Hukum yang Berlaku atas Keabsahan Perolehan Bukti Elektronik Lintas Yurisdiksi dalam KUHAP 2025

Oleh:
Bony Daniel (Hakim PN Serang)

Persoalan bukti elektronik lintas negara sebenarnya dapat dipahami dari contoh sederhana. Penyidik berada di Indonesia, tetapi data yang dibutuhkan tidak selalu berada sepenuhnya dalam sistem Indonesia. Surat elektronik tersangka dapat dikelola oleh perusahaan di Amerika Serikat. Riwayat percakapan dapat berada dalam penguasaan penyedia layanan yang berkedudukan di Irlandia. Catatan transaksi aset kripto dapat dikuasai oleh bursa yang beroperasi dari Singapura. Bahkan satu data yang sama dapat disalin atau disimpan pada beberapa pusat data di negara yang berbeda.

Karena itu, persoalan ini tidak hanya muncul dalam kejahatan siber. Dalam perkara penipuan, perjudian, pencucian uang, korupsi, narkotika, perdagangan orang, dan berbagai tindak pidana lain, bukti yang dibutuhkan penyidik juga dapat berbentuk data elektronik yang berkaitan dengan lebih dari satu negara.

Masalah tersebut sebenarnya sudah lama dikenal dalam praktik penegakan hukum. Yang berubah setelah berlakunya UU 20/2025 adalah cara hukum Indonesia menilai bukti tersebut. Sejak 2 Januari 2026, dengan tetap memperhatikan ketentuan peralihan dalam Pasal 361, KUHAP baru tidak hanya memperhatikan isi alat bukti, tetapi juga cara alat bukti itu diperoleh. Pembahasan dalam tulisan ini karena itu ditujukan pada perkara yang memang tunduk pada UU 20/2025 berdasarkan ketentuan peralihannya.

Perubahan tersebut terlihat dalam Pasal 235. Ketentuan ini menempatkan bukti elektronik sebagai alat bukti dan sekaligus menentukan syarat penggunaannya. Pasal 235 ayat (3) mensyaratkan agar alat bukti dapat dibuktikan autentikasinya dan diperoleh secara tidak melawan hukum. Ayat (4) memberikan kewenangan kepada hakim untuk menilai kedua syarat tersebut. Jika salah satu syarat tidak terpenuhi, ayat (5) menentukan bahwa alat bukti tersebut tidak dapat digunakan dan tidak mempunyai kekuatan pembuktian.

Di sini terdapat 2 persoalan yang harus dibedakan. *Pertama*, apakah data yang diajukan memang asli dan tetap utuh. Ini merupakan persoalan autentikasi. *Kedua*, apakah cara mendapatkan data tersebut dibenarkan oleh hukum. Ini merupakan persoalan keabsahan perolehan. Keduanya tidak selalu menghasilkan jawaban yang sama. Sebuah data dapat terbukti asli, tetapi diperoleh tanpa kewenangan. Sebaliknya, data dapat diperoleh melalui prosedur yang sah, tetapi kemudian tidak dapat dibuktikan bahwa data yang diajukan di persidangan masih sama dengan data yang pertama kali diperoleh.

Kesulitan mulai muncul ketika proses memperoleh data melibatkan negara lain. Pasal 235 memang mensyaratkan agar bukti "diperoleh secara tidak melawan hukum", tetapi tidak menjelaskan hukum mana yang harus digunakan apabila proses perolehannya berkaitan dengan beberapa negara.

Misalnya, penyidik Indonesia meminta data dari penyedia layanan yang berkedudukan di Amerika Serikat, sementara data tersebut disimpan atau diproses di negara lain. Dalam

keadaan seperti itu, apakah keabsahan perolehannya cukup dinilai berdasarkan hukum Indonesia? Apakah harus mengikuti hukum negara tempat penyedia berada? Apakah lokasi *server* yang menentukan? Atau justru hukum yang mengatur pihak yang menyerahkan data?

KUHAP belum memberikan jawaban tegas terhadap pertanyaan tersebut. KUHAP juga belum menjelaskan apakah setiap pelanggaran terhadap hukum negara lain otomatis membuat bukti harus dikesampingkan.

Dengan demikian, persoalan utamanya bukan lagi sekadar apakah bukti elektronik berasal dari luar negeri. Persoalan yang lebih penting adalah hukum mana yang harus digunakan untuk menilai sah atau tidaknya cara memperoleh bukti tersebut, dan bagaimana hasil penilaian itu kemudian diterapkan melalui Pasal 235 KUHAP.

Persoalan akses bukti elektronik lintas batas sendiri sudah lama dibahas.[1] Di Indonesia, Josua Sitompul telah meneliti akses lintas batas terhadap bukti elektronik sebelum KUHAP 2025 lahir. Kajian tersebut menyentuh hukum internasional, hukum acara pidana, kedaulatan, perlindungan data, Budapest Convention, direct cooperation dengan penyedia layanan, serta berbagai persoalan yurisdiksi.[2] Literatur internasional juga telah lama mempersoalkan ketergantungan pada lokasi fisik data. Jennifer Daskal, misalnya, menunjukkan bahwa data digital dapat berpindah, direplikasi, dan diakses dari tempat yang berbeda dengan tempat penyimpanannya.[3] Karena itu, lokasi fisik server tidak selalu mempunyai arti hukum yang sama dengan lokasi benda berwujud.

Literatur kerja sama pidana internasional juga telah mengenal perdebatan antara *locus regit actum* dan *forum regit actum*.[4] Pendekatan pertama menempatkan hukum negara pelaksana sebagai hukum yang mengatur tindakan pembentukan bukti. Pendekatan kedua memberi tempat lebih besar kepada hukum negara peminta agar bukti yang diperoleh dapat digunakan di forum. Perdebatan ini memperlihatkan bahwa hukum yang mengatur lahirnya suatu bukti tidak selalu sama dengan hukum yang menentukan akibat pembuktiannya.

Pada bukti elektronik, masalahnya bahkan lebih kompleks. Penyedia dapat didirikan pada satu negara, menawarkan layanan di negara lain, mempunyai perwakilan di negara ketiga, sedangkan data direplikasi pada pusat data yang tersebar di beberapa yurisdiksi. Dalam keadaan seperti itu, kewajiban penyedia, hukum yang mengatur pengungkapan data, lokasi sistem, dan kewenangan negara peminta dapat saling bertemu. Penentuan hukum

---

[1] Athina Sachoulidou, "Cross-Border Access to Electronic Evidence in Criminal Matters: The New EU Legislation and the Consolidation of a Paradigm Shift in the Area of 'Judicial' Cooperation," *New Journal of European Criminal Law*, June 6, 2024, abstract; Fran Casino et al., "SoK: Cross-Border Criminal Investigations and Digital Evidence," *Journal of Cybersecurity* (2022), abstract; Jennifer C. Daskal, "Unpacking the CLOUD Act" (2018), abstract.

[2] Josua Sitompul, "Developing A Legal Framework of Personal Data Protection in The Indonesian Criminal Procedure Law," *Indonesia Law Review* (2019): abstract and body; Josua Sitompul, "Improving the Role of Experts under Indonesian Criminal Procedure Law: Lessons Learned from the Dutch Legal System," *Indonesia Law Review* (2018): abstract and body; Josua Sitompul, "Cybercrime Regulations in the National Criminal Code," *Indonesia Law Review* (2025), abstract.

[3] Daskal, "Borders and Bits," 2018; Daskal, "Google Inc. v. Equustek Solutions Inc.," *American Journal of International Law* (2018); Jennifer C. Daskal, "Unpacking the CLOUD Act" (2018).

[4] Krisztina Karsai, "Locus/Forum Regit Actum – a Dual Principle in Transnational Criminal Matters," *Hungarian Journal of Legal Studies* (2019); Tadija Bubalović, "A Notion and Forms of International Criminal Justice Assistance with Special Emphasis on Rights of Suspects and the Accused in an Extradition Proceeding" (2015).

hanya berdasarkan tempat *server* berada menjadi terlalu sederhana untuk menggambarkan hubungan hukum yang sebenarnya.

Perkembangan di Uni Eropa menguatkan hal tersebut. Regulation (EU) 2023/1543 membentuk *European Production Order* dan *European Preservation Order*, tetapi regulasi itu tidak berhenti pada persoalan siapa yang dapat diperintah menyerahkan data.[5] Regulasi juga mengantisipasi keadaan ketika kewajiban yang timbul dari perintah tersebut bertentangan dengan hukum negara ketiga. Dengan kata lain, problem *e-evidence* modern bukan sekadar menemukan 1 *applicable law*. Dalam suatu perkara, beberapa hukum dapat sama-sama berlaku, dan kewajibannya tidak selalu dapat dipenuhi bersamaan.[6]

Tulisan ini tidak berangkat dari anggapan bahwa bukti elektronik yang berada di luar negeri merupakan persoalan baru. Demikian pula, pandangan bahwa lokasi *server* bukan satu-satunya dasar untuk menentukan hukum yang berlaku sudah lama dikenal. Persoalan yang menjadi perhatian justru muncul setelah berlakunya UU 20/2025.

Mengapa demikian? Karena setelah KUHAP baru berlaku, terdapat beberapa ketentuan yang harus dibaca bersama. Pasal 124 ayat (4) secara tegas mengatur permohonan penyitaan terhadap benda yang berada di luar negeri. Pada saat yang sama, Pasal 235 ayat (3) sampai dengan ayat (5) mensyaratkan bahwa alat bukti harus diperoleh secara tidak melawan hukum dan memberi akibat apabila syarat tersebut tidak terpenuhi. Sementara itu, apabila tindakan harus dilakukan di negara lain, mekanisme yang tersedia masih terutama mengacu pada UU 1/2006 tentang Bantuan Timbal Balik dalam Masalah Pidana.

Di sinilah persoalan hukumnya muncul. 3 pengaturan tersebut berbicara mengenai hal yang saling berhubungan, tetapi tidak secara langsung menjelaskan bagaimana hubungan di antara ketiganya harus dipahami ketika objek yang dicari adalah bukti elektronik yang melibatkan lebih dari 1 negara.

Karena itu, tulisan ini berusaha membaca Pasal 124 ayat (4), Pasal 235 ayat (3) sampai dengan ayat (5), dan UU 1/2006 dalam satu kerangka. Tujuannya adalah mencari jawaban atas pertanyaan hukum apa yang harus digunakan untuk menentukan sah atau tidaknya cara memperoleh bukti elektronik lintas yurisdiksi setelah KUHAP 2025 menjadikan legalitas perolehan sebagai salah satu syarat penggunaan alat bukti.

---

[5] Athina Sachoulidou, "Cross-Border Access to Electronic Evidence in Criminal Matters: The New EU Legislation and the Consolidation of a Paradigm Shift in the Area of 'Judicial' Cooperation," *New Journal of European Criminal Law* (2024); T. C. Silva and Evandro Piza Duarte, "E-Evidence Regulation 1544/2023 in the European Union: a Paradigm Shift from Judicial to 'Direct' Cooperation," *Observatório de la Economía Latinoamericana* (2025); Hanna Kuczyńska, "The EU E-Evidence Package from the Polish Perspective: High Time for a Systemic Change," *Studia Iuridica Lublinensia* (2024); Andor Gál, "New Area of Judicial Cooperation on Criminal Matters in the European Union: The Transmission of Electronic Evidence between Member States," *Studia Iuridica Lublinensia* (2024).

