Wajah Hukum

Vol 10, No 2 (2026): Oktober, 1021-1034
Fakultas Hukum Universitas Batanghari Jambi
ISSN 2598-604X (Online) | DOI 10.33087/wjh.v10i2.2208

Konstruksi Pembuktian *Tempus Delicti* dan *Locus Delicti* dalam Tindak Pidana Siber di Indonesia Pasca Pembaruan KUHP dan KUHAP

Ariy Khaerudin, Ida Aryati Diyah Purnomo Wulan, Koko Noviana
Program Studi Magister Hukum, Fakultas Hukum, Universitas Islam Batik Surakarta
Correspondence: ari.khaerudin@gmail.com, idaaryatiwulan@gmail.com

Article Info

Keywords:
tempus delicti, locus delicti, Cybercrime, electronic evidence, digital forensics

Submitted: *14-08-2026*
Revised: *09-09-2026*
Accepted: *24-10-2026*
Published: *25-10-2026*

Abstract

Determining the time and place of a Cybercrime cannot be reduced to reading a single timestamp, Internet Protocol address, or server location, because the conduct, systems, data, victims, and effects may be distributed across jurisdictions and time zones. This study aims to analyse the evidentiary construction of tempus delicti and locus delicti following the entry into force of Law Number 1 of 2023 on the Penal Code and Law Number 20 of 2025 on the Criminal Procedure Code. It employs normative legal research with statutory, conceptual, case, and limited comparative approaches; legal materials are analysed qualitatively through grammatical, systematic, and teleological interpretation. The findings show that the Elucidation of Articles 10 and 11 of the Penal Code provides three normative points, namely the physical act, the operation of an instrument, and the occurrence of an effect, which must be linked to the elements of the offence. The article proposes a three-layer temporal construction, four locus nodes, a substantial-connection test, and a four-stage test covering legality of acquisition, authentication-integrity, attribution, and relevance-causation. Initial uncertainty about location and the offender's whereabouts is a matter for inquiry, not a ground for rejecting a report or complaint.

Kata Kunci:
tempus delicti, *locus delicti*, tindak pidana siber, bukti elektronik, forensik digital

Abstrak

Penentuan waktu dan tempat tindak pidana siber tidak dapat disamakan dengan pembacaan satu *timestamp*, alamat *Internet Protocol*, atau lokasi server karena perbuatan, sistem, data, korban, dan akibat dapat tersebar pada beberapa wilayah dan zona waktu. Penelitian ini bertujuan menganalisis konstruksi pembuktian *tempus delicti* dan *locus delicti* setelah berlakunya Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana dan Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana. Metode yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan, konseptual, kasus, dan perbandingan terbatas; bahan hukum dianalisis secara kualitatif melalui interpretasi gramatikal, sistematis, dan teleologis. Hasil penelitian menunjukkan bahwa Penjelasan Pasal 10 dan Pasal 11 KUHP menyediakan tiga titik normatif, yaitu perbuatan fisik, bekerjanya alat, dan timbulnya akibat, yang harus dipertautkan dengan unsur delik. Artikel ini menawarkan konstruksi tiga lapis *tempus*, empat simpul *locus*, uji hubungan substansial, serta uji empat tahap yang meliputi legalitas perolehan, autentikasi-integritas, atribusi, dan relevansi-kausalitas. Ketidakpastian awal mengenai tempat dan keberadaan pelaku merupakan objek penyelidikan, bukan alasan untuk menolak laporan atau pengaduan.

PENDAHULUAN

Ruang siber mengubah cara tindak pidana dilakukan dan cara fakta pidana dibuktikan. Dalam satu peristiwa, seseorang dapat mengendalikan akun dari perangkat bergerak, menggunakan koneksi yang dialihkan melalui *virtual private network*, mengakses layanan yang infrastrukturnya tersebar di beberapa negara, dan menimbulkan kerugian pada korban di wilayah pengadilan yang berbeda. Karena itu, tempat pelaku berada, tempat perangkat digunakan, lokasi infrastruktur, lokasi data, tempat korban menerima komunikasi, dan tempat akibat terjadi tidak selalu berimpit. Perbedaan zona waktu, konfigurasi sistem, dan kebijakan pencatatan juga dapat menghasilkan beberapa penanda waktu untuk satu rangkaian kejadian.

Literatur sebelum berlakunya KUHP dan KUHAP baru telah mengenali anonimitas, penyebaran server, penggunaan enkripsi, dan perbedaan zona waktu sebagai sumber ketidakpastian *tempus* dan *locus*.[1] Literatur tersebut juga menghubungkan ketidakpastian dengan kewenangan pengadilan, validitas dakwaan, dan efektivitas investigasi.[2] Akan tetapi, sebagian besar kajian masih dibangun di atas KUHP lama yang tidak merumuskan waktu dan tempat tindak pidana secara eksplisit serta Undang-Undang Nomor 8 Tahun 1981 tentang KUHAP. Rahmawati, misalnya, menggunakan teori perbuatan materiil, teori alat, dan teori akibat untuk menjelaskan *locus delicti* dalam perkara siber.[3] Kajian itu penting sebagai landasan doktrinal, tetapi pengaturannya kini perlu dibaca ulang karena KUHP Nasional telah mengadopsi rumusan waktu dan tempat tindak pidana, sedangkan KUHAP baru mengubah tata letak norma dakwaan, kompetensi relatif, dan pembuktian.[4]

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP) berlaku sejak 2 Januari 2026. Pasal 4 huruf c KUHP memperluas penerapan hukum pidana Indonesia terhadap tindak pidana di bidang teknologi informasi atau tindak pidana lain yang akibatnya dialami atau terjadi di wilayah Indonesia. Pasal 10 KUHP menyatakan bahwa waktu tindak pidana merupakan saat dilakukannya perbuatan yang dapat dipidana, sedangkan Pasal 11 KUHP menyatakan bahwa tempat tindak pidana merupakan tempat dilakukannya perbuatan yang dapat dipidana. Rumusan singkat tersebut memperoleh arti operasional dari Penjelasan Pasal 10 dan Pasal 11 KUHP: waktu dan tempat dapat ditautkan pada perbuatan fisik, bekerjanya alat atau bahan, dan timbul atau terjadinya akibat. Dengan demikian, pembaruan hukum bukan sekadar memindahkan doktrin ke dalam undang-undang, melainkan menyediakan kerangka untuk memilih titik yuridis dari sekumpulan peristiwa teknis.

Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana (KUHAP), yang juga berlaku sejak 2 Januari 2026, melalui Pasal 75 mengharuskan surat dakwaan menguraikan tindak pidana secara cermat, jelas, dan lengkap dengan menyebut waktu serta tempat; kekurangan pada syarat materiil itu mengakibatkan dakwaan batal demi hukum, dengan kesempatan satu kali bagi penuntut umum untuk memperbaikinya. Pasal 165 dan Pasal 167 KUHAP mengatur kompetensi relatif pengadilan untuk perkara di dalam beberapa daerah hukum maupun perkara yang dilakukan di luar negeri. Pada saat yang sama, Pasal 235 KUHAP menempatkan bukti elektronik sebagai salah satu alat bukti, mensyaratkan autentikasi serta perolehan yang tidak melawan hukum, dan menyerahkan penilaian tersebut kepada hakim. Pasal 242 KUHAP kemudian mencakup segala bentuk Informasi Elektronik, Dokumen Elektronik, dan/atau sistem elektronik yang berkaitan dengan tindak pidana.

