil Pengaksesan Akun Cloud Computing Tanpa Prosedur sebagai Alat Bukti yang Sah di Persidangan

Dalam hukum acara pidana, proses pembuktian di persidangan merupakan fase esensial untuk memperoleh kebenaran materiil guna menentukan bersalah atau tidaknya terdakwa. Untuk meyakinkan hakim berdasarkan teori

pembuktian undang-undang secara negatif (*negatief wettelijk bewijstheorie*) yang dianut di Indonesia, keabsahan alat bukti yang dihadirkan di persidangan bersifat mutlak.

Eksistensi alat bukti elektronik diatur melalui perluasan alat bukti dalam Pasal 5 ayat (1) dan (2) UU ITE, yang membaginya menjadi: Pertama, Informasi dan/atau Dokumen Elektronik: Berdiri sebagai alat bukti mandiri (perluasan alat bukti). Kedua, Hasil Cetak (*print out*): Berfungsi sebagai alat bukti surat sebagaimana diatur dalam KUHAP.

Agar memiliki nilai kekuatan pembuktian (*bewijskracht*), bukti elektronik wajib memenuhi dua syarat kumulatif yang diatur dalam Pasal 5 ayat (3) dan Pasal 6 UU ITE: Pertama, Syarat Formil: Sistem elektronik yang digunakan harus sesuai dengan ketentuan UU ITE (andal, aman, dan beroperasi sebagaimana mestinya). Kedua, Syarat Materiil: Informasi di dalamnya harus dapat diakses, ditampilkan, dijamin keutuhannya (*integrity*), dan dapat dipertanggungjawabkan (*reliability*) sehingga mampu menerangkan suatu keadaan.

Apabila penyidik memperoleh dokumen elektronik dari akun *cloud computing* melalui tindakan pengaksesan yang tidak sah seperti tanpa izin pemilik, tanpa penetapan pengadilan, atau melompati prosedur forensik standar maka dokumen tersebut tidak memenuhi syarat materiil keutuhan (*integrity*) karena mata rantai penjagaan bukti (*chain of custody*) telah terputus. Tindakan penyitaan digital yang melanggar prosedur formal hukum acara dikategorikan sebagai tindakan yang tidak sah (*unlawful search and seizure*).

Dalam praktik peradilan di Indonesia, konsekuensi yuridis terhadap alat bukti yang diperoleh secara tidak sah ini dinilai sangat *rigid* oleh hakim. Apabila suatu alat bukti elektronik diperoleh secara tidak sah, maka alat bukti tersebut tidak dapat dipertimbangkan oleh hakim dalam menjatuhkan putusan. Prinsip moralitas hukum menegaskan bahwa hakim tidak mungkin menegakkan hukum dengan cara melanggar hukum (*the exclusionary rule* atau doktrin *fruit of the poisonous tree*).

Hal ini tecermin secara implisit dalam analisis kasus *PT Riau Andalan Pulp and Paper (RAPP) v. Richard Constantine van Lee* di Pengadilan Negeri Pangkalan Kerinci (**Widodo, 2013; Putusan Pengadilan Negeri Pelalawan Nomor 182/Pid.B/2011/PN.PLW, 2011; Putusan Pengadilan Tinggi Pekanbaru Nomor 06/PID/2012/PT.PBR, 2012**). Terdakwa dituntut atas tindakan menyalin dan mengirim data riset perusahaan ke surel pribadinya (melanggar Pasal 32 ayat (1) UU ITE). Namun, pada tingkat banding, hukuman terdakwa diperingan karena di dalam berkas persidangan tidak ditemukan bukti dokumen yang menunjukkan bahwa penyidik melakukan pengaksesan resmi terhadap akun surel terdakwa maupun perusahaan untuk membuktikan pengiriman data tersebut. Ketiadaan akses legal dan forensik yang valid membuat hakim ragu dan menyatakan terdakwa tidak terbukti mentransfer data ke pihak luar dengan niat jahat.

Dengan demikian, dokumen elektronik hasil pengaksesan akun *cloud computing* dalam proses penyidikan yang dilakukan tidak sesuai prosedur (tanpa hak atau melanggar *due process of law*) tidak dapat digunakan sebagai alat bukti yang sah untuk pembuktian di pengadilan. Dokumen tersebut kehilangan legitimasi hukumnya, tidak memiliki nilai kekuatan mengikat, dan wajib dikesampingkan oleh Majelis Hakim demi hukum.