[6] M. Cole and T. Quintel, "Transborder Access to e-Evidence by Law Enforcement Agencies: A First Comparative View on the Commission's Proposal for a Regulation on a European Preservation/Production Order and Accompanying Directive," SSRN (2018); S. Tosza, "All Evidence Is Equal, but Electronic Evidence Is More Equal than Any Other: The Relationship between the European Investigation Order and the European Production Order," *New Journal of European Criminal Law* (2020); Jorge A. Espina Ramos, "European Preservation and Production Orders: A Non-Exclusive Approach to E-Evidence within the EU," *eucrim* (2025); Adam Juszczak and Elisa Sason, "The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice: An Introduction to the New EU Package on E-Evidence," *eucrim* (2023); Vanessa Franssen, "The European Commission's E-Evidence Proposal: Toward an EU-Wide Obligation for Service Providers to Cooperate with Law Enforcement?" *European Law Blog* (2018)

Dari persoalan tersebut, ada 3 pertanyaan yang perlu dijawab. *Pertama*, hukum mana yang harus digunakan untuk menilai sah atau tidaknya cara memperoleh bukti elektronik apabila prosesnya berkaitan dengan lebih dari satu negara. *Kedua*, apa yang harus dilakukan jika 2 atau lebih hukum sama-sama berlaku, tetapi kewajiban yang diatur di dalamnya saling bertentangan. *Ketiga*, kapan pelanggaran terhadap hukum negara lain dapat dinilai sebagai perolehan bukti secara melawan hukum dalam pengertian Pasal 235 KUHAP.

Istilah hukum yang digunakan dalam tulisan ini tidak dimaksudkan sebagai pilihan hukum dalam hubungan keperdataan. Persoalannya lebih sederhana. Yang dicari adalah hukum yang menentukan siapa yang berwenang melakukan suatu tindakan, siapa yang berwenang menyerahkan data, dan bagaimana bukti tersebut boleh diperoleh.

Karena 1 proses memperoleh bukti elektronik dapat melibatkan beberapa negara, tidak setiap hukum yang mempunyai hubungan dengan data otomatis berlaku. Harus dilihat terlebih dahulu hubungan nyata antara hukum tersebut dengan pihak atau tindakan yang sedang diperiksa.

Tulisan ini didasarkan pada penelitian yang dilakukan secara doktrinal dengan menggunakan pendekatan peraturan perundang-undangan, konsep hukum, putusan, dan perbandingan. Bahan hukum yang digunakan antara lain UU 20/2025, UU 1/2006, Putusan MK Nomor 20/PUU-XIV/2016, SEMA 1/1985, *Budapest Convention*, dan *United Nations Convention against Cybercrime*. Instrumen asing digunakan sebagai pembanding untuk melihat bagaimana persoalan yang sama diperlakukan dalam sistem hukum lain.

Cara membacanya harus dimulai dengan memisahkan fungsi setiap aturan. Tidak semua aturan menjawab pertanyaan yang sama. Ada aturan yang menentukan apakah aparat Indonesia berwenang melakukan suatu tindakan. Ada aturan yang menentukan bagaimana tindakan dilakukan di negara lain. Ada pula aturan yang menentukan apakah hasil tindakan tersebut akhirnya dapat digunakan sebagai alat bukti di pengadilan Indonesia.

Misalnya, penyidik Indonesia membutuhkan data yang berada di luar negeri. Pertanyaan pertama adalah apakah penyidik mempunyai dasar menurut hukum Indonesia untuk meminta atau melakukan tindakan tersebut. Pertanyaan berikutnya adalah hukum apa yang mengatur pelaksanaan tindakan di negara tempat data diperoleh. Setelah itu baru muncul pertanyaan terakhir, yaitu apakah hasil yang diperoleh dapat digunakan sebagai alat bukti menurut KUHAP.

Dengan demikian, 1 proses memperoleh bukti dapat berhubungan dengan beberapa sistem hukum sekaligus. Namun masing-masing hukum dapat mempunyai fungsi yang berbeda.

Pasal 124 ayat (4) memberi contoh yang cukup jelas. Pasal tersebut menggunakan tempat keberadaan benda untuk menentukan pengadilan yang berwenang memberikan izin penyitaan. Jika benda berada di luar negeri, permohonan tersebut menjadi kewenangan PN Jakarta Pusat.

Namun kewenangan PN Jakarta Pusat harus dibaca secara tepat. Pasal 124 ayat (4) menentukan pengadilan Indonesia yang berwenang memberikan izin. Ketentuan itu tidak menyatakan bahwa setelah izin diberikan, penyidik Indonesia kemudian boleh datang atau masuk ke wilayah negara lain dan melakukan penyitaan sendiri.

Perbedaannya dapat dijelaskan dengan sederhana. PN Jakarta Pusat berwenang memberi penilaian dari sisi hukum Indonesia. Tetapi pelaksanaan tindakan di wilayah negara lain tetap menyangkut kewenangan negara tersebut.

Jadi, izin dari pengadilan Indonesia tidak dengan sendirinya berubah menjadi kewenangan bagi aparat Indonesia untuk menjalankan tindakan penegakan hukum di luar wilayah Indonesia.

Di sinilah pentingnya membedakan kewenangan menurut hukum Indonesia dan kewenangan untuk melaksanakan tindakan di negara lain. Keduanya saling berhubungan, tetapi bukan hal yang sama.

Perbedaannya penting. Pengadilan Indonesia dapat berwenang menilai dan mengizinkan penyitaan untuk kepentingan perkara di Indonesia, tetapi kewenangan tersebut tidak otomatis memberi aparat Indonesia hak untuk menjalankan tindakan penegakan hukum di negara lain.[7] Dalam hukum internasional dikenal perbedaan antara *prescriptive jurisdiction* dan *enforcement jurisdiction*.[8] Suatu negara dapat mempunyai kewenangan untuk menerapkan hukum pidananya terhadap perkara yang mempunyai hubungan dengan negara lain, tetapi pelaksanaan tindakan seperti penggeledahan atau penyitaan di wilayah negara lain tetap memerlukan dasar hukum tersendiri.

Dengan demikian, penetapan PN Jakarta Pusat berfungsi sebagai bentuk pengawasan yudisial menurut hukum Indonesia. Penetapan tersebut tidak dengan sendirinya mengikat pejabat asing, penyedia layanan yang tunduk pada hukum negara lain, atau menghapus persyaratan hukum yang berlaku di negara tempat penyitaan atau tindakan lain dilaksanakan.

Persoalan berikutnya muncul ketika Pasal 124 ayat (4) dibaca bersama UU 1/2006. Pasal 3 ayat (1) UU tersebut menentukan bahwa bantuan berkaitan dengan penyidikan, penuntutan, dan pemeriksaan di sidang pengadilan dilaksanakan menurut hukum Negara Diminta. Pasal 19 dan Pasal 20 memberi dasar kepada Menteri untuk meminta tindakan yang antara lain dapat berupa penggeledahan dan penyitaan.

Hubungan antara UU 1/2006 dan Pasal 124 ayat (4) KUHAP 2025 sebenarnya dapat dipahami dari pertanyaan sederhana, yaitu jika penyidik Indonesia membutuhkan penyitaan terhadap benda yang berada di luar negeri, apakah cukup menggunakan mekanisme bantuan timbal balik dalam UU 1/2006, atau harus lebih dahulu memperoleh penetapan dari PN Jakarta Pusat?

UU 1/2006 tidak memberikan jawaban tegas terhadap pertanyaan tersebut. UU itu tidak menyatakan bahwa setiap permintaan penyitaan kepada negara asing harus lebih dahulu memperoleh penetapan PN Jakarta Pusat. Sebaliknya, Pasal 124 ayat (4) KUHAP 2025 justru secara khusus menyebut benda yang berada di luar negeri dan memberikan kewenangan kepada PN Jakarta Pusat untuk memeriksa permohonan penyitaannya. Karena itu, hubungan

---

[7] Cédric Ryngaert, "The Concept of Jurisdiction in International Law," in *Research Handbook on Jurisdiction and Immunities in International Law*, ed. Alexander Orakhelashvili (Cheltenham: Edward Elgar, 2015), 58–59; Dan E. Stigall, "Ungoverned Spaces, Transnational Crime, and the Prohibition on Extraterritorial Enforcement Jurisdiction in International Law" (2013), 1–2.

[8] Gleider Hernández, "Jurisdiction," in *International Law* (2019), sec. 8; Cédric Ryngaert, "The Concept of Jurisdiction in International Law," in *Research Handbook on Jurisdiction and Immunities in International Law*, ed. Alexander Orakhelashvili (Cheltenham: Edward Elgar, 2015), 58.

antara kedua undang-undang tersebut masih perlu ditafsirkan.

Ada 2 kemungkinan cara memahami hubungan itu.

Kemungkinan pertama, Pasal 124 ayat (4) dipahami sebagai pengawasan pengadilan dari sisi Indonesia. Artinya, sebelum Indonesia meminta negara lain melakukan penyitaan, terlebih dahulu ada penilaian dari pengadilan Indonesia mengenai perlu atau tidaknya penyitaan tersebut. Setelah penetapan diberikan, penyitaan di negara lain tetap dilakukan oleh pejabat negara yang diminta memberikan bantuan dan mengikuti hukum negara tersebut.

Kemungkinan kedua, UU 1/2006 dipahami sebagai aturan khusus mengenai bantuan kepada dan dari negara lain. Jika cara berpikir ini digunakan, penyitaan terhadap benda di luar negeri pada akhirnya dilakukan oleh pejabat negara asing berdasarkan hukum negara tersebut. Karena itu, dapat muncul pendapat bahwa penetapan PN Jakarta Pusat tidak selalu menjadi syarat sebelum Menteri mengajukan permintaan berdasarkan Pasal 19 atau Pasal 20 UU 1/2006.

Kedua kemungkinan tersebut sama-sama menimbulkan persoalan. Jika Pasal 124 ayat (4) dianggap tidak mempunyai hubungan sama sekali dengan permintaan penyitaan kepada negara asing, muncul pertanyaan mengapa KUHAP 2025 secara khusus menyebut benda yang berada di luar negeri. Namun jika setiap permintaan penyitaan melalui MLA dianggap wajib selalu didahului penetapan PN Jakarta Pusat, kewajiban tersebut seharusnya dinyatakan secara jelas dalam undang-undang.

Karena itu, pemahaman yang lebih dapat digunakan adalah menempatkan Pasal 124 ayat (4) sebagai bentuk kontrol pengadilan menurut hukum Indonesia. Penetapan PN Jakarta Pusat diperlukan untuk menilai penyitaan dari sisi kewenangan hukum Indonesia, sedangkan tindakan penyitaan di negara lain tetap dilaksanakan oleh negara yang diminta memberikan bantuan menurut hukum negara tersebut.

Cara memahami hubungan ini penting karena ada 2 hal yang tidak boleh dicampur. *Pertama*, apakah menurut hukum Indonesia penyitaan tersebut dapat diminta. *Kedua*, apakah menurut hukum negara tempat tindakan dilakukan, penyitaan tersebut dapat dilaksanakan. Keduanya berkaitan, tetapi menjawab pertanyaan yang berbeda.

Masalah kemudian menjadi lebih rumit ketika benda yang hendak diperoleh bukan barang fisik, melainkan data elektronik.

KUHAP 2025 memang telah mengakui bahwa objek pemeriksaan tidak selalu berbentuk benda fisik. Pasal 112 secara tegas menyebut Informasi Elektronik dan Dokumen Elektronik sebagai objek penggeledahan. Selain itu, Pasal 1 angka 35 memasukkan benda berwujud maupun tidak berwujud dalam pengertian penyitaan.