Perubahan normatif itu belum dengan sendirinya menyelesaikan persoalan pembuktian. *Timestamp* dapat merekam waktu sistem, waktu aplikasi, waktu server, waktu penyedia layanan, atau waktu perubahan berkas. Alamat IP dapat bersifat dinamis, dibagi melalui *network address translation*, dialihkan, atau dipalsukan. Identitas pelanggan, pemilik rekening, dan pemilik perangkat juga tidak selalu sama dengan pengguna aktual. Pedoman NIST menggambarkan forensik digital sebagai proses pengumpulan, pemeriksaan, analisis, dan pelaporan yang harus menjaga integritas data.[5] Pedoman yang sama memperingatkan bahwa metode penyalinan tertentu dapat mengubah waktu berkas dan bahwa analisis garis waktu harus memperhatikan pengaturan tanggal, waktu, zona waktu, serta sinkronisasi antarsistem.[6] Alamat IP juga tidak boleh diperlakukan sebagai identitas seseorang tanpa korelasi, karena alamat dapat dialokasikan secara dinamis, berada di balik NAT, atau muncul melalui teknik anonimisasi dan *spoofing*.[7]

Kesenjangan penelitian terletak pada belum terintegrasinya tiga lapisan analisis. Pertama, lapisan normatif yang menentukan titik waktu dan tempat berdasarkan unsur delik. Kedua, lapisan prosedural

---

[1] Dwi Nugroho Marsudianto dan Evita Isretno Israhadi, "Uncertainty of Locus Delicti and Tempus Delicti as an Obstacle to Law Enforcement against Cybercrime," *Greenation International Journal of Law and Social Sciences, Volume 3, Nomor 2,* (2025): 114-117.

[2] *Ibid,* hlm. 117-120.

[3] Rahmawati, "Penentuan Tempus dan Locus Delicti dalam Cyber Crime," *Sol Justicia, Volume 3, Nomor 1,* (2020): 96-98.

[4] *Ibid,* hlm. 98-100.

[5] Karen Kent et al., *Guide to Integrating Forensic Techniques into Incident Response*, NIST Special Publication 800-86 (Gaithersburg: National Institute of Standards and Technology, 2006), hlm.3-7.

[6] *Ibid,* hlm. 4.

[7] *Ibid,* hlm. 6.

yang menguji yurisdiksi, kompetensi relatif, kecermatan dakwaan, dan legalitas bukti. Ketiga, lapisan teknis yang menilai sumber, integritas, akurasi, serta kemampuan artefak digital untuk mengatribusikan suatu perbuatan kepada orang tertentu. Kajian kasus yang dilakukan Simada dkk. menunjukkan pentingnya lokasi pelaku, lokasi korban, lokasi server, dan kompetensi relatif dalam praktik.[8] Namun, kajian berdasarkan perkara sebelum pembaruan hukum acara belum menjawab bagaimana autentikasi dan legalitas perolehan dalam Pasal 235 KUHAP baru harus disatukan dengan penentuan *tempus* dan *locus*.[9]

Berdasarkan kesenjangan tersebut, artikel ini bertujuan menganalisis konstruksi normatif *tempus delicti* dan *locus delicti* setelah berlakunya KUHP dan KUHAP baru, menjelaskan cara fakta teknis dari bukti elektronik ditransformasikan menjadi fakta hukum mengenai waktu, tempat, dan pelaku, serta merumuskan model pengujian yang dapat mencegah perluasan yurisdiksi dan atribusi pelaku secara spekulatif. Kebaruan penelitian berupa integrasi konstruksi tiga lapis *tempus*, empat simpul *locus*, uji hubungan substansial, dan uji pembuktian empat tahap. Model ini dimaksudkan sebagai kerangka argumentasi, bukan rumus mekanis yang menggantikan penilaian hakim.

METODE

1. Pendekatan

   Penelitian ini merupakan penelitian hukum normatif yang bersifat preskriptif. Pendekatan yang digunakan terdiri atas pendekatan perundang-undangan (*statute approach*), konseptual (*conceptual approach*), kasus (*case approach*), dan perbandingan terbatas (*comparative approach*). Pendekatan perundang-undangan digunakan untuk memeriksa hubungan antara yurisdiksi, waktu dan tempat tindak pidana, kompetensi relatif, syarat dakwaan, serta bukti elektronik. Pendekatan konseptual digunakan untuk membedakan fakta teknis dari fakta yuridis dan untuk mengembangkan konsep atribusi serta hubungan substansial. Pendekatan kasus diarahkan pada Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016 mengenai legalitas informasi atau dokumen elektronik dalam penegakan hukum. Pendekatan perbandingan terbatas menggunakan NIST SP 800-86, ISO/IEC 27037:2012, *Budapest Convention on Cybercrime*, dan *United Nations Convention against Cybercrime* sebagai bahan evaluasi, bukan sebagai norma nasional yang otomatis berlaku.[10]
2. Rancangan Kegiatan

   Rancangan kegiatan penelitian disusun dalam empat tahap, yaitu inventarisasi bahan hukum yang relevan, klasifikasi norma menurut isu yurisdiksi, waktu dan tempat tindak pidana, kompetensi relatif, syarat dakwaan, dan bukti elektronik, interpretasi dan korelasi norma dengan pedoman forensik digital serta penyusunan preskripsi dalam bentuk konstruksi, uji, dan matriks pembuktian.
3. Ruang Lingkup Atau Objek

   Ruang lingkup atau objek penelitian adalah norma mengenai *tempus delicti*, *locus delicti*, yurisdiksi, kompetensi relatif, dan bukti elektronik dalam KUHP dan KUHAP yang berlaku sejak 2 Januari 2026, dengan fokus pada pola perkara akses tanpa hak, gangguan sistem, penipuan daring, dan distribusi konten elektronik.
4. Bahan Dan Alat Utama

   Bahan hukum utama terdiri atas bahan hukum primer dan sekunder. Bahan hukum primer meliputi Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana sebagaimana telah diubah dengan Undang-Undang Nomor 1 Tahun 2026 tentang Penyesuaian Pidana, Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana terakhir diubah dengan Undang-Undang Nomor 1 Tahun 2024, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Peraturan Kepolisian Negara Republik Indonesia Nomor 7 Tahun 2022 tentang Kode Etik Profesi dan Komisi Kode Etik Kepolisian Negara Republik Indonesia, serta Putusan Mahkamah Konstitusi Nomor 20/PUU-

[8] Arthur Simada et al., "Penentuan Locus Delictie dalam Tindak Pidana Cyber Crime (Merusak dan Mengganggu Sistem Elektronik dan Komunikasi Milik Orang Lain)," *Locus Journal of Academic Literature Review, Volume 3, Nomor 4,* (2024): 356-359, https://doi.org/10.56128/ljoalr.v3i4.314.

[9] *Ibid,* hlm. 359-360.

[10] Karen Kent dkk, *Op.Cit,* hlm.5-7.

XIV/2016. Bahan hukum sekunder meliputi artikel jurnal, standar teknis forensik digital, dan instrumen internasional di bidang kejahatan siber. Alat utama penelitian berupa lembar inventarisasi dan matriks analisis bahan hukum.

5. Tempat

   Tempat penelitian tidak terikat pada lokasi lapangan tertentu karena penelitian dilakukan melalui studi kepustakaan terhadap dokumen hukum resmi dan literatur, baik cetak maupun daring.

6. Teknik Pengumpulan Data

   Teknik pengumpulan data dilakukan melalui studi dokumen (*library research*), yaitu penelusuran, pencatatan, dan pengelompokan bahan hukum sesuai isu penelitian.