KESIMPULAN

Pertama, di Indonesia, pengaksesan akun komputasi awan oleh aparat penegak hukum secara normatif dibatasi oleh koridor Pasal 30 jo. Pasal 43 UU ITE (Undang-Undang Nomor 1 Tahun 2024) serta rezim perlindungan privasi

dalam UU Perlindungan Data Pribadi (UU Nomor 27 Tahun 2022). Tindakan penyidikan wajib menjunjung tinggi asas *due process of law* agar tidak dikategorikan sebagai akses ilegal (*illegal access*). Sementara itu, dalam sistem *common law* (Amerika Serikat), batasan kaku kerahasiaan data yang semula diproteksi oleh *Electronic Communications Privacy Act* (ECPA) kini telah diakomodasi untuk kepentingan penegakan hukum transnasional melalui instrumen CLOUD Act guna mempercepat birokrasi lintas batas negara. Kendati demikian, akibat belum adanya harmonisasi regulasi di Indonesia, penyidik di lapangan sering mengambil jalan pintas dengan memanfaatkan perangkat yang telah masuk log (*logged in*) milik tersangka secara sepihak, yang rentan melanggar hak privasi dan yurisdiksi.

Kedua, dokumen elektronik hasil pengaksesan akun *cloud computing* yang diperoleh tidak sesuai prosedur (tanpa penetapan pengadilan atau melanggar protokol *digital forensics*) tidak dapat digunakan sebagai alat bukti yang sah di persidangan. Sesuai dengan Pasal 5, 6, dan 7 UU ITE, alat bukti elektronik harus dijamin aksesibilitas, keandalan, keutuhan (*integrity*), dan dapat dipertanggungjawabkan (*chain of custody*). Pengoleksian bukti yang dilakukan secara melawan hukum (*unlawful search and seizure*) akan mengakibatkan alat bukti tersebut cacat hukum berdasarkan doktrin *fruit of the poisonous tree* (*the exclusionary rule*). Dokumen tersebut kehilangan kekuatan pembuktian (*bewijs kracht*) dan wajib dikesampingkan oleh hakim demi tegaknya keadilan materiil.

REFERENSI

Sumber Buku

- Agus Rahardjo. (2002). *Cybercrime: Pemahaman dan upaya pencegahan kejahatan berteknologi*. Citra Aditya Bakti.
- Alfitra. (2011). *Hukum pembuktian dalam beracara pidana, perdata dan korupsi di Indonesia*. Raih Asa Sukses.
- Andi Hamzah. (2008). *Hukum acara pidana Indonesia*. Sinar Grafika.
- Danrivanto Budhijanto. (2010). *Hukum telekomunikasi, penyiaran, dan teknologi informasi: Regulasi dan konvergensi*. Refika Aditama.
- Edmon Makarim. (2003). *Kompilasi hukum telematika*. RajaGrafindo Persada.
- M. Yahya Harahap. (2008). *Pembahasan permasalahan dan penerapan KUHP: Penyidikan dan penuntutan*. Sinar Grafika.
- Ninie Suparni. (2009). *Cyberspace: Problematika dan antisipasi pengaturannya*. Sinar Grafika.
- Otje Salman, & Eddy Damian. (Eds.). (2011). *Konsep-konsep hukum dalam pembangunan: Kumpulan karya tulis Prof. Dr. Mochtar Kusumaatmadja, S.H., LL.M. PT. Alumni*.
- Ramelan. (2006). *Hukum acara pidana: Teori dan implementasi*. Sumber Ilmu Jaya.
- Shinta Dewi. (2009). *Cyberlaw: Perlindungan privasi atas informasi pribadi dalam e-commerce menurut hukum internasional*. Widya Padjajaran.
- Sri Untari Indah, dkk. (2005). *Pengantar hukum Indonesia*. Fakultas Hukum Universitas Trisakti.
- Sudikno Mertokusumo. (2006). *Hukum acara perdata Indonesia*. Liberty.
- Sunaryo, & Ajen Dianawati. (2009). *Tanya jawab seputar hukum acara pidana*. Visimedia.
- Widodo. (2013). *Hukum pidana di bidang teknologi informasi (Cybercrime law): Telaah teoritik dan bedah kasus*. Aswaja.

Sumber Lain

Berkah I. Santoso. (t.t.). *Cloud computing dan strategi IT modern*. <http://www.cloudindonesia.org/>

Heru Soeprapto. (2001). Kejahatan komputer dan cyber serta antisipasi pengaturan pencegahannya di Indonesia. *Jurnal Hukum Bisnis*, 12.

Herwin Anggerian, dkk. (t.t.). *Cloud computing*.
<http://lutung.library.ums.ac.id/dokumen/ebooks/Komputer/Cloud%20Computing/Cloud-Computing.pdf>

Irawan Afrianto. (2011). Pengenalan cloud computing. Dalam *Prosiding Seminar IT Cloud Computing: Today Tomorrow*, Bandung.

Justia US Law. (2011). *Case law: 10-35793*. <https://law.justia.com/cases/federal/appellate-courts/ca9/10-35793/10-35793-2011-10-03.html>