Namun rumusan mengenai penggeledahan dan penyitaan tidak sepenuhnya sama. Pada penggeledahan, Informasi Elektronik dan Dokumen Elektronik disebut secara langsung. Sementara itu, Pasal 123 mengenai penyitaan masih menggunakan istilah benda. Karena itu, ketika yang hendak disita adalah data elektronik, masih diperlukan penafsiran mengenai bagaimana data tersebut ditempatkan sebagai objek penyitaan.

Setelah itu muncul persoalan lain, yaitu lokasi data.

Untuk benda fisik, menentukan lokasi relatif mudah. Sebuah kendaraan dapat berada di Jakarta, Singapura, atau negara lain. Tempat bendanya berada dapat diketahui. Pasal 124

dibangun dengan logika seperti ini, yaitu menentukan kewenangan pengadilan berdasarkan tempat benda berada.

Data elektronik tidak selalu dapat diperlakukan dengan cara yang sama.

1 akun dapat dikelola oleh perusahaan yang didirikan di satu negara, digunakan oleh orang di Indonesia, dilayani melalui infrastruktur di negara lain, dan datanya disimpan atau disalin pada beberapa pusat data sekaligus. Sistem juga dapat memindahkan atau menggandakan data tanpa ada tindakan langsung dari pengguna.

Karena itu, mencari 1 lokasi data sebagai jawaban atas seluruh persoalan hukum dapat menyesatkan. Tempat penyimpanan fisik tetap dapat penting, tetapi tidak selalu menjadi faktor yang paling menentukan.

Dalam kasus tertentu, yang lebih penting justru adalah tempat penyedia layanan berada. Dalam kasus lain, yang perlu dilihat adalah tempat pihak yang diperintahkan menyerahkan data berada. Bisa juga yang lebih menentukan adalah siapa yang secara hukum mempunyai penguasaan atau kendali atas data tersebut.

Jadi, ketika berhadapan dengan bukti elektronik, pertanyaannya tidak cukup hanya "data ini disimpan di mana?". Pertanyaan yang lebih tepat adalah siapa yang menguasai data, siapa yang diminta menyerahkannya, tindakan apa yang dilakukan untuk memperoleh data, dan hukum mana yang mengatur tindakan tersebut.

Perbedaan ini juga terlihat dalam *United Nations Convention against Cybercrime*. Konvensi tersebut belum mengikat Indonesia sehingga hanya digunakan sebagai perbandingan.[9] *Article* 27 mengatur perintah kepada orang atau penyedia layanan yang menguasai data untuk menyerahkannya. Sementara itu, *Article* 28 mengatur penggeledahan atau penyitaan terhadap sistem dan data yang berada dalam wilayah suatu negara.[10] Dengan demikian, hukum yang berlaku dapat berbeda bergantung pada tindakan yang dilakukan.

Kalau kita berbicara mengenai bukti elektronik, persoalan pertama yang harus dipahami adalah bahwa data tidak selalu berada di satu tempat. Penyidik dapat berada di Jakarta, pemilik akun berada di Surabaya, penyedia layanan berkedudukan di Amerika Serikat, sementara data disimpan atau diproses melalui sistem yang tersebar di beberapa negara.

Contoh yang cukup mudah dilihat adalah teknologi *torrent*. Dalam sistem ini, satu *file* tidak selalu diperoleh secara utuh dari satu tempat. *File* tersebut dapat dibagi menjadi beberapa bagian, kemudian setiap bagian diperoleh dari pengguna atau *peer* yang berbeda. Setelah bagian-bagian itu terkumpul, sistem memeriksa dan menyusunnya kembali hingga menjadi satu file yang utuh.

Artinya, ketika sebuah file akhirnya tersimpan secara lengkap pada perangkat penyidik

---

[9] D. D. Shtodina, "United Nations Convention against Cybercrime, 2024 – the Outcome of 'Cyber Compromise'?," *Moscow Journal of International Law*, no. 1 (2025): 95–109; Adrian-Cristian Moise, "Preventing and Combating Cybercrime in Light of the Regulations of the United Nations Convention against Cybercrime," *International Journal of Legal and Social Order* (2026): 94–100.

[10] Decebal Manole Bogdan, "International Judicial Cooperation in the Context of the Adoption in 2024 by the United Nations of the Convention on Cybercrime," *AGORA International Journal of Juridical Sciences* (2025); Adrian-Cristian Moise, "Preventing and Combating Cybercrime in Light of the Regulations of the United Nations Convention against Cybercrime," *International Journal of Legal and Social Order* (2026): 94–100.

di Indonesia, belum tentu seluruh bagian *file* tersebut berasal dari satu lokasi. Sebagian dapat berasal dari satu negara dan bagian lainnya berasal dari negara lain. Contoh ini memperlihatkan mengapa lokasi data elektronik tidak selalu dapat ditentukan dengan cara yang sama seperti lokasi benda fisik.

Karena itu, pertanyaan hukumnya tidak cukup hanya "data ini akhirnya tersimpan di mana?" atau "*server*-nya berada di negara mana?". Yang lebih penting adalah bagaimana data tersebut diperoleh, dari siapa data diperoleh, siapa yang melakukan tindakan untuk mendapatkannya, dasar kewenangan apa yang digunakan, dan hukum mana yang memang mengatur tindakan tersebut.

Dengan cara berpikir seperti ini, hubungan dengan hukum negara lain tidak muncul hanya karena sebagian data secara teknis berada di negara tersebut. Harus dilihat terlebih dahulu apakah hukum negara itu memang mengatur pihak atau tindakan yang menghasilkan bukti.

Dalam mekanisme *Mutual Legal Assistance* atau MLA, persoalan tersebut relatif lebih mudah karena UU 1/2006 sudah memberi petunjuk. Pasal 3 ayat (1) menyatakan bahwa bantuan dilaksanakan menurut hukum Negara Diminta.

Maksudnya sederhana. Jika Indonesia meminta negara lain melakukan penggeledahan, penyitaan, atau tindakan lain untuk memperoleh bukti, maka tindakan yang dilakukan di negara tersebut mengikuti hukum negara yang melaksanakannya. Indonesia meminta bantuan, tetapi pejabat negara yang diminta tetap bekerja berdasarkan hukum negaranya sendiri.

Misalnya, Indonesia meminta Negara A menyita data untuk kepentingan perkara pidana di Indonesia. Pertanyaan apakah pejabat di Negara A berwenang melakukan penyitaan, prosedur apa yang harus digunakan, dan syarat apa yang harus dipenuhi pada dasarnya dinilai berdasarkan hukum Negara A.

Karena itu, jika tindakan tersebut dilakukan oleh pejabat yang sebenarnya tidak berwenang atau dilakukan dengan cara yang bertentangan dengan hukum Negara Diminta, persoalan keabsahan proses memperoleh bukti dapat muncul.

Hubungan ini cukup jelas karena UU 1/2006 sendiri yang menunjuk hukum Negara Diminta. Dalam tulisan ini, hubungan semacam itu disebut *textual bridge*. Istilah tersebut pada dasarnya hanya menjelaskan bahwa ada ketentuan dalam hukum Indonesia yang secara langsung menghubungkan proses perolehan bukti dengan hukum negara lain.

UU 1/2006 juga mengatur apa yang terjadi setelah hasil bantuan diperoleh. Pasal 12 ayat (2) mengatur pernyataan yang diperoleh dari negara asing, sedangkan Pasal 12 ayat (3) mengakui dokumen atau alat bukti lain yang diperoleh melalui permintaan bantuan sebagai alat bukti dalam proses yang berkaitan dengan permintaan tersebut.

Di sini perlu dibedakan fungsi UU 1/2006 dan Pasal 235 KUHAP. Pasal 12 ayat (3) UU 1/2006 menjawab pertanyaan apakah hasil MLA dapat masuk dan digunakan dalam proses pembuktian di Indonesia. Pasal 235 KUHAP menjawab pertanyaan berikutnya, yaitu apakah alat bukti tersebut memenuhi syarat untuk benar-benar digunakan dalam persidangan.

Dengan kata lain, fakta bahwa bukti diperoleh melalui jalur MLA belum otomatis berarti bukti tersebut pasti sah dan dapat langsung digunakan. Hakim tetap harus memeriksa

autentikasinya dan menilai apakah bukti itu diperoleh secara tidak melawan hukum.

Jadi, jalur MLA memang memberi dasar yang lebih jelas mengenai hukum yang mengatur tindakan di negara lain, tetapi MLA tidak menghapus kewajiban hakim untuk melakukan pengujian berdasarkan Pasal 235 KUHAP.

Di luar MLA, persoalannya berbeda dan lebih sulit.

Misalnya, penyedia layanan asing secara sukarela menyerahkan data kepada aparat Indonesia. Atau pemegang akun memberikan persetujuan kepada penyidik untuk membuka data. Bisa juga aparat Indonesia meminta langsung data kepada penyedia asing atau mengakses suatu sistem dari Indonesia.

Dalam keadaan seperti ini, KUHAP tidak secara tegas menyatakan bahwa hukum negara tertentu harus digunakan untuk menilai keabsahan cara memperoleh bukti.

Karena itu, hakim tidak dapat langsung mengatakan bahwa suatu hukum asing berlaku hanya karena data mempunyai hubungan dengan negara tersebut. Harus lebih dahulu dicari hubungan yang nyata antara hukum negara itu dengan pihak atau tindakan yang menghasilkan bukti.

Misalnya, apakah penyedia layanan tunduk pada hukum negara tersebut. Apakah orang yang menyerahkan data berada di wilayah negara tersebut. Apakah hukum negara tersebut mengatur kewenangan penyedia untuk membuka data pelanggan. Atau apakah tindakan aparat mempunyai akibat langsung terhadap sistem yang berada dalam yurisdiksi negara tersebut.

Di luar MLA, hubungan dengan hukum asing tidak diberikan secara langsung oleh satu ketentuan seperti Pasal 3 ayat (1) UU 1/2006. Hubungan itu harus dibangun melalui penafsiran terhadap kewenangan para pihak, hubungan yurisdiksi, serta sifat tindakan yang dilakukan.[11]

Dalam tulisan ini, hubungan tersebut disebut *doctrinal bridge*.[12]

Perbedaannya dapat dipahami dengan sederhana. Dalam MLA, hukum Negara Diminta berlaku karena UU 1/2006 secara langsung mengatakan demikian. Di luar MLA, hakim masih harus menjelaskan mengapa hukum suatu negara mempunyai hubungan yang cukup dengan tindakan memperoleh bukti.

Karena itu, dasar penerapan hukum asing dalam MLA lebih jelas. Sementara itu, di luar MLA, hakim harus melakukan pemeriksaan lebih lanjut sebelum menyimpulkan bahwa hukum negara tertentu memang relevan terhadap proses memperoleh bukti.

Persoalan ini dapat dilihat pada *production order*. Dalam mekanisme tersebut, aparat

---

[11] I. Kurniawan dan V. Setyawan, "Opportunities to Implement Mutual Legal Assistance in Criminal Law Enforcement in Indonesia," Fundamental: Jurnal Ilmiah Hukum 11, no. 1 (2022): 1–13. Rujukan ini dipakai karena artikel tersebut menjelaskan bahwa MLA dibentuk sebagai dasar hukum kerja sama antara Indonesia dan negara lain dalam meminta atau menerima bantuan pidana, tetapi juga menegaskan bahwa pelaksanaannya dibatasi oleh kedaulatan negara, kesediaan negara yang diminta, dan status pihak asing yang tidak tunduk begitu saja pada hukum Indonesia. Lihat khususnya hlm. 4, 8–11.