7. Definisi Operasional Variabel Penelitian

   Definisi operasional konsep penelitian adalah sebagai berikut. *Tempus delicti* adalah waktu dilakukannya perbuatan yang dapat dipidana sebagaimana dimaksud Pasal 10 KUHP beserta Penjelasannya. *Locus delicti* adalah tempat dilakukannya perbuatan yang dapat dipidana sebagaimana dimaksud Pasal 11 KUHP beserta Penjelasannya, yang dapat berupa tempat perbuatan fisik, tempat bekerjanya alat atau bahan, atau tempat timbulnya akibat. Tindak pidana siber adalah tindak pidana yang dilakukan dengan menggunakan atau menyasar sistem elektronik, informasi elektronik, atau dokumen elektronik. Bukti elektronik adalah alat bukti sebagaimana dimaksud Pasal 235 dan Pasal 242 KUHAP. Atribusi adalah proses menghubungkan suatu artefak digital dengan orang tertentu sebagai pelaku.

8. Teknik Analisis

   Teknik analisis dilakukan secara kualitatif melalui inventarisasi, klasifikasi, interpretasi, dan preskripsi. Interpretasi gramatikal dipakai untuk membaca frasa "perbuatan yang dapat dipidana " dalam Pasal 10 dan Pasal 11 KUHP. Interpretasi sistematis menghubungkan pasal tersebut dengan Pasal 4 KUHP, Pasal 75, Pasal 165, Pasal 167, Pasal 235, dan Pasal 242 KUHAP. Interpretasi teleologis digunakan untuk menyeimbangkan efektivitas penegakan hukum, kepastian yurisdiksi, pelindungan privasi, dan hak terdakwa untuk menguji bukti. Preskripsi kemudian disusun dalam bentuk matriks yang dapat diterapkan pada berbagai pola tindak pidana siber.

HASIL

Pergeseran Kerangka Normatif Setelah KUHP Dan KUHAP Baru

Pembaruan KUHP mengubah titik berangkat perdebatan. Dalam rezim lama, teori perbuatan, teori alat, dan teori akibat berkembang terutama melalui ilmu hukum dan praktik. Dalam rezim baru, batang tubuh Pasal 10 dan Pasal 11 Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana memang menekankan "perbuatan yang dapat dipidana ", tetapi Penjelasan kedua pasal tersebut secara eksplisit menyebut tiga kemungkinan: perbuatan fisik, bekerjanya alat atau bahan, dan akibat. Norma tersebut tidak membenarkan pemilihan titik waktu atau tempat secara bebas. Pemilihan harus mengikuti rumusan delik yang didakwakan, bentuk penyertaan, tahapan pelaksanaan, dan hubungan kausal.

Pada delik formil, titik dominan berada pada selesainya perbuatan yang dilarang, walaupun akibat dapat membantu pembuktian. Pada delik materiil, akibat merupakan unsur sehingga waktu dan tempat terjadinya akibat memiliki kedudukan normatif. Pada percobaan, titik relevan terletak pada permulaan pelaksanaan yang langsung menuju penyelesaian delik. Dalam penyertaan, lebih dari satu pelaku dapat melakukan kontribusi pada tempat dan waktu yang berbeda. Karena itu, istilah "satu tindak pidana " tidak selalu berarti satu koordinat dan satu detik.

Pasal 4 huruf c Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana memperkuat dimensi akibat untuk tindak pidana teknologi informasi dan tindak pidana lain yang akibatnya dialami atau terjadi di Indonesia. Ketentuan tersebut adalah norma yurisdiksi negara, bukan bukti otomatis bahwa setiap pengadilan di Indonesia berwenang secara relatif. Yurisdiksi menjawab apakah hukum pidana Indonesia dapat diterapkan; kompetensi relatif menjawab pengadilan negeri mana yang berwenang memeriksa; pembuktian menjawab apakah titik perbuatan, alat, atau akibat yang diklaim benar-benar terbukti. Mencampurkan ketiganya berisiko menghasilkan argumen melingkar: akibat dianggap terjadi di Indonesia karena hukum Indonesia diterapkan, sementara hukum Indonesia diterapkan karena akibat dianggap terjadi di Indonesia.

Untuk mencegah perluasan tanpa batas, tempat akibat harus memenuhi uji hubungan substansial. Pertama, akibat tersebut harus merupakan unsur delik atau konsekuensi yang secara yuridis relevan.

Kedua, akibat harus mempunyai hubungan kausal dengan perbuatan yang didakwakan. Ketiga, hubungan dengan Indonesia tidak boleh hanya berupa aksesibilitas konten secara kebetulan. Keempat, penggunaan forum harus dapat diperkirakan secara wajar oleh pelaku berdasarkan sasaran, korban, sistem, atau akibat yang dituju. Kelima, pemilihan forum tidak boleh meniadakan kesempatan terdakwa untuk membela diri secara efektif.

KUHAP baru memisahkan isu itu pada tahapan prosedural. Pasal 75 Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana memerintahkan penuntut umum menyebutkan waktu dan tempat dalam uraian yang cermat, jelas, dan lengkap. Dalam perkara siber, syarat tersebut tidak harus selalu dinyatakan dengan satu waktu tunggal. Rentang waktu dapat digunakan apabila perbuatan berlangsung berulang, log hanya menyediakan ketelitian tertentu, atau terdapat proses konversi zona waktu. Namun, rentang harus mempunyai batas rasional dan dikaitkan dengan tindakan yang memenuhi unsur. Formula "pada waktu yang tidak dapat ditentukan " tidak boleh menjadi pengganti kekurangan penyidikan.

Kompetensi relatif diatur dalam Pasal 165 Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana. Pengadilan negeri pada prinsipnya berwenang terhadap tindak pidana yang dilakukan di daerah hukumnya. Norma itu dilengkapi pilihan berdasarkan tempat tinggal atau ditemukannya terdakwa, kedekatan sebagian besar saksi, beberapa tindak pidana dalam beberapa daerah hukum, dan satu tindak pidana yang berlangsung pada beberapa daerah hukum. Untuk perbuatan di luar negeri yang dapat diadili menurut hukum Indonesia, Pasal 167 KUHAP menunjuk pengadilan negeri di ibu kota negara, dengan persyaratan yang dirumuskan oleh pasal tersebut. Oleh sebab itu, dakwaan perkara siber perlu menyebut fungsi setiap lokasi: lokasi tindakan inti, lokasi alat bekerja, lokasi akibat, atau dasar alternatif kompetensi relatif.

Matriks 1. Pergeseran kerangka pembuktian setelah KUHP dan KUHAP baru

Aspek	Sebelum	Setelah 2 Januari 2026	Implikasi
Waktu tindak pidana	Bertumpu pada doktrin dan interpretasi	Pasal 10 KUHP beserta Penjelasan	Titik waktu harus dipilih menurut unsur dan tiga kemungkinan normatif
Tempat tindak pidana	Bertumpu pada doktrin dan praktik	Pasal 11 KUHP beserta Penjelasan	Tempat dapat mencakup lokasi perbuatan fisik, bekerjanya alat, atau timbulnya akibat
Yurisdiksi siber	Tersebar pada asas teritorial dan undang-undang sektoral	Pasal 4 huruf c KUHP	Akibat di Indonesia dapat menjadi dasar yurisdiksi, tetapi keberadaan akibat tetap harus dibuktikan
Syarat dakwaan	Pasal 143 KUHAP lama	Pasal 75 KUHAP baru	Waktu dan tempat tetap merupakan syarat materiil dakwaan
Kompetensi relatif	Pasal 84 -86 KUHAP lama	Pasal 165 -167 KUHAP baru	Perkara multi-lokus harus dipetakan menurut dasar forum yang paling tepat
Bukti elektronik	UU ITE dan undang-undang khusus	Pasal 235 dan Pasal 242 KUHAP baru	Autentikasi dan legalitas perolehan menjadi perintah eksplisit

Sumber: diolah oleh penulis berdasarkan KUHP dan KUHAP.

Konstruksi Tiga Lapis Tempus Delicti

Kekeliruan yang umum terjadi adalah menyamakan *timestamp* dengan *tempus delicti*. *Timestamp* hanya data yang dihasilkan oleh suatu sistem berdasarkan jam, konfigurasi, dan peristiwa teknis tertentu. *Tempus delicti* adalah kesimpulan hukum mengenai kapan perbuatan yang dapat dipidana dilakukan. Untuk menjembatani keduanya, artikel ini membedakan tiga lapisan.

Lapisan pertama adalah *tempus normatif*, yakni waktu yang dituntut oleh rumusan delik. Pertanyaannya bukan "jam berapa yang tercatat ", melainkan "peristiwa apa yang membuat unsur

delik terpenuhi ". Dalam akses tanpa hak, titik tersebut dapat berupa keberhasilan memperoleh akses atau permulaan pelaksanaan yang relevan. Dalam gangguan sistem, titiknya dapat berupa saat perintah berbahaya bekerja atau ketika sistem terganggu. Dalam penipuan daring, rangkaian dapat meliputi penyampaian tipu muslihat, keputusan korban, transfer, penerimaan dana, dan penguasaan hasil. Hanya titik yang berkaitan dengan unsur yang layak ditempatkan dalam dakwaan sebagai *tempus* utama.

Lapisan kedua adalah *tempus teknis*, yaitu waktu yang direkam oleh perangkat atau layanan. Satu peristiwa dapat muncul dalam log aplikasi, sistem operasi, *firewall*, penyedia layanan, bank, atau operator telekomunikasi. Masing-masing dapat menggunakan UTC, waktu lokal, atau format lain. NIST menekankan bahwa garis waktu dapat terganggu oleh perbedaan pengaturan waktu yang disengaja maupun tidak disengaja, dan analis perlu mengetahui tanggal, waktu, zona waktu, serta cara alat menampilkan waktu pembuatan, akses, dan perubahan berkas.[11] Karena itu, laporan forensik harus menyatakan sumber jam, zona waktu asli, metode konversi, ketelitian, dan penyimpangan yang ditemukan.

Lapisan ketiga adalah *tempus evidensial*, yakni tingkat keyakinan yang dapat ditarik setelah beberapa sumber waktu dikorelasikan. Waktu pada perangkat yang tidak tersinkronisasi memiliki bobot berbeda dari waktu server yang tercatat secara terpusat. Waktu pada tangkapan layar merupakan representasi tampilan, bukan otomatis waktu asli pada basis data. Waktu pembuatan berkas dapat berubah ketika berkas disalin dengan metode tertentu.[12] Karena itu, *tempus evidensial* harus dinyatakan sebagai waktu pasti, rentang, atau urutan relatif sesuai kualitas data bukan dipaksakan menjadi ketelitian detik apabila sumber hanya mendukung ketelitian menit atau jam.

Konstruksi tiga lapis menghasilkan langkah analisis berikut. Pertama, uraikan unsur delik dan tentukan peristiwa yang relevan secara normatif. Kedua, inventarisasi semua sumber waktu. Ketiga, normalisasi zona waktu tanpa menghilangkan data asli. Keempat, ukur selisih jam antarsistem dengan peristiwa pembanding. Kelima, susun garis waktu yang membedakan observasi dan inferensi. Keenam, tetapkan tingkat kepastian serta alternatif penjelasan. Dengan langkah ini, perbedaan dua jam tidak langsung dianggap manipulasi; perbedaan dapat berasal dari zona waktu, *daylight saving time*, konfigurasi perangkat, keterlambatan pencatatan, atau proses ekspor.

Empat Simpul Locus dan Uji Hubungan Substansial

Locus delicti dalam perkara siber lebih tepat dipetakan sebagai beberapa simpul daripada dicari sebagai satu titik geografis sejak awal. Simpul pertama adalah pelaku dan perangkat, yakni tempat seseorang secara fisik mengoperasikan, menguasai, atau mengarahkan sarana. Simpul kedua adalah jaringan dan sistem, yaitu tempat koneksi, layanan, atau instrumen teknis bekerja. Simpul ketiga adalah data atau objek, yaitu tempat data yang diserang, dipindahkan, diubah, atau dikuasai berada secara logis dan, bila relevan, secara fisik. Simpul keempat adalah korban dan akibat, yaitu tempat komunikasi diterima, kerugian timbul, layanan terganggu, atau akibat lain yang merupakan unsur terjadi.

Keempat simpul tidak mempunyai bobot yang selalu sama. Lokasi server dapat relevan sebagai tempat alat bekerja, tetapi tidak otomatis membuktikan lokasi pelaku. Lokasi korban dapat relevan sebagai tempat akibat, tetapi tidak otomatis menjadi *locus* jika akibat tersebut bukan unsur atau tidak mempunyai hubungan kausal yang cukup. Alamat IP dapat membantu menelusuri titik koneksi, namun karakter dinamis, NAT, *proxy*, VPN, dan *spoofing* menuntut korelasi dengan data pelanggan pada waktu tertentu, log alokasi, perangkat, kredensial, dan bukti lain.[13]

Uji hubungan substansial digunakan untuk memilih simpul yang memiliki arti yuridis. Uji tersebut mencakup: (a) keterkaitan simpul dengan unsur delik; (b) kekuatan hubungan kausal; (c) kesengajaan atau keterarahan perbuatan terhadap sistem, orang, atau kepentingan di wilayah tersebut; (d) kualitas bukti yang menempatkan peristiwa pada simpul itu; dan (e) kewajaran forum bagi penuntutan dan pembelaan. Uji ini menolak dua ekstrem. Ekstrem pertama menyatakan bahwa hanya lokasi tubuh pelaku yang relevan. Ekstrem kedua menganggap setiap tempat konten dapat diakses sebagai *locus*. Keduanya mengabaikan Penjelasan Pasal 11 KUHP dan fungsi perlindungan hukum acara.

[11] Kent dkk, *Op.Cit*, hlm. 4.
[12] *Ibid,* hlm. 4-5.
[13] *Ibid,* hlm. 5 dan 6.

Dalam serangan terhadap sistem, lokasi perangkat pengendali, *command-and-control server*, sistem sasaran, dan tempat gangguan dirasakan dapat seluruhnya relevan. Namun, dakwaan harus menyebut mengapa suatu lokasi dipilih. Apabila dasar utama adalah tempat alat bekerja, bukti harus menunjukkan fungsi alat tersebut dalam penyelesaian tindak pidana. Apabila dasar utama adalah tempat akibat, bukti harus menunjukkan bahwa akibat yang terjadi bukan sekadar konsekuensi jauh atau kebetulan.

Dalam penipuan daring, tempat korban membaca pesan, membuat keputusan, melakukan transfer, dan mengalami kerugian dapat berbeda. Tempat rekening penerima terdaftar juga belum tentu tempat pelaku menguasai dana. Rekening *nominee*, perbankan digital, dan penarikan melalui pihak ketiga memisahkan identitas administratif dari pengendali aktual. Oleh karena itu, pemetaan *locus* harus diikuti pembuktian atribusi, bukan berhenti pada nama pemilik rekening.