[12] Afifah Kusumadara, "Pemakaian Hukum Asing dalam Hukum Perdata Internasional: Kewajiban dan Pelaksanaannya di Pengadilan Indonesia," *Arena Hukum* 15, no. 3 (2022).
Rujukan ini dipakai karena artikel tersebut menegaskan bahwa hukum asing dipakai apabila memiliki hubungan atau titik taut terdekat dengan para pihak atau objek, dan bahwa legalitas formal suatu tindakan pada prinsipnya dapat dikaitkan dengan hukum tempat tindakan itu dilakukan. Kerangka ini mendukung penggunaan istilah *doctrinal bridge* untuk menjelaskan jembatan penalaran normatif di luar dasar tekstual eksplisit.

tidak mengambil data dengan masuk langsung ke dalam sistem komputer. Data diperoleh dengan memerintahkan orang atau penyedia layanan yang menguasainya untuk menyerahkan data tersebut.[13] Karena itu, perhatian tidak semata-mata tertuju pada lokasi *server*. Yang juga perlu diperiksa adalah tempat penyedia berada, dasar kewenangan negara untuk memberikan perintah, jenis data yang diminta, serta apakah penyedia memang memiliki penguasaan atau kendali atas data tersebut.[14]

Article 27 *United Nations Convention against Cybercrime* menggunakan pendekatan serupa. Ketentuan tersebut tidak hanya melihat siapa yang menguasai atau mengendalikan data, tetapi juga hubungan antara orang atau penyedia yang diperintah dengan wilayah negara yang mengeluarkan perintah.[15] KUHAP Indonesia belum mempunyai pengaturan *production order* elektronik lintas negara dengan konstruksi seperti itu. Karena itu, perintah kepada penyedia asing tidak tepat apabila langsung diperlakukan sebagai penyitaan. Jenis tindakannya dan sumber kewenangannya harus ditentukan lebih dahulu.

Situasinya berbeda ketika data diserahkan secara sukarela oleh penyedia layanan atau melalui *voluntary disclosure*.[16] Kesediaan penyedia untuk memberikan data belum cukup untuk membuktikan bahwa penyerahannya sah. Pertanyaan berikutnya tetap harus dijawab, yaitu apakah penyedia tersebut memang mempunyai kewenangan menurut hukum yang berlaku untuk membuka dan menyerahkan data tersebut.

Stored Communications Act Amerika Serikat memberi gambaran mengenai persoalan ini. Section 2702 membatasi pengungkapan data oleh kategori penyedia tertentu, tetapi pada saat yang sama juga memuat sejumlah pengecualian.[17] Karena itu, data yang secara sukarela diberikan perusahaan Amerika kepada aparat Indonesia tidak dapat langsung dinilai sah hanya karena diserahkan tanpa paksaan. Sebaliknya, penyerahan tersebut juga tidak dapat langsung dianggap melanggar hukum. Jenis penyedia, kategori data, dan dasar hukum pengungkapannya tetap harus diperiksa.

CLOUD Act memperlihatkan bentuk kerja sama yang lain. Amerika Serikat dapat membuat *executive agreement* dengan negara tertentu sehingga penyedia yang termasuk

---

[13] P. de Hert and Johannes Thumfart, "Legal Arguments Used in Courts Regarding Territoriality and Cross-Border Production Orders," *New Journal of European Criminal Law* 9, no. 3 (2018): 326–27; Justin D. Hemmings, Sreenidhi Srinivasan, and Peter P. Swire, "Defining the Scope of 'Possession, Custody, or Control' for Privacy Issues and the Cloud Act" (2019), 1–2.

[14] Justin D. Hemmings, Sreenidhi Srinivasan, and Peter P. Swire, "Defining the Scope of 'Possession, Custody, or Control' for Privacy Issues and the Cloud Act" (2019), 1–3; P. de Hert and Johannes Thumfart, "Legal Arguments Used in Courts Regarding Territoriality and Cross-Border Production Orders," *New Journal of European Criminal Law* 9, no. 3 (2018): 340–41; Andrew Woods, "Litigating Data Sovereignty," *Yale Law Journal* 128 (2018): 355–56.

[15] P. de Hert and Johannes Thumfart, "Legal Arguments Used in Courts Regarding Territoriality and Cross-Border Production Orders," *New Journal of European Criminal Law* 9, no. 3 (2018): 340–41; Ya. A. Abdelkarim, "UN Cybercrime Convention: Implementing the Mutual Legal Assistance in the Digital Age," *Journal of Digital Technologies and Law* (2025): discussion of domestic-law compliance and territorial control in cross-border evidence requests.

[16] T. McIntyre, "Voluntary Disclosure of Data to Law Enforcement: The Curious Case of US Internet Firms, their Irish Subsidiaries and European Legal Standards" (2020).

[17] S. Rosenbloom, "Crying Wolf in the Digital Age: Voluntary Disclosure under the Stored Communications Act" (2008). Rujukan ini dipakai karena abstraknya secara langsung menyatakan bahwa *Stored Communications Act* membatasi kemampuan penyedia layanan elektronik untuk mengungkapkan komunikasi dan data pelanggan secara sukarela, sekaligus mengakui adanya pengecualian darurat terhadap pembatasan itu.

dalam cakupan perjanjian dapat memenuhi perintah yang sah dari negara mitra berdasarkan persyaratan tertentu.[18] Mekanisme tersebut tentu tidak dapat digunakan Indonesia tanpa dasar hukumnya sendiri. Nilai perbandingannya terletak pada hal yang lebih mendasar. Kerja sama langsung dengan penyedia asing membutuhkan aturan yang jelas mengenai pihak yang dapat diperintah, jenis data yang dapat diminta, prosedur yang harus ditempuh, perlindungan bagi pihak yang berkepentingan, mekanisme keberatan, dan penyelesaian apabila muncul pertentangan antara kewajiban hukum yang berbeda.

Persetujuan atau *consent* pun tidak selalu membuat persoalan menjadi sederhana. Seseorang dapat memiliki akses terhadap suatu akun, tetapi belum tentu mempunyai kewenangan hukum untuk membuka seluruh data di dalamnya. Karena itu, hakim tidak cukup hanya mengetahui bahwa persetujuan pernah diberikan. Perlu diperiksa siapa yang memberikannya, hubungan orang tersebut dengan akun atau data, sejauh mana kewenangannya, apakah persetujuan diberikan secara bebas, dan apakah tindakan aparat setelah menerima persetujuan masih memerlukan dasar kewenangan tersendiri.

Article 32 *Budapest Convention* dapat digunakan sebagai pembanding. Ketentuan tersebut mengenal akses terhadap data yang tersedia untuk umum dan akses berdasarkan persetujuan yang sah serta diberikan secara sukarela oleh orang yang mempunyai kewenangan untuk mengungkapkan data.[19] Indonesia bukan negara pihak pada konvensi tersebut sehingga Article 32 tidak dapat menjadi dasar kewenangan bagi aparat Indonesia. Namun ketentuan tersebut menunjukkan bahwa keberadaan persetujuan saja belum menyelesaikan masalah. Yang perlu dipastikan adalah apakah orang yang memberikan persetujuan memang mempunyai *lawful authority* atas data yang dibuka.

Persoalan menjadi lebih rumit ketika aparat memperoleh data melalui *remote access*.[20] Tidak semua akses jarak jauh mempunyai karakter hukum yang sama. Membuka data yang memang tersedia untuk umum berbeda dengan memasuki akun tertutup. Membaca data yang sudah tersimpan pada perangkat di Indonesia juga tidak sama dengan menggunakan kata sandi, token, atau kredensial dari perangkat tersebut untuk meminta sistem di luar negeri mengirimkan data baru. Demikian pula, akses yang dilakukan berdasarkan persetujuan yang sah tidak dapat disamakan dengan akses tanpa izin.

---

[18] Théodore Christakis, "21 Thoughts and Questions about the UK/US CLOUD Act Agreement: (and an Explanation of How it Works – With Charts)," *SSRN Electronic Journal* (2019). Rujukan ini dipakai karena secara langsung menjelaskan bahwa perjanjian UK–US adalah perjanjian eksekutif pertama yang dibayangkan oleh *CLOUD Act* dan ditujukan untuk memfasilitasi akses lintas batas terhadap data elektronik untuk penanggulangan kejahatan serius.

[19] P. Verdelho, "Obtaining Digital Evidence in the Global World," *UNIO – EU Law Journal* (2019); Anna-Maria Osula, "Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study," *International Journal of Law and Information Technology* (2016); Martina Conversano, "Il fattore temporale nell'acquisizione transfrontaliera delle e-evidence: il bilanciamento operato nel secondo Protocollo addizionale alla Convenzione di Budapest," *La Nuova Giuridica* (2025). Ketiga rujukan ini dipakai karena sama-sama menyatakan isi pokok *Article* 32: huruf (a) mengenai publicly available data, dan huruf (b) mengenai akses berdasarkan lawful and voluntary consent dari orang yang mempunyai kewenangan hukum untuk mengungkapkan data.

[20] Anna-Maria Osula, "Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study," *International Journal of Law and Information Technology* (2016). Rujukan ini dipakai karena paling langsung membedakan jenis akses dalam *Article* 32: akses ke data yang tersedia untuk umum dan akses ke data tersimpan berdasarkan lawful and voluntary consent dari orang yang memiliki lawful authority untuk mengungkapkannya.

Tidak setiap *remote access* dapat langsung dianggap sebagai tindakan paksa yang dilakukan di luar wilayah Indonesia. Kita harus melihat terlebih dahulu bagaimana akses itu dilakukan dan data apa yang diambil.

Misalnya, penyidik di Jakarta membuka informasi yang memang tersedia untuk umum pada suatu situs. Keadaan ini tentu berbeda dengan penyidik yang menggunakan kata sandi atau kredensial tertentu untuk masuk ke sistem yang dikelola di negara lain dan kemudian mengambil data dari sistem tersebut.

Masalah yurisdiksi mulai menjadi serius ketika aparat Indonesia secara langsung mengakses sistem atau data yang mempunyai hubungan nyata dengan negara lain tanpa persetujuan yang sah, tanpa perjanjian, tanpa mekanisme kerja sama, dan tanpa dasar hukum lain yang membenarkan tindakan itu. Pada keadaan seperti ini, yang perlu ditanyakan bukan hanya apakah datanya berhasil diperoleh, tetapi apakah aparat Indonesia memang mempunyai kewenangan untuk melakukan tindakan tersebut.

Di sini penting membedakan kemampuan teknis dan kewenangan hukum. Penyidik mungkin secara teknis dapat membuka suatu sistem dari Jakarta. Namun kemampuan untuk mengakses sistem tidak otomatis berarti penyidik mempunyai hak secara hukum untuk mengambil data dari sistem yang berada atau dikelola dalam yurisdiksi negara lain.

Jadi, dalam *remote access*, pertanyaan utamanya bukan "apakah data bisa diakses?", melainkan "apakah aparat berwenang melakukan akses tersebut dan berdasarkan hukum apa kewenangan itu digunakan?".

Keadaan teknis data juga perlu diperiksa dengan cermat. Informasi yang terlihat pada layar telepon belum tentu seluruhnya tersimpan di dalam perangkat. Data dapat berupa *cache*, metadata, token autentikasi, salinan sementara, atau informasi yang baru ditampilkan setelah perangkat terhubung kembali dengan sistem lain.[21] Karena itu, lokasi data dan hukum yang berkaitan dengannya tidak dapat ditentukan hanya dari apa yang tampak pada layar perangkat.

Setelah suatu hukum asing ditemukan mempunyai hubungan dengan bukti, persoalan belum selesai. Hakim masih harus menilai apakah hukum tersebut benar-benar berlaku terhadap pihak atau tindakan yang sedang diperiksa. Hubungan faktual dengan suatu negara belum tentu cukup.

Sebagian data, misalnya, dapat pernah disimpan di suatu negara.[22] Keadaan itu tidak

---

[21] Balkibaeva Janagul Ismaylovna, "Problems of Admissibility and Reliability of Metadata as Evidence," *International Journal of Law and Policy* 2, no. 8 (2024); Dragi Rashkovsk and Veronika Rashkovska, "The Difference between Digital Evidence and Evidence in Digital Form," *Iustinianus Primus Law Review* (2025); Jaehyeok Han et al., "ECo-Bag: An Elastic Container Based on Merkle Tree as a Universal Digital Evidence Bag," *Forensic Science International: Digital Investigation* 49 (2024); Nakul S. Sharma et al., "EvidenceX: A Comprehensive Digital Forensics Tool for Evidence Extraction," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* (2025).
Rujukan ini dipakai karena sama-sama menegaskan bahwa bukti digital tidak berhenti pada apa yang terlihat di layar. Metadata adalah "data about data" yang penting untuk asal-usul dan integritas bukti. Sebagian artefak justru tersembunyi dari investigator biasa; dan pemeriksaan forensik modern menuntut analisis metadata, log, perangkat asal, serta informasi tersembunyi.

[22] Oskar Peče and M. Šepec, "The Dilemma of the Location of Digital Evidence," *Problemy Prawa Karnego* (2024); Shelli Gimelstein, "A Location-Based Test for Jurisdiction over Data: The Consequences for Global Online Privacy" (2018); Yuki Okamura et al., "Party Autonomy in Determining the Law Applicable to Non-contractual Obligations concerning Cross-Border Data Transfers," *arXiv* (2026). Rujukan ini dipakai untuk

otomatis membuat seluruh hukum negara tersebut berlaku terhadap proses perolehannya. Hal yang sama berlaku terhadap tempat pendirian perusahaan. Fakta bahwa penyedia didirikan di negara tertentu belum tentu berarti seluruh tindakannya terhadap setiap data hanya diatur oleh hukum negara tersebut.

Kalau bukti elektronik berkaitan dengan lebih dari 1 negara, hakim tidak bisa langsung mengatakan bahwa semua hukum negara yang tersangkut otomatis berlaku. Harus ada hubungan yang cukup jelas antara hukum suatu negara dengan pihak atau tindakan yang sedang dinilai.

Hubungan itu bisa muncul dari beberapa hal. Misalnya, tindakan dilakukan di negara tersebut, pihak yang diperintahkan menyerahkan data berada di sana, penyedia layanan tunduk pada hukum negara itu, sistem yang diakses berada di wilayahnya, atau pihak tertentu secara hukum menguasai dan mengendalikan data. Perjanjian internasional juga dapat menjadi dasar hubungan tersebut.

Jadi, pertanyaan awalnya adalah sederhana, yaitu mengapa hukum negara tertentu dianggap relevan terhadap proses memperoleh bukti ini?

Kalau ternyata hukum negara itu sebenarnya tidak mengatur pihak atau tindakan yang diperiksa, dugaan pelanggaran terhadap hukum tersebut tidak penting untuk menilai keabsahan bukti berdasarkan Pasal 235 KUHAP.

Tetapi setelah diketahui bahwa suatu hukum memang berlaku, pemeriksaan belum selesai. Hakim masih harus melihat apakah pelanggaran terhadap hukum tersebut benar-benar memengaruhi keabsahan cara memperoleh bukti.

Tidak setiap pelanggaran harus berakhir dengan dikesampingkannya alat bukti.

Contohnya, suatu aturan menentukan bahwa hanya pejabat tertentu yang boleh meminta data, penyerahan data harus lebih dahulu mendapat izin pengadilan, pemilik akun harus memberikan persetujuan, data tertentu dilarang untuk dibuka, atau aparat hanya boleh mengakses sistem sampai batas tertentu. Aturan seperti ini berhubungan langsung dengan boleh atau tidaknya data diperoleh.

Kalau aturan semacam itu dilanggar, pelanggarannya dapat memengaruhi penilaian terhadap keabsahan proses memperoleh bukti.

Keadaannya berbeda jika yang dilanggar hanya persyaratan administratif yang tidak menentukan kewenangan memperoleh data. Kesalahan administratif seperti itu tidak seharusnya langsung membuat alat bukti tidak dapat digunakan.

Jadi, sebelum menerapkan Pasal 235 KUHAP, hakim pada dasarnya perlu menjawab 2 pertanyaan. *Pertama*, apakah hukum yang diduga dilanggar memang berlaku terhadap pihak atau tindakan yang menghasilkan bukti. *Kedua*, kalau memang berlaku, apakah pelanggarannya cukup penting untuk memengaruhi keabsahan cara memperoleh bukti.

---

mendukung proposisi bahwa riwayat lokasi data tidak otomatis menentukan hukum yang berlaku. Peče dan Šepec menekankan bahwa lokasi bukti digital menimbulkan ambiguitas hukum, terutama pada cloud storage, dan bahwa persoalannya adalah kapan dan bagaimana negara dapat memperoleh bukti tersebut, bukan sekadar di mana data itu pernah berada Peče2024. Gimelstein menunjukkan bahwa menjadikan lokasi fisik data sebagai satu-satunya dasar yurisdiksi menghasilkan konsekuensi yang tidak dapat diprediksi Gimelstein2018. Okamura dkk. menambahkan bahwa dalam arsitektur cloud terdistribusi, data dapat tersebar di banyak yurisdiksi sehingga sering tidak mungkin menentukan satu lokasi tunggal sebagai dasar hukum yang pasti

2 pertanyaan itu harus dibedakan. Misalnya, suatu aturan asing memang berlaku terhadap penyedia layanan. Hal itu baru menjawab pertanyaan pertama. Belum tentu setiap pelanggaran terhadap aturan tersebut langsung menjadikan bukti diperoleh secara melawan hukum. Hakim masih harus melihat apa yang diatur oleh ketentuan yang dilanggar dan seberapa erat hubungannya dengan proses memperoleh data.

Pembedaan tersebut diperlukan agar Pasal 235 tidak diterapkan terlalu luas. Kalau setiap ketidakpatuhan terhadap hukum asing langsung dianggap sebagai perolehan bukti secara melawan hukum, kesalahan yang sebenarnya tidak berkaitan dengan kewenangan atau cara memperoleh data pun dapat menyebabkan alat bukti dikesampingkan.

Persoalan berikutnya adalah bahwa dalam perkara lintas negara, satu tindakan sering kali berkaitan dengan lebih dari satu hukum.

Misalnya, sebuah penyedia layanan didirikan di Negara A, memberikan layanan kepada pengguna di Negara B, menyimpan sebagian data di Negara C, sedangkan perkara pidananya diperiksa di Indonesia. Dalam keadaan seperti ini, mungkin saja lebih dari satu hukum mempunyai hubungan dengan proses memperoleh data tersebut.

Kalau demikian, pertanyaannya tidak lagi hanya “hukum negara mana yang berlaku?”. Pertanyaan berikutnya adalah apakah semua hukum yang berlaku itu masih dapat dipatuhi secara bersamaan.

Jika seluruh kewajiban masih dapat dipenuhi, sebenarnya tidak ada konflik hukum. Pihak yang memperoleh atau menyerahkan data cukup memenuhi semua kewajiban yang berlaku terhadapnya.

Konflik baru benar-benar muncul apabila memenuhi satu kewajiban justru menyebabkan pelanggaran terhadap kewajiban lain.

Contohnya, hukum suatu negara mewajibkan penyedia menyerahkan data berdasarkan perintah yang sah, tetapi hukum negara lain yang juga mengikat penyedia melarang data yang sama untuk diungkapkan dalam keadaan tersebut. Di sini terdapat dua kewajiban hukum yang sama-sama berlaku, tetapi tidak mungkin dipenuhi sekaligus.

Pada titik inilah hakim harus membedakan 3 hal. *Pertama*, hukum mana yang memang berlaku. *Kedua*, apakah hukum-hukum tersebut benar-benar bertentangan. *Ketiga*, jika ada pelanggaran, apakah pelanggaran itu cukup penting untuk memengaruhi penilaian bahwa bukti diperoleh secara tidak melawan hukum menurut Pasal 235 KUHAP.

Regulation (EU) 2023/1543 dapat digunakan sebagai pembanding. Dalam regulasi ini, terbitnya *European Production Order* oleh pihak yang berwenang belum selalu menyelesaikan persoalan. Perintah tersebut pada dasarnya mewajibkan penyedia layanan menyerahkan data tertentu. Namun, jika pemenuhan perintah itu justru menyebabkan penyedia melanggar hukum negara ketiga yang juga mengikatnya, pertentangan tersebut tetap harus diperiksa. Karena itu, keabsahan perintah dari negara yang meminta data tidak dengan sendirinya meniadakan kewajiban hukum yang berlaku terhadap penyedia di negara lain. Regulasi ini menunjukkan bahwa dalam perolehan bukti elektronik lintas negara, pertanyaan tidak berhenti pada apakah suatu negara berwenang mengeluarkan perintah, tetapi juga apakah perintah tersebut dapat dilaksanakan tanpa melanggar hukum lain yang sama-sama

berlaku.[23] Kemungkinan adanya pertentangan dengan hukum negara lain tetap diperiksa. Hubungan perkara dengan masing-masing negara, hubungan penyedia dengan negara tersebut, serta kepentingan hukum yang dilindungi dapat dipertimbangkan.

Pengalaman Uni Eropa tidak berarti Indonesia harus mengikuti mekanisme yang sama. Hal yang penting dari pengalaman tersebut adalah 1 gagasan sederhana, yaitu 1 tindakan memperoleh bukti dapat tunduk pada hukum lebih dari 1 negara. Masalah muncul apabila hukum-hukum tersebut memberikan kewajiban yang berbeda, bahkan saling bertentangan.

Misalnya, penyidik Indonesia mempunyai dasar hukum untuk meminta data dari suatu penyedia layanan di luar negeri. Dari sisi hukum Indonesia, permintaan itu mungkin sah. Namun penyedia layanan tersebut juga tunduk pada hukum negara tempat penyedia berkedudukan. Hukum negara itu dapat menentukan bahwa data pelanggan hanya boleh diserahkan apabila syarat tertentu dipenuhi atau bahkan melarang penyerahan jenis data tertentu.

Dalam keadaan seperti itu, hakim tidak cukup hanya bertanya apakah aparat Indonesia berwenang meminta data. Hakim juga perlu melihat apakah pihak yang diminta menyerahkan data diperbolehkan oleh hukum yang mengaturnya untuk memenuhi permintaan tersebut.

Tetapi adanya 2 hukum yang berlaku belum tentu berarti terjadi konflik. Pertama-tama harus dilihat apakah kedua hukum tersebut masih dapat dipatuhi secara bersamaan.

Misalnya, hukum Indonesia membolehkan aparat meminta data, sedangkan hukum negara tempat penyedia berada membolehkan penyerahan data sepanjang terdapat izin pengadilan. Jika izin tersebut dapat diperoleh, kedua hukum sebenarnya masih dapat dipenuhi. Dalam keadaan demikian tidak ada konflik hukum. Yang harus dilakukan adalah memenuhi seluruh persyaratan yang berlaku.

Konflik baru muncul apabila memenuhi satu kewajiban membuat pihak yang bersangkutan harus melanggar kewajiban lain.