Kedudukan, Legalitas, dan Autentikasi Bukti Elektronik

Pasal 235 ayat (1) Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana menyebut bukti elektronik secara mandiri. Ayat (3) sampai dengan ayat (5) pasal tersebut menetapkan tiga konsekuensi: autentikasi harus dapat dibuktikan; perolehan tidak boleh melawan hukum; dan bukti yang dinyatakan tidak autentik atau diperoleh secara melawan hukum tidak dapat digunakan serta tidak memiliki kekuatan pembuktian. Pasal 242 KUHAP memperluas cakupan bukti elektronik hingga Informasi Elektronik, Dokumen Elektronik, dan/atau sistem elektronik yang berkaitan dengan tindak pidana. Rumusan tersebut mengakhiri perdebatan mengenai apakah bukti elektronik hanya perlu diposisikan sebagai perluasan alat bukti lain, tetapi tidak menghapus persyaratan teknis dan prosedural.

Pasal 5 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana terakhir diubah dengan Undang-Undang Nomor 1 Tahun 2024 (UU ITE) tetap memberikan dasar bahwa Informasi Elektronik, Dokumen Elektronik, dan hasil cetaknya merupakan alat bukti hukum yang sah, dengan pengecualian untuk dokumen yang menurut undang-undang harus dibuat tertulis atau dalam bentuk akta notaris/pejabat pembuat akta. Ketentuan itu harus dibaca bersama Pasal 16 UU ITE yang mensyaratkan bahwa sistem elektronik mampu menampilkan kembali informasi secara utuh, menjaga ketersediaan, keutuhan, keautentikan, kerahasiaan, dan keteraksesan sesuai ketentuan hukum. Dengan demikian, hasil cetak tidak menggantikan kebutuhan untuk menjelaskan sumber elektroniknya ketika keaslian, kelengkapan, atau konteks dipersoalkan.

Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016 memberi dasar konstitusional terhadap legalitas perolehan, terutama dalam konteks informasi atau dokumen elektronik yang diperoleh melalui intersepsi untuk penegakan hukum. Mahkamah menekankan perlunya intersepsi dilakukan secara sah dan memasukkan pembatasan itu dalam amar putusan. KUHAP baru kemudian merumuskan legalitas perolehan sebagai syarat umum alat bukti. Konsekuensinya, penilaian tidak cukup berhenti pada pertanyaan apakah data "asli "; hakim juga perlu menilai siapa yang memperoleh, berdasarkan kewenangan apa, melalui prosedur apa, dalam lingkup apa, dan apakah penggunaan data sejalan dengan tujuan perolehannya.

Autentikasi berbeda dari atribusi. Autentikasi menjawab apakah data adalah data yang diklaim, berasal dari sumber yang dijelaskan, dan tidak berubah secara material. Atribusi menjawab apakah data tersebut dapat dihubungkan kepada orang tertentu. Sebuah log yang autentik dapat membuktikan bahwa akun digunakan dari alamat IP tertentu, tetapi belum tentu membuktikan siapa pengguna aktual. Sebaliknya, penguasaan perangkat oleh terdakwa tidak otomatis membuktikan bahwa seluruh aktivitas pada perangkat dilakukan olehnya.

Nilai *hash* dapat membantu memverifikasi apakah salinan data berubah setelah akuisisi, tetapi *hash* bukan sertifikat kebenaran isi dan bukan bukti identitas pelaku. NIST menjelaskan penggunaan *message digest* untuk membandingkan salinan dengan sumbernya.[14] Namun, autentikasi tetap memerlukan dokumentasi konteks: identitas barang, kondisi awal, metode akuisisi, alat dan versinya, waktu akuisisi, petugas, media penyimpanan, perpindahan penguasaan, dan tindakan pemeriksaan.

Rantai penguasaan (*chain of custody*) menjaga keterlacakan sejak identifikasi sampai penyajian. Dokumentasi ideal mencatat setiap orang yang menguasai bukti, tindakan yang dilakukan, waktu dan tempat tindakan, penyimpanan, pembuatan salinan kerja, serta verifikasi integritas sumber dan

[14] Kent dkk, *Op.Cit*, hlm. 4.

salinan.[15] ISO/IEC 27037:2012 melengkapi prinsip itu melalui pedoman identifikasi, pengumpulan, akuisisi, dan preservasi bukti digital potensial.[16] Standar teknis tersebut bukan dasar kewenangan penggeledahan, penyitaan, atau permintaan data; kewenangan tetap harus berasal dari hukum nasional.

Pelindungan data pribadi menuntut pembatasan tujuan, relevansi, dan keamanan. Perangkat dapat memuat komunikasi keluarga, data kesehatan, biometrik, data keuangan, foto, dan informasi pihak ketiga yang tidak berkaitan dengan perkara. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, antara lain dalam Pasal 16, Pasal 20, Pasal 35, dan Pasal 36, mengatur dasar pemrosesan, prinsip pemrosesan, serta kewajiban pengendali dan prosesor data. Dalam konteks pembuktian, akuisisi forensik menyeluruh mungkin dibutuhkan untuk mempertahankan struktur data, tetapi pencarian, analisis, pengungkapan, dan penyajian harus dibatasi pada tujuan penegakan hukum yang sah serta data yang relevan.

Transformasi Artefak Digital Menjadi Fakta Yuridis

Artefak digital tidak "berbicara sendiri ". Ia dihasilkan oleh perangkat lunak dan perangkat keras berdasarkan konfigurasi tertentu. Karena itu, transformasi dari artefak menjadi fakta yuridis harus menjelaskan rangkaian inferensi. Untuk *timestamp*, rangkaian tersebut meliputi peristiwa yang memicu pencatatan, sumber jam, zona waktu, sinkronisasi, format, ketelitian, kemungkinan perubahan, dan konversi. Untuk alamat IP, rangkaian meliputi sumber log, waktu, *port*, protokol, log alokasi pelanggan, NAT, VPN, dan korelasi perangkat. Untuk akun, rangkaian meliputi pendaftaran, penguasaan kredensial, autentikasi, pemulihan akun, perangkat yang pernah masuk, dan kemungkinan penggunaan bersama.

Tangkapan layar adalah representasi visual pada waktu tertentu. Ia dapat berguna untuk menunjukkan apa yang dilihat saksi, tetapi biasanya tidak memuat keseluruhan percakapan, *header*, identitas sumber, log server, atau riwayat perubahan. Oleh karena itu, tangkapan layar sebaiknya dikorelasikan dengan ekspor data asli, perangkat sumber, data platform, atau keterangan saksi. Apabila hanya tangkapan layar yang tersedia, keterbatasannya harus dinilai dalam bobot pembuktian, bukan disembunyikan.

Metadata juga harus dibaca sesuai konteks. Waktu pembuatan dapat berarti saat berkas dibuat pada suatu media, bukan saat isi pertama kali diciptakan. Waktu modifikasi dapat berubah karena penyuntingan atau proses aplikasi. Waktu akses dapat berubah akibat pemeriksaan yang tidak tepat. Penyalinan logis dengan alat tertentu juga dapat mengubah waktu pembuatan pada salinan.[17] Dengan demikian, satu kolom metadata tidak cukup untuk menyimpulkan kronologi tanpa memahami sistem berkas dan metode akuisisi.

Analisis multi-sumber merupakan pengaman terhadap salah inferensi. NIST menunjukkan bahwa peristiwa dapat dikorelasikan dari berkas, sistem operasi, lalu lintas jaringan, dan aplikasi untuk memperoleh gambaran yang lebih akurat.[18] Korelasi yang baik menggunakan sumber yang relatif independen. Log aplikasi dan tampilan yang dihasilkan dari basis data yang sama bukan dua bukti independen. Sebaliknya, log platform, catatan operator, mutasi bank, artefak perangkat, CCTV, dan keterangan saksi dapat saling menguatkan apabila asal serta mekanisme pembentukannya berbeda.

Matriks 2. Daya bukti artefak digital dan kebutuhan korelasinya

Artefak	Fakta minimum	Belum otomatis terbukti	Korelasi yang diperlukan
Timestamp	Sistem mencatat peristiwa pada nilai waktu tertentu	Waktu hukum, ketepatan jam, dan pelaku	Zona waktu, NTP, log lain, serta peristiwa pembanding
Alamat IP	Koneksi tercatat menggunakan alamat tertentu	Identitas dan lokasi fisik pengguna	Log alokasi, port, NAT, perangkat, akun, dan data operator

[15] *Ibid,* hlm. 3-4.

[16] International Organization for Standardization, *Information Technology Security Techniques Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*, ISO/IEC 27037:2012 (Geneva: ISO, 2012), klausul 5-7.

[17] Kent dkk, *Op.Cit*, hlm. 4.

[18] *Ibid,* hlm. 8.

Artefak	Fakta minimum	Belum otomatis terbukti	Korelasi yang diperlukan
Akun	Aktivitas terjadi melalui identitas akun	Pengguna aktual dan kesengajaan	Riwayat masuk, perangkat, kredensial, serta komunikasi
Tangkapan layar	Tampilan tertentu dilihat atau disimpan	Keutuhan, asal, konteks, dan riwayat perubahan	Data asli, ekspor platform, perangkat, dan saksi
Metadata berkas	Atribut teknis tercatat pada berkas	Waktu penciptaan isi dan identitas pembuat	Sistem berkas, metode penyalinan, serta log aplikasi
Lokasi perangkat	Perangkat menghasilkan atau menyimpan data lokasi	Lokasi pasti pengguna pada setiap saat	Akurasi sensor, izin aplikasi, BTS/Wi-Fi, dan saksi
Mutasi rekening	Dana bergerak antarrekening	Pengendali rekening dan unsur tipu muslihat	Komunikasi, KYC, perangkat bank, CCTV, dan aliran lanjutan

Sumber: diolah oleh penulis berdasarkan norma autentikasi KUHAP dan pedoman forensik digital.

Uji Pembuktian Empat Tahap

Artikel ini menawarkan uji berurutan untuk menilai penggunaan artefak digital dalam pembuktian *tempus*, *locus*, dan pelaku.

1. Tahap pertama: legalitas perolehan. Pertanyaan utama mencakup dasar kewenangan, izin atau penetapan yang dibutuhkan, ruang lingkup, prosedur penggeledahan dan penyitaan, permintaan data, intersepsi, serta pembatasan penggunaan. Bukti yang relevan secara teknis dapat kehilangan kedudukan pembuktian apabila diperoleh secara melawan hukum sebagaimana konsekuensi Pasal 235 KUHAP. Penilaian perlu membedakan data yang diserahkan sukarela oleh pemilik, data yang diambil dari perangkat, data yang diperoleh dari penyelenggara sistem elektronik, dan data hasil intersepsi karena dasar kewenangannya tidak selalu sama.
2. Tahap kedua: autentikasi dan integritas. Pemeriksa menilai sumber data, cara pembentukan, keutuhan, kelengkapan, *hash*, *audit trail*, dan *chain of custody*. Pertanyaan tidak terbatas pada ada atau tidaknya perubahan. Data yang utuh tetapi berasal dari akun yang keliru tetap tidak autentik terhadap proposisi yang hendak dibuktikan. Sebaliknya, perubahan format yang terdokumentasi tidak selalu merusak nilai bukti apabila data sumber tersedia dan transformasinya dapat direplikasi.
3. Tahap ketiga: atribusi. Pemeriksa menilai hubungan antara artefak dengan orang. Atribusi dibangun dari kombinasi penguasaan perangkat, akses eksklusif, kredensial, biometrik, pola penggunaan, isi komunikasi, data pelanggan, hubungan rekening, saksi, dan perilaku sebelum atau sesudah peristiwa. Identitas administratif adalah titik awal, bukan kesimpulan. Semakin mudah akun, perangkat, atau jaringan digunakan bersama, semakin kuat kebutuhan akan korelasi independen.
4. Tahap keempat: relevansi dan kausalitas. Data yang sah, autentik, dan teratribusi masih harus dihubungkan dengan unsur delik, waktu, tempat, dan akibat. Contohnya, keberadaan perangkat di suatu lokasi tidak otomatis membuktikan bahwa perintah dikirim dari lokasi itu; artefak mungkin merupakan hasil sinkronisasi dari perangkat lain. Demikian pula, transfer dana kepada rekening terdakwa tidak otomatis membuktikan penipuan tanpa hubungan dengan komunikasi yang menggerakkan korban.

Keempat tahap harus dibedakan tetapi dibaca sebagai satu rangkaian. Kegagalan legalitas dapat menutup penggunaan bukti. Kelemahan autentikasi dapat menurunkan keandalan. Kelemahan atribusi membatasi kesimpulan mengenai pelaku. Ketiadaan relevansi atau kausalitas memutus hubungan dengan unsur delik. Struktur ini membantu hakim menjelaskan alasan penerimaan dan bobot bukti secara transparan.

Penerapan Model pada Pola Perkara Siber

1. Akses Tanpa Hak dan Gangguan Sistem

   Penyidik terlebih dahulu menentukan perbuatan inti menurut pasal yang diterapkan: percobaan masuk, akses berhasil, eskalasi hak, pengambilan data, penanaman program, atau gangguan sistem. *Tempus normatif* tidak selalu sama dengan waktu pertama alamat IP muncul. Log autentikasi, sistem operasi, *firewall*, *intrusion detection system*, DHCP, dan data penyedia layanan

kemudian dipetakan ke zona waktu yang sama. Apabila terdapat serangan dari banyak alamat, kemungkinan botnet dan *spoofing* harus diuji; NIST mengingatkan bahwa kecocokan alamat tidak dengan sendirinya memastikan alamat penyerang.[19]

Empat simpul *locus* dapat berupa lokasi perangkat pengendali, jaringan perantara, sistem sasaran, dan tempat gangguan dialami. Lokasi server perantara tidak otomatis dipilih sebagai tempat pelaku. Apabila akibat gangguan dialami oleh sistem di Indonesia, Pasal 4 huruf c Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana dapat menjadi dasar yurisdiksi, tetapi bukti harus menunjukkan hubungan serangan dengan gangguan tersebut. Atribusi kepada terdakwa memerlukan artefak perangkat, riwayat perintah, kepemilikan atau penguasaan infrastruktur, komunikasi, pembayaran layanan, dan bukti lain.

2. Penipuan Daring dan Aliran Dana

Garis waktu penipuan seharusnya memisahkan pembuatan identitas, komunikasi awal, penyampaian tipu muslihat, keputusan korban, transfer, penerimaan, dan pemindahan dana. Waktu platform dan waktu bank dapat berbeda; keduanya perlu dinormalisasi dan tidak boleh dipaksa sama. Tempat korban menerima pesan dan mengambil keputusan dapat relevan, demikian pula tempat kerugian terjadi dan tempat dana dikuasai. Namun, *locus* yang dipilih harus dihubungkan dengan unsur pasal dan kompetensi relatif.