Sebagai contoh, hukum Indonesia memerintahkan penyedia menyerahkan data tertentu, tetapi hukum negara lain yang juga mengikat penyedia secara tegas melarang pengungkapan data tersebut dalam keadaan yang sama. Penyedia kemudian berada dalam posisi yang sulit. Jika data diserahkan, hukum negara lain dilanggar. Jika data tidak diserahkan, perintah berdasarkan hukum Indonesia tidak dipenuhi.

Pada keadaan seperti inilah persoalan konflik hukum benar-benar muncul.

Hakim pertama-tama perlu melihat apakah undang-undang, traktat, atau perjanjian internasional telah mengatur cara menyelesaikan pertentangan tersebut. Jika sudah ada aturan

---

[23] Jorge A. Espina Ramos, "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* (2025); M. Warchoł, "Access to Electronic Evidence in Criminal Proceedings in the Light of European Union Law," *Law • Education • Security* (2026); Hanna Kuczyńska, "The EU E-evidence Package from the Polish Perspective: High Time for a Systemic Change," *Studia Iuridica Lublinensia* (2024); Adam Juszczak and Elisa Sason, "The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice: An Introduction to the New EU Package on E-evidence," *eucrim* (2023). Rujukan ini dipakai untuk menunjukkan bahwa *Regulation* 2023/1543 membentuk mekanisme direct request kepada penyedia layanan, tetapi pihak berwenang tetap harus menilai dasar hukum yang tepat dan tidak menganggap penerbitan order sebagai akhir dari analisis.

khusus, penyelesaiannya mengikuti aturan itu.

Jika belum ada aturan khusus, hakim perlu melihat hubungan masing-masing hukum dengan tindakan memperoleh bukti. Artinya, hakim harus menilai mengapa hukum suatu negara berlaku dan apa yang sebenarnya hendak dilindungi oleh aturan tersebut.

Misalnya, aturan yang melarang penyedia menyerahkan isi komunikasi pribadi tanpa izin mempunyai hubungan langsung dengan proses memperoleh bukti. Aturan tersebut menentukan apakah data boleh atau tidak boleh diserahkan. Pelanggarannya karena itu dapat berpengaruh terhadap keabsahan cara memperoleh bukti.

Keadaannya berbeda dengan pelanggaran administratif yang tidak menentukan boleh atau tidaknya data diperoleh. Kesalahan administratif seperti itu tidak seharusnya langsung mengakibatkan alat bukti dikesampingkan.

Dari sini dapat dipahami bahwa pelanggaran hukum asing tidak otomatis berarti bukti diperoleh secara melawan hukum. Hakim masih harus melihat dua hal. Pertama, apakah hukum asing tersebut memang berlaku terhadap pihak atau tindakan yang menghasilkan bukti. Kedua, jika memang berlaku, apakah ketentuan yang dilanggar mempunyai hubungan yang cukup penting dengan keabsahan proses memperoleh bukti.

Cara menerapkan Pasal 235 KUHAP kemudian dapat dijelaskan secara bertahap.

Langkah pertama adalah mengetahui bagaimana bukti diperoleh. Ini harus ditentukan terlebih dahulu karena cara memperoleh data dapat berbeda-beda. Data mungkin diperoleh melalui MLA, melalui perintah langsung kepada penyedia layanan, melalui penyerahan sukarela, melalui persetujuan pemegang akun, atau melalui akses langsung oleh penyidik.

Pembedaan itu penting karena masing-masing cara memperoleh data mempunyai dasar hukum yang berbeda.

Langkah kedua adalah memeriksa kewenangan aparat Indonesia. Hakim harus memastikan apakah penyidik memang mempunyai dasar hukum untuk melakukan atau meminta tindakan tersebut. Dengan kata lain, sebelum membicarakan hukum negara lain, harus dipastikan lebih dahulu bahwa tindakan aparat mempunyai dasar menurut hukum Indonesia.

Langkah ketiga adalah menentukan apakah ada hukum negara lain yang juga berlaku terhadap tindakan tersebut. Dalam perkara bukti elektronik, kemungkinan ini cukup besar. Penyidik dapat berada di Indonesia, penyedia layanan berada di Amerika Serikat, sedangkan data diproses melalui sistem di negara lain.

Karena itu, hukum yang berlaku tidak dapat ditentukan hanya dengan melihat lokasi *server*. Hakim perlu melihat siapa yang melakukan tindakan, siapa yang diminta menyerahkan data, siapa yang menguasai atau mengendalikan data, dan hukum apa yang mengatur pihak atau tindakan tersebut.

Langkah keempat dilakukan apabila ternyata lebih dari satu hukum berlaku. Hakim harus melihat apakah seluruh hukum itu masih dapat dipatuhi secara bersamaan. Jika dapat, tidak ada konflik. Seluruh persyaratan yang berlaku harus dipenuhi.

Jika tidak dapat dipenuhi bersama, barulah hakim menghadapi konflik hukum.

Langkah kelima adalah menilai arti pelanggaran yang ditemukan. Tidak semua pelanggaran mempunyai hubungan yang sama dengan keabsahan bukti.

Pelanggaran terhadap aturan mengenai siapa yang berwenang memperoleh data, siapa yang boleh menyerahkan data, keharusan memperoleh izin pengadilan, keabsahan persetujuan pemegang akun, larangan membuka data tertentu, atau batas akses terhadap sistem mempunyai hubungan langsung dengan cara memperoleh bukti.

Sebaliknya, pelanggaran administratif yang tidak memengaruhi kewenangan atau hak untuk memperoleh data tidak seharusnya diperlakukan dengan cara yang sama.

Setelah seluruh pemeriksaan tersebut dilakukan, barulah hakim kembali kepada Pasal 235 KUHAP.

Di sini perlu dipahami kedudukan hukum asing. Hukum asing tidak secara langsung memutuskan apakah suatu alat bukti boleh digunakan di pengadilan Indonesia. Keputusan akhir tetap ditentukan berdasarkan KUHAP sebagai hukum acara yang berlaku di pengadilan Indonesia.

Hukum asing mempunyai fungsi yang lebih terbatas. Hukum tersebut membantu hakim menentukan apakah tindakan yang menghasilkan bukti dilakukan berdasarkan kewenangan dan prosedur yang sah.

Jika bukti hanya dapat diperoleh dengan melanggar aturan yang memang berlaku dan aturan tersebut secara langsung menentukan siapa yang berwenang memperoleh atau menyerahkan data, mensyaratkan izin, membatasi akses, atau melarang pengungkapan data, maka pelanggaran tersebut harus diperhitungkan dalam penilaian Pasal 235.

Dalam keadaan seperti itu, hakim dapat menilai bahwa syarat alat bukti harus “diperoleh secara tidak melawan hukum” sebagaimana dimaksud dalam Pasal 235 ayat (3) tidak terpenuhi. Akibat selanjutnya ditentukan menurut Pasal 235 ayat (5).

Sebaliknya, apabila pelanggaran yang ditemukan tidak mempunyai hubungan yang nyata dengan kewenangan atau keabsahan cara memperoleh bukti, alat bukti tidak seharusnya langsung dikesampingkan.

Dengan demikian, cara berpikirnya adalah hakim pertama-tama mencari tahu bagaimana bukti diperoleh. Setelah itu hakim memeriksa kewenangan aparat Indonesia. Berikutnya ditentukan hukum lain yang memang berlaku terhadap tindakan tersebut. Jika beberapa hukum berlaku, hakim melihat apakah hukum-hukum tersebut dapat dipatuhi bersama atau justru bertentangan. Jika terdapat pelanggaran, hakim kemudian menilai apakah pelanggaran itu cukup penting untuk memengaruhi keabsahan perolehan. Baru setelah seluruh tahap tersebut selesai, akibatnya ditentukan berdasarkan Pasal 235 KUHAP.

Masalahnya, hukum Indonesia saat ini belum memberikan jawaban lengkap untuk seluruh kemungkinan tersebut. Karena itu, apabila tidak terdapat aturan khusus, hakim perlu melihat hubungan masing-masing hukum dengan tindakan yang sedang dinilai.

Di sini yang harus diperhatikan adalah fungsi dari aturan yang dilanggar. Tidak semua pelanggaran mempunyai arti yang sama.

Misalnya, suatu hukum melarang penyedia membuka isi komunikasi pribadi tanpa izin pengadilan. Aturan seperti ini berhubungan langsung dengan boleh atau tidaknya data diserahkan. Karena itu, pelanggarannya mempunyai hubungan yang kuat dengan keabsahan cara memperoleh bukti.

Hal tersebut berbeda dengan pelanggaran administratif yang tidak menentukan boleh

atau tidaknya data diperoleh. Jika kesalahan yang terjadi hanya berupa pelanggaran administratif dan tidak memengaruhi kewenangan memperoleh atau menyerahkan data, pelanggaran tersebut tidak semestinya langsung menyebabkan alat bukti tidak dapat digunakan.

Dari sini dapat dilihat bahwa hakim sebenarnya harus menjawab 2 pertanyaan yang berbeda. Pertama, apakah aturan yang diduga dilanggar memang berlaku terhadap pihak atau tindakan yang menghasilkan bukti. Kedua, jika aturan tersebut memang berlaku, apakah pelanggarannya cukup penting untuk memengaruhi keabsahan proses memperoleh bukti.

Pertanyaan kedua inilah yang berkaitan dengan tingkat penting atau materialitas pelanggaran.

Pasal 235 tidak seharusnya dipahami bahwa setiap pelanggaran hukum asing otomatis membuat alat bukti menjadi tidak sah. Jika pendekatan seperti itu digunakan, kesalahan administratif yang tidak mempunyai hubungan nyata dengan proses memperoleh data pun dapat menyebabkan bukti dikesampingkan. Akibatnya, ruang lingkup Pasal 235 menjadi terlalu luas.

Yang harus dilihat adalah apakah pelanggaran tersebut menyentuh hal yang menentukan legalitas perolehan bukti. Misalnya, kewenangan aparat, kewenangan pihak yang menyerahkan data, keharusan memperoleh izin, larangan mengungkapkan data tertentu, keabsahan persetujuan, atau batas akses terhadap sistem.

Jika pelanggaran menyentuh hal-hal tersebut, barulah pelanggaran tersebut mempunyai arti bagi Pasal 235.

Dengan demikian, urutan berpikir hakim sebenarnya dapat dibuat cukup sederhana. *Pertama*, tentukan bagaimana bukti diperoleh.[24] *Kedua*, pastikan aparat Indonesia mempunyai kewenangan. *Ketiga*, tentukan hukum lain yang benar-benar berlaku terhadap tindakan atau pihak yang terlibat. *Keempat*, jika ada lebih dari 1 hukum, lihat apakah keduanya dapat dipatuhi atau justru bertentangan.[25] *Kelima*, jika terdapat pelanggaran, nilai apakah pelanggaran tersebut benar-benar memengaruhi keabsahan cara memperoleh bukti. Setelah seluruh pertanyaan itu dijawab, barulah hakim menerapkan Pasal 235.

---

[24] Arief Setia Nugroho, Amad Sudiro, and Hery Firmansya, "Reassessing Mass Media Reporting as Criminal Evidence in Indonesia toward Social Media Justice," *Journal of Sustainable Development and Regulatory Issues (JSDERI)*, March 31, 2026; Fahrezi Arfa Akbar Harahap and Rachmad Abduh, "A Legal Analysis of the Evidence System in Criminal Procedure: A Study of Evidence in Indonesia and Thailand," *JHSS (Journal of Humanities and Social Studies)*, March 15, 2026; M. Safii, S. Sanusi, and F. Sudewo, "Comparison of Criminal Evidence Between the Indonesian and United States' Legal Systems," in *Proceedings of the 1st International Conference on Law, Social Science, Economics, and Education, MALAPY 2022* (2022). Rujukan ini menopang 2 premis dasar: Pasal 235 mengakui alat bukti yang lebih luas, tetapi tetap mensyaratkan bahwa bukti harus diperoleh secara sah, dan sistem pembuktian Indonesia tetap mengaitkan alat bukti yang sah dengan keyakinan hakim

[25] I. Kurniawan and V. Setyawan, "Opportunities to Implement Mutual Legal Assistance in Criminal Law Enforcement in Indonesia," *Fundamental: Jurnal Ilmiah Hukum*, May 12, 2022; Untung Setyardi, "The Role of Mutual Legal Assistance in Obtaining Testimony from Foreign Witnesses," *Citizen: Jurnal Ilmiah Multidisiplin Indonesia*, January 25, 2025; Eloisa de Sousa Arruda and Silvio José Farinholi Arcuri, "International Legal Cooperation in Criminal Matters: Principles and Aspects Related to the Production of Evidence Abroad," *International Journal of Advanced Engineering Research and Science*, 2023. Rujukan ini dipakai untuk langkah tentang applicable external law dan kemungkinan konflik kewajiban, karena bukti yang diperoleh lintas batas bergantung pada mekanisme kerja sama internasional, kesediaan pihak asing, izin negara tempat pihak itu berada, dan saluran hukum untuk produksi bukti di luar negeri

Dalam istilah yang lebih teknis, urutan tersebut dapat disebut *characterisation, domestic authority, applicable external law, conflict of applicable laws, materiality,* dan *consequence under Article 235*.[26]

Namun istilah itu tidak perlu membuat persoalan terlihat rumit. Intinya tetap sama. Hakim harus mengetahui apa yang dilakukan, siapa yang berwenang, hukum apa yang mengatur tindakan tersebut, apakah terdapat pertentangan antarhukum, apakah pelanggarannya cukup penting, dan akhirnya apa akibatnya terhadap alat bukti.

Pada tahap terakhir ini Pasal 235 bekerja.

Hukum negara lain tidak menentukan sendiri apakah alat bukti boleh digunakan di pengadilan Indonesia. Hukum asing hanya membantu menjawab satu bagian dari persoalan, yaitu apakah pihak atau tindakan yang menghasilkan bukti mempunyai dasar hukum yang sah.

Keputusan akhir tetap berada pada hakim Indonesia berdasarkan KUHAP.

Apabila hakim menemukan bahwa cara memperoleh data melanggar aturan yang benar-benar berlaku dan pelanggaran tersebut berkaitan langsung dengan sumber kewenangan, izin, larangan memperoleh atau menyerahkan data, keabsahan persetujuan, atau batas tindakan aparat, maka hakim mempunyai alasan untuk menilai bahwa syarat “diperoleh secara tidak melawan hukum” dalam Pasal 235 ayat (3) tidak terpenuhi.

Setelah hakim menemukan bahwa pelanggaran yang terjadi memang berhubungan langsung dengan keabsahan cara memperoleh bukti, akibat hukumnya kembali kepada Pasal 235 KUHAP. Jika pelanggaran tersebut menyebabkan syarat “diperoleh secara tidak melawan hukum” dalam Pasal 235 ayat (3) tidak terpenuhi, Pasal 235 ayat (5) menentukan bahwa alat bukti tersebut tidak dapat digunakan dalam persidangan dan tidak mempunyai kekuatan pembuktian. Sebaliknya, pelanggaran yang tidak berhubungan nyata dengan kewenangan atau cara memperoleh bukti tidak seharusnya langsung menghasilkan akibat yang sama.

Sampai di sini perlu dibedakan 1 persoalan lain, yaitu autentikasi. Autentikasi dan *lawful acquisition* sama-sama menjadi syarat dalam Pasal 235, tetapi keduanya menjawab pertanyaan yang berbeda.

Autentikasi berkaitan dengan pertanyaan apakah data yang diajukan benar merupakan data yang diklaim dan apakah data tersebut tetap utuh. *Lawful acquisition* berkaitan dengan pertanyaan apakah tindakan untuk memperoleh data dilakukan berdasarkan kewenangan dan prosedur yang sah.

Perbedaannya dapat dilihat dari contoh sederhana. Suatu rekaman percakapan dapat terbukti asli dan tidak pernah diubah. Namun, jika rekaman itu diperoleh dengan memasuki

---

[26] Shanty Syafyuana Putri, Ismansyah Ismansyah, and Lucky Raspati, “The Urgency of Regulating Illegally Obtained Evidence (the Exclusionary Rule) in the Indonesian Criminal Justice System: A Perspective on Harmonizing the New Criminal Code and Criminal Procedure Code,” *Journal of Creative Power and Ambition (JCPA)*, September 7, 2026; O. V. Shypilov, “Acquisition by Information Obtained through International Legal Assistance of the Status of Evidence in Criminal Proceedings: Problems of Admissibility and Procedural Transformation,” *Analytical and Comparative Jurisprudence*, July 22, 2026. Rujukan ini dipakai untuk langkah materiality dan consequence, karena keduanya menekankan bahwa informasi yang diperoleh dari luar kerangka prosedural nasional tidak otomatis menjadi bukti; ia harus diuji legalitas perolehannya, kesesuaiannya dengan standar fair trial dan HAM, serta kemungkinan verifikasinya oleh pembela sebelum dinilai dapat dipakai atau dikesampingkan

akun tanpa kewenangan, autentikasinya mungkin tidak bermasalah, sedangkan cara memperolehnya tetap dapat dipersoalkan. Sebaliknya, aparat dapat memperoleh data melalui prosedur yang sah, tetapi kemudian tidak mampu membuktikan bahwa data yang diajukan di persidangan masih sama dengan data yang pertama kali diperoleh. Dalam keadaan terakhir, persoalannya terletak pada autentikasi.

Karena itu, hakim harus memeriksa keduanya secara tersendiri. Untuk autentikasi, perhatian diarahkan pada asal data, identitasnya, metode pengambilan atau ekstraksi, integritas, penyimpanan, dan *chain of custody*. Untuk *lawful acquisition*, yang diperiksa adalah siapa yang memperoleh data, berdasarkan kewenangan apa, melalui prosedur apa, dan hukum apa yang mengatur tindakan tersebut.

Kedua pemeriksaan itu memang dapat berhubungan. Masalah pada *chain of custody*, misalnya, dapat menimbulkan keraguan terhadap integritas data sekaligus memperlihatkan persoalan dalam cara bukti ditangani. Namun secara hukum keduanya tetap berbeda. Hal itu juga terlihat dari Pasal 235 ayat (5) yang menggunakan rumusan "tidak autentik dan/atau diperoleh secara melawan hukum". Artinya, masalah autentikasi dan masalah legalitas perolehan dapat masing-masing menimbulkan akibat terhadap penggunaan alat bukti.

Sebelum KUHAP 2025 berlaku, hukum Indonesia sebenarnya sudah mengenal sebagian persoalan mengenai kewenangan memperoleh bukti elektronik. Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016, misalnya, memberikan perhatian pada siapa yang meminta atau memperoleh bukti elektronik dan dalam konteks kewenangan apa tindakan itu dilakukan.

Namun putusan tersebut tidak menentukan hukum negara mana yang harus dipakai apabila proses memperoleh bukti melibatkan yurisdiksi asing. Karena itu, Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016 tidak dapat diperlakukan sebagai aturan untuk menentukan hukum yang berlaku terhadap bukti elektronik lintas negara. Relevansinya lebih terbatas, yaitu memperlihatkan bahwa kewenangan pihak yang memperoleh bukti merupakan bagian dari penilaian terhadap keabsahan penggunaannya.

Pasal 235 KUHAP 2025 membawa persoalan tersebut lebih jauh karena legalitas cara memperoleh alat bukti sekarang dinyatakan secara langsung sebagai syarat pembuktian.

SEMA Nomor 1 Tahun 1985 juga perlu ditempatkan secara tepat. SEMA tersebut berhubungan dengan kekuatan pembuktian berita acara pemeriksaan saksi dan *visum et repertum* yang dibuat di luar negeri. Ruang lingkupnya karena itu terlalu terbatas untuk digunakan sebagai aturan umum mengenai bukti elektronik yang diperoleh dari luar negeri.

Nilai SEMA tersebut lebih bersifat historis. SEMA itu memperlihatkan bahwa hukum acara Indonesia sejak lama telah menghadapi persoalan mengenai bukti yang dibentuk di luar negeri. Hanya saja, persoalan bukti elektronik sekarang jauh lebih rumit karena proses memperoleh, menyimpan, memproses, dan menyerahkan data dapat melibatkan beberapa negara sekaligus.

Pengalaman negara lain dapat membantu menjelaskan mengapa persoalan tersebut memerlukan aturan yang lebih jelas.

Perkara *Microsoft Ireland* di Amerika Serikat, misalnya, memperlihatkan persoalan mengenai sejauh mana perintah yang dikeluarkan berdasarkan hukum suatu negara dapat

menjangkau data yang disimpan di luar wilayah negara tersebut.[27] Inti perkaranya bukan semata-mata lokasi *server*. Persoalan yang lebih mendasar adalah batas kewenangan hukum nasional terhadap data yang mempunyai hubungan dengan yurisdiksi lain.

Amerika Serikat kemudian mengesahkan CLOUD Act. Bagi Indonesia, arti perbandingannya bukan bahwa model tersebut harus ditiru. Pelajaran yang dapat diambil adalah bahwa jika suatu negara hendak memberi kewenangan kepada aparatnya untuk memperoleh data di luar wilayah melalui penyedia layanan, dasar, ruang lingkup, dan batas kewenangan itu perlu diatur secara jelas.[28] Hukum juga perlu memberi jawaban ketika kewajiban menyerahkan data menurut hukum satu negara bertentangan dengan larangan menurut hukum negara lain.

Uni Eropa menghadapi persoalan serupa melalui Regulation (EU) 2023/1543. Regulasi tersebut mengenal *European Production Order* dan *European Preservation Order*, yang memungkinkan otoritas tertentu memerintahkan penyedia untuk menyerahkan atau mempertahankan data.

Hal yang relevan bagi pembahasan ini adalah bahwa terbitnya perintah yang sah tidak selalu mengakhiri persoalan. Jika pelaksanaan perintah tersebut dapat menyebabkan penyedia melanggar kewajiban berdasarkan hukum negara ketiga, pertentangan itu tetap perlu diperiksa. Dengan demikian, sahnya kewenangan negara yang meminta data belum tentu berarti bahwa semua persoalan hukum telah selesai.

Pengalaman tersebut memberikan pelajaran yang cukup sederhana. Kemampuan untuk meminta atau mengakses data secara teknis tidak sama dengan kewenangan hukum untuk memperolehnya. Karena itu, hukum harus dapat menjawab siapa yang boleh diperintah, berdasarkan kewenangan apa, data apa yang dapat diminta, prosedur apa yang harus ditempuh, dan bagaimana pertentangan dengan hukum negara lain diselesaikan.