Data rekening membuktikan aliran dana, bukan seluruh unsur penipuan. Atribusi memerlukan data pembukaan rekening, perangkat perbankan, alamat IP, nomor telepon, CCTV penarikan, komunikasi dengan korban, dan aliran lanjutan. Rekening yang dibuka atas nama pihak lain atau dijual kepada pelaku menuntut pemisahan antara pemilik formal, pengendali, dan penerima manfaat. Uji empat tahap mencegah pemilik formal otomatis diposisikan sebagai pelaku utama tanpa bukti kesengajaan.

3. Distribusi Konten dan Komunikasi Elektronik

Dalam perkara distribusi konten, *tempus normatif* ditentukan oleh kata kerja delik: membuat dapat diakses, mentransmisikan, mendistribusikan, mengirim, atau tindakan lain yang dirumuskan undang-undang. Waktu pembuatan berkas tidak selalu sama dengan waktu unggah. Waktu tangkapan layar tidak selalu sama dengan waktu publikasi. Riwayat platform, URL, identitas unggahan, perangkat, dan saksi penerima perlu dikorelasikan.

Lokasi pengguna, sistem platform, penerima, dan akibat dapat berada di tempat berbeda. Aksesibilitas dari suatu wilayah saja belum cukup; harus ada hubungan substansial dengan sasaran, penerima, atau akibat yang dimaksud delik. Apabila akun diduga diretas atau digunakan bersama, atribusi membutuhkan riwayat masuk, notifikasi keamanan, pergantian kata sandi, perangkat yang dikenal, dan tindakan pemulihan akun.

4. Matriks Operasional

Matriks 3. Operasional pembuktian perkara siber

Pola perkara	Tempus	Sumber waktu	Locus	Atribusi	Risiko pembelaan
Akses tanpa hak	Saat akses atau permulaan pelaksanaan	Log autentikasi, sistem operasi, dan firewall	Perangkat, jaringan, dan sistem sasaran	Perangkat, kredensial, serta log ISP	IP dinamis, VPN atau akun bersama
Gangguan sistem	Saat perintah bekerja atau akibat timbul	IDS, log aplikasi dan laporan insiden	Pengendal, alat, sistem, dan tempat akibat	Malware, konfigurasi serta komunikasi	Botnet, false positive, atau jam tidak sinkron
Tipu muslihat daring	Saat representasi palsu diterima dan	Percakapan, surel, dan log platform	Pelaku, korban, serta sistem komunikasi	Akun, perangkat, dan isi pesan	percakapan tidak utuh atau akun diretas

[19] *Ibid,* hlm. 6-17.

Pola perkara	Tempus	Sumber waktu	Locus	Atribusi	Risiko pembelaan
	memengaruhi korban				
Transfer kerugian	Saat debit, kredit, atau penguasaan dana	Sistem core banking dan aplikasi bank	Korban, rekening, dan pengendali dana	Data KYC, perangkat, CCTV, serta aliran dana	Rekening nominee atau SIM dipindahtangakan
Distribusi konten	Saat unggah, transmisi, atau konten dapat diakses sesuai unsur	Log platform, metadata, dan perangkat	Pengunggah, platform, penerima, serta tempat akibat	Riwayat masuk, perangkat, dan saksi	Unggah ulang, cache, atau manipulasi tangkapan layar

Matriks diisi sejak tahap penyidikan dan diperbarui sampai persidangan. Setiap baris harus menyebut sumber asli, metode akuisisi, zona waktu, nilai integritas, keterbatasan, serta proposisi yang didukung. Kolom "risiko pembelaan " bukan hambatan penegakan hukum, melainkan alat untuk menguji apakah kesimpulan telah menutup alternatif yang rasional.

Penerimaan Laporan atau Pengaduan ketika Tempus, Locus, dan Keberadaan Terduga Pelaku Belum Pasti

Tahap penerimaan laporan atau pengaduan harus dibedakan dari tahap penentuan yurisdiksi, kompetensi relatif, dan pembuktian. Pasal 13 ayat (1) Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana menentukan bahwa penyelidik yang mengetahui atau menerima laporan atau pengaduan mengenai peristiwa yang patut diduga merupakan tindak pidana wajib segera melakukan tindakan penyelidikan yang diperlukan. Pasal 14 KUHAP selanjutnya mengatur bahwa laporan atau pengaduan tertulis ditandatangani oleh pelapor atau pengadu, sedangkan laporan atau pengaduan lisan dicatat dan ditandatangani oleh pelapor atau pengadu serta penyelidik. Struktur norma ini menunjukkan bahwa pintu masuk proses pidana adalah informasi mengenai suatu peristiwa yang patut diduga sebagai tindak pidana, bukan pembuktian lengkap mengenai seluruh unsur, identitas pelaku, atau koordinat *locus delicti*.

Dalam tindak pidana siber, korban sering hanya mengetahui perangkat yang digunakan, akun atau nomor yang menghubunginya, waktu komunikasi, tautan, bukti transfer, atau akibat yang dialami. Korban belum tentu mengetahui lokasi fisik orang yang mengendalikan akun, lokasi alat bekerja, lokasi server, maupun tempat dana akhirnya dikuasai. Ketidakpastian tersebut tidak identik dengan ketiadaan *locus delicti*. Pasal 10 dan Pasal 11 Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana beserta Penjelasannya justru memungkinkan waktu dan tempat ditelusuri melalui perbuatan fisik, bekerjanya alat atau bahan, serta timbulnya akibat. Oleh karena itu, penetapan titik *tempus* dan *locus* yang paling tepat merupakan hasil korelasi fakta dan unsur delik melalui penyelidikan dan penyidikan.

Keberadaan terduga pelaku juga tidak boleh dipertukarkan dengan *locus delicti*. Tempat orang yang diduga sebagai pelaku berada pada saat laporan dibuat dapat berbeda dari tempat perbuatan dilakukan, tempat alat bekerja, atau tempat akibat timbul. Bahkan identitas dan keberadaan pelaku dapat belum diketahui sama sekali. Kondisi tersebut merupakan alasan untuk melakukan penelusuran antara lain melalui data pelanggan, log akses, informasi perangkat, aliran dana, dan kerja sama antarsatuan atau lintas wilayah bukan alasan untuk menutup akses korban kepada mekanisme pelaporan. Penentuan forum baru dilakukan kemudian berdasarkan Pasal 165 sampai dengan Pasal 167 KUHAP mengenai kompetensi relatif pengadilan dan perkara yang dilakukan di luar negeri.

Kewajiban menerima dan menindaklanjuti informasi awal tidak berarti setiap laporan harus otomatis dinyatakan sebagai tindak pidana atau langsung ditingkatkan ke tahap penyidikan. Setelah laporan dicatat, penyelidik tetap wajib menilai apakah peristiwa itu patut diduga sebagai tindak pidana, mengklarifikasi fakta, menentukan pasal yang relevan, memetakan *tempus* dan *locus*, serta menentukan satuan yang berwenang. Apabila hasil pemeriksaan menunjukkan peristiwa bukan tindak pidana, tidak

cukup bukti, atau terdapat dasar hukum lain untuk penghentian, keputusan harus ditempuh melalui prosedur yang sah dan dapat dipertanggungjawabkan; penilaian tersebut tidak boleh digantikan dengan penolakan informal di meja pelayanan. Pembedaan tersebut sejalan dengan Pasal 13 ayat (1), Pasal 14, dan Pasal 21 KUHAP yang memisahkan penerimaan informasi awal dari tindakan penyelidikan, serta dengan Pasal 165 sampai dengan Pasal 167 KUHAP yang mengatur penentuan kompetensi relatif.