United Nations Convention against Cybercrime bergerak dalam arah yang sama. Indonesia menandatangani konvensi tersebut pada 24 September 2026. Berdasarkan status depositori Perserikatan Bangsa-Bangsa per 30 September 2026, terdapat 95 negara penandatangan dan 3 negara pihak. Konvensi tersebut belum berlaku karena Article 65 mensyaratkan 40 instrumen ratifikasi, penerimaan, persetujuan, atau aksesi sebelum mulai

---

[27] Shelli Gimelstein, "A Location-Based Test for Jurisdiction over Data: The Consequences for Global Online Privacy" (March 19, 2018); T. Christakis, "Data, Extraterritoriality and International Solutions to Transatlantic Problems of Access to Digital Evidence. Legal Opinion on the Microsoft Ireland Case (Supreme Court of the United States)" (November 29, 2017); D. Svantesson and F. Gerry, "Access to Extraterritorial Evidence: The Microsoft Cloud Case and Beyond," *Computer Law & Security Review* (August 1, 2015). Rujukan ini mendukung proposisi bahwa *Microsoft Ireland* berpusat pada pertanyaan apakah perintah berdasarkan hukum nasional dapat memaksa pengungkapan data yang disimpan di luar negeri

[28] Jennifer C. Daskal, "Unpacking the CLOUD Act" (2018); Jessica Shurson, "Data Protection and Law Enforcement Access to Digital Evidence: Resolving the Reciprocal Conflicts between EU and US Law," *International Journal of Law and Information Technology* (2020). Rujukan ini dipakai untuk mendukung pernyataan bahwa *CLOUD Act* memperjelas jangkauan kewenangan atas data di luar wilayah. Daskal menjelaskan bahwa undang-undang itu "detail[s] the reach of U.S. law enforcement authority over extraterritorially located data" dan bahwa tidak ada kewajiban pengungkapan bila data tidak berada dalam *possession, custody, or control* perusahaan Daskal2018. Shurson menegaskan bahwa bagian pertama *CLOUD Act* mengklarifikasi bahwa jangkauan *SCA warrants* meluas ke data yang berada dalam *possession, custody or control* penyedia layanan Amerika Serikat, tanpa mempersoalkan di mana data itu disimpan.

berlaku pada hari ke-90 setelah instrumen keempat puluh disimpan.[29]

Karena konvensi tersebut belum berlaku, Article 27 dan Article 28 belum dapat digunakan sebagai sumber kewenangan langsung bagi aparat Indonesia. Bahkan jika Indonesia kemudian meratifikasinya, hukum nasional tetap perlu menentukan bagaimana kewenangan yang dimaksud dalam konvensi dilaksanakan.

Namun kedua ketentuan tersebut berguna untuk memperlihatkan perbedaan antara dua bentuk tindakan. Article 27 mengatur *production order*, yaitu perintah kepada pihak yang mempunyai penguasaan atau kendali atas data untuk menyerahkannya. Article 28 mengatur penggeledahan dan penyitaan terhadap sistem komputer dan data.

Perbedaannya penting. Memerintahkan penyedia layanan untuk menyerahkan data tidak sama dengan aparat sendiri mengakses sistem dan mengambil data. Pada tindakan pertama, data diberikan oleh pihak yang diperintah. Pada tindakan kedua, aparat melakukan tindakan langsung terhadap sistem atau data. Karena subjek yang bertindak dan bentuk tindakannya berbeda, dasar kewenangan dan persoalan yurisdiksinya juga dapat berbeda.

Hukum Indonesia belum membedakan berbagai bentuk perolehan bukti elektronik tersebut secara memadai. Akibatnya, setelah KUHAP 2025 berlaku, persoalan yang harus dijawab tidak berhenti pada bagaimana aparat Indonesia dapat memperoleh data dari luar negeri. Pertanyaan yang lebih mendasar adalah hukum apa yang harus digunakan untuk menilai sah atau tidaknya tindakan yang menghasilkan data tersebut.

Setelah hukum yang berlaku ditentukan, hakim kemudian menilai apakah terdapat pertentangan dengan hukum lain dan apakah pelanggaran yang terjadi benar-benar berhubungan dengan legalitas perolehan. Hasil pemeriksaan itulah yang selanjutnya digunakan untuk menentukan apakah syarat “diperoleh secara tidak melawan hukum” dalam Pasal 235 terpenuhi.

Dengan demikian, adanya hubungan dengan negara lain tidak dengan sendirinya membuat suatu alat bukti sah ataupun tidak sah. Unsur asing hanya menjadi titik awal untuk menentukan hukum yang relevan. Penilaian akhirnya tetap bergantung pada tindakan yang dilakukan, kewenangan yang digunakan, hukum yang mengatur tindakan tersebut, dan arti pelanggaran yang ditemukan terhadap keabsahan proses memperoleh bukti.

Undang-Undang Nomor 1 Tahun 2006 juga perlu disesuaikan dengan cara kerja bukti elektronik saat ini. Data elektronik dapat berubah atau hilang dengan cepat. Karena itu, tindakan seperti menjaga agar data tidak dihapus (*preservation*), meminta data langsung kepada penyedia layanan (*direct cooperation*), atau memerintahkan penyedia menyerahkan data (*production order*) membutuhkan proses yang lebih cepat daripada mekanisme MLA biasa. Namun kecepatan tidak boleh menghilangkan pengawasan pengadilan dan perlindungan terhadap hak seseorang.

---

[29] M. Watney, “The Legal Pitfalls to Ratification of the United Nations Convention Against Cybercrime,” in *European Conference on Cyber Warfare and Security* (2025); I. Tennant, “Applying the Right Lessons from the Negotiation and Implementation of the UNTOC and the UNCAC to the Implementation of the Newly Agreed UN ‘Cybercrime’ Treaty,” *Journal of Cyber Policy* (2024); J. Pielemeier, “Convention Against Cybercrime (U.N.),” *International Legal Materials* (2025); K. Bannelier, “Risks and Opportunities of the UN Cybercrime Convention for the UNODC & the Fight Against Transnational Organised Crime: A First Assessment,” *Transnational Criminal Law Review* (2025). Rujukan ini dipakai untuk mendukung bahwa konvensi diadopsi pada 24 Desember 2024 dan dibuka untuk penandatanganan pada 2025.

Ratifikasi *United Nations Convention against Cybercrime* dapat membantu pembaruan tersebut, tetapi ratifikasi saja belum cukup. Hukum Indonesia tetap harus mengatur siapa yang berwenang meminta atau mengambil data, bagaimana prosedurnya, perlindungan apa yang diberikan kepada pemilik data, kapan hukum negara lain harus diperhatikan, bagaimana menyelesaikan pertentangan antara beberapa hukum, dan apa akibatnya terhadap penggunaan bukti di persidangan.

Dari sini dapat dipahami perubahan penting yang dibawa KUHAP 2025. Dalam perkara bukti elektronik lintas negara, pertanyaannya tidak cukup lagi hanya "data ini berada di Indonesia atau di luar Indonesia?". Pertanyaan yang lebih penting adalah "bagaimana data itu diperoleh dan apakah cara memperolehnya sah?".

Pasal 235 KUHAP meminta hakim memeriksa dua hal, yaitu apakah bukti tersebut autentik dan apakah bukti itu diperoleh secara sah. Pasal 124 ayat (4) memberi kewenangan kepada PN Jakarta Pusat untuk menangani permohonan penyitaan benda yang berada di luar negeri. Namun ketentuan itu tidak berarti aparat Indonesia bebas melakukan penyitaan sendiri di wilayah negara lain. Sementara itu, UU 1/2006 mengatur bantuan timbal balik dengan negara lain dan menentukan bahwa tindakan di Negara Diminta dilaksanakan menurut hukum negara tersebut.

Karena itu, cara menilai bukti elektronik lintas negara sebaiknya dimulai dari tindakan yang dilakukan. Hakim terlebih dahulu melihat bagaimana bukti diperoleh. Setelah itu diperiksa apakah aparat Indonesia mempunyai kewenangan. Berikutnya ditentukan hukum negara lain yang memang mengatur pihak atau tindakan tersebut. Jika lebih dari satu hukum berlaku, hakim melihat apakah semua aturan itu masih dapat dipatuhi atau justru saling bertentangan. Jika ada pelanggaran, barulah dinilai apakah pelanggaran tersebut benar-benar berpengaruh terhadap sah atau tidaknya cara memperoleh bukti.

Dalam MLA, persoalannya lebih mudah karena UU 1/2006 secara langsung menyatakan bahwa tindakan di Negara Diminta mengikuti hukum negara tersebut. Jadi, hubungan dengan hukum asing sudah diberikan oleh undang-undang.

Keadaannya berbeda jika data diperoleh di luar MLA, misalnya melalui penyerahan sukarela oleh penyedia layanan, persetujuan pemegang akun, permintaan langsung kepada penyedia asing, atau akses langsung terhadap sistem. Dalam keadaan seperti itu, tidak ada satu ketentuan yang langsung mengatakan hukum negara mana yang harus digunakan. Hakim harus lebih dahulu menjelaskan mengapa hukum negara tertentu memang mempunyai hubungan dengan pihak atau tindakan yang menghasilkan bukti.

Di sini fungsi hukum asing harus ditempatkan secara tepat. Hukum asing tidak langsung menentukan apakah bukti boleh digunakan di pengadilan Indonesia. Keputusan itu tetap ditentukan berdasarkan KUHAP. Namun hukum asing juga tidak boleh diabaikan apabila hukum tersebut memang mengatur pihak yang menyerahkan data atau tindakan yang menghasilkan bukti.

Pelanggaran terhadap hukum asing juga tidak otomatis membuat bukti harus dikesampingkan. Pertama-tama harus dipastikan bahwa hukum tersebut memang berlaku. Setelah itu baru dinilai apakah aturan yang dilanggar berhubungan langsung dengan kewenangan memperoleh data, izin yang diperlukan, larangan menyerahkan data, persetujuan

pemilik akun, atau batas akses terhadap sistem. Jika hubungannya tidak langsung, pelanggaran tersebut tidak semestinya otomatis membawa akibat berdasarkan Pasal 235.

Autentikasi tetap diperiksa secara tersendiri. Bukti yang diperoleh melalui cara yang sah belum tentu autentik. Sebaliknya, bukti yang terbukti asli dan tidak berubah belum tentu diperoleh secara sah. Karena itu, hakim harus memeriksa keduanya.

Dari seluruh pembahasan tersebut, persoalan utama bukti elektronik lintas negara setelah KUHAP 2025 sebenarnya dapat dirumuskan dengan sederhana. Yang dicari bukan hanya tempat data berada, tetapi juga cara data diperoleh, siapa yang memperoleh atau menyerahkannya, dasar kewenangan yang digunakan, hukum apa yang mengatur tindakan tersebut, dan apakah terdapat pelanggaran yang benar-benar memengaruhi keabsahan perolehan bukti.

Penulis tidak menawarkan gagasan baru bahwa data elektronik dapat melintasi batas negara. Hal itu sudah lama diketahui. Yang ingin penulis sampaikan adalah upaya menghubungkan Pasal 124 ayat (4), Pasal 235 ayat (3) sampai dengan ayat (5), dan UU 1/2006 sebagai sebuah cara pengujian bagi hakim untuk menentukan hukum yang relevan dan menilai akibatnya terhadap bukti elektronik lintas yurisdiksi.

Namun kerangka penafsiran saja belum cukup untuk jangka panjang. Pembentuk undang-undang tetap perlu memperjelas hubungan antara penyitaan di luar negeri, MLA, kewajiban penyedia layanan, berbagai cara memperoleh bukti elektronik, dan kemungkinan pertentangan antara hukum beberapa negara. Tanpa aturan yang lebih jelas, tindakan memperoleh bukti yang sebenarnya sama dapat dinilai berbeda karena hakim atau aparat menggunakan dasar hubungan hukum yang berbeda. Keadaan seperti itu dapat mengurangi kepastian hukum.