Dari sisi etik profesi, Pasal 12 huruf a Peraturan Kepolisian Negara Republik Indonesia Nomor 7 Tahun 2022 tentang Kode Etik Profesi dan Komisi Kode Etik Kepolisian Negara Republik Indonesia melarang pejabat Polri menolak atau mengabaikan permintaan pertolongan, bantuan, atau laporan dan pengaduan masyarakat yang termasuk lingkup tugas, fungsi, dan kewenangannya. Pasal 12 huruf f juga melarang tindakan mempersulit masyarakat yang membutuhkan perlindungan, pengayoman, dan pelayanan. Norma ini harus dibaca bersama kewajiban pelayanan yang cepat, tepat, mudah, transparan, dan akuntabel dalam Pasal 7 huruf c. Jika satuan penerima menilai perkara berkaitan dengan wilayah atau fungsi lain, respons yang tepat ialah menerima dan mendokumentasikan informasi awal, memberi penjelasan, serta melakukan koordinasi atau pelimpahan sesuai prosedur bukan menolak semata-mata karena korban belum dapat menunjukkan lokasi pelaku.

Secara operasional, laporan perkara siber sebaiknya sedikitnya memuat waktu yang diketahui korban beserta zona waktunya, lokasi korban ketika menerima komunikasi atau mengalami akibat, identitas akun/nomor/tautan, kronologi, nilai dan tujuan transfer, perangkat yang digunakan, serta bukti digital yang masih tersedia. Petugas harus segera mengamankan kebutuhan preservasi karena data pelanggan, log, dan rekaman platform dapat berubah atau terhapus. Data awal tersebut berfungsi membangun hipotesis tempus dan locus yang kemudian diuji, bukan membebankan kepada korban kewajiban untuk terlebih dahulu menemukan pelaku.[20]

Implikasi Bagi Penegak Hukum, Advokat, Ahli Dan Hakim

Bagi penyidik, rencana pembuktian harus dimulai dari unsur delik dan volatilitas data. Data memori, koneksi aktif, dan log berumur pendek perlu diprioritaskan dengan tetap memperhatikan kewenangan serta risiko perubahan. Permintaan kepada penyelenggara sistem elektronik harus menyebut akun, rentang waktu, zona waktu, jenis data, format, parameter ekstraksi, dan kebutuhan preservasi. Dokumentasi kondisi awal perangkat mencegah perselisihan mengenai tindakan yang mungkin mengubah data.

Bagi penuntut umum, penelitian berkas harus memeriksa konsistensi antara garis waktu teknis, lokasi, berita acara, laporan ahli, dan rumusan dakwaan. Dakwaan dapat menggunakan beberapa titik tempat apabila fungsi yuridis masing-masing dijelaskan. Penyebutan "bertempat di wilayah hukum pengadilan " tanpa uraian hubungan perbuatan, alat, akibat, atau dasar alternatif kompetensi berisiko menghilangkan fungsi perlindungan Pasal 75 KUHAP.

Bagi advokat, pengujian sebaiknya tidak berhenti pada pernyataan bahwa bukti elektronik "mudah dimanipulasi ". Pengujian yang efektif mengidentifikasi sumber jam, proses konversi, *hash*, metode akuisisi, versi alat, kekosongan log, akses pihak lain, status alamat IP, NAT, VPN, dan kesesuaian antara proposisi penuntut dengan kemampuan artefak. Hak pembelaan memerlukan akses yang memadai terhadap laporan, data dasar yang relevan, dan metode yang digunakan, disertai perlindungan proporsional terhadap data pihak ketiga.

Bagi ahli, laporan harus memisahkan observasi, inferensi, asumsi, dan keterbatasan. Kalimat "akun ini digunakan dari alamat IP X " berbeda secara epistemik dari "terdakwa menggunakan akun ini ". Ahli dapat menjelaskan tingkat konsistensi artefak dengan suatu skenario, tetapi kesimpulan mengenai kesalahan pidana tetap berada pada hakim. Pedoman teknis juga harus diterapkan dengan menyadari ruang lingkupnya; NIST SP 800-86 menyatakan dirinya sebagai pedoman awal pengembangan kapabilitas forensik organisasi, bukan nasihat hukum atau petunjuk tunggal investigasi pidana.[21]

Bagi hakim, pertimbangan putusan perlu menguraikan mengapa suatu sumber waktu dipercaya, bagaimana selisih jam diselesaikan, atas dasar apa suatu lokasi dipilih, bagaimana legalitas perolehan dinilai, dan apa bukti yang menghubungkan akun atau perangkat dengan terdakwa. Penyebutan "bukti elektronik telah sesuai " tanpa analisis sumber, integritas, dan atribusi tidak cukup untuk menunjukkan

[20] Kent, dkk, *Op.Cit*, hlm. 3 dan 4.
[21] *Ibid,* hlm. 1-2.

proses penalaran. Pasal 235 KUHAP memberi kerangka bagi pertimbangan yang eksplisit, sedangkan uji empat tahap membantu membedakan dapat-digunakannya bukti dari bobot bukti.

Preservasi Dan Kerja Sama Lintas Batas

Data perkara siber sering dikuasai penyelenggara yang berada di luar Indonesia. Tantangannya meliputi perbedaan hukum, retensi, format respons, kewenangan, dan waktu pemenuhan. Preservasi cepat dibutuhkan agar data tidak terhapus sebelum bantuan hukum timbal balik atau mekanisme formal selesai. Budapest Convention mengatur preservasi data, produksi, pencarian dan penyitaan data komputer, kerja sama internasional, serta jaringan kontak 24/7, Council of Europe, *Convention on Cybercrime*, ETS No. 185 Pasal 14-21 dan Pasal 23-35. United Nations Convention against *Cybercrime* mengembangkan kerangka global untuk kerja sama dan pertukaran bukti elektronik. Keduanya hanya digunakan sebagai pembanding sesuai status keterikatan Indonesia dan mekanisme hukum nasional.

Kecepatan tidak membenarkan pengabaian hak. Permintaan data harus spesifik, proporsional, dan mempunyai batas tujuan. Data yang diterima perlu disertai informasi mengenai sumber, parameter ekstraksi, zona waktu, format, serta pihak yang melakukan ekstraksi. Jika penyelenggara hanya menyerahkan surat keterangan atau tabel tanpa data dasar yang dapat diverifikasi, keterbatasannya perlu dinyatakan dan diuji.

SIMPULAN

Pertama, KUHP Nasional telah mengubah dasar penentuan *tempus delicti* dan *locus delicti*. Pasal 10 dan Pasal 11 beserta Penjelasannya mengakui perbuatan fisik, bekerjanya alat, dan akibat sebagai titik normatif. Pemilihannya harus mengikuti unsur delik, bukan kemudahan menemukan satu artefak. Pasal 4 huruf c menyediakan yurisdiksi berbasis akibat untuk tindak pidana teknologi informasi, tetapi akibat harus memiliki hubungan kausal dan substansial dengan Indonesia.

Kedua, yurisdiksi negara, kompetensi relatif, dan pembuktian merupakan tiga persoalan berbeda. Pasal 75 KUHAP mensyaratkan uraian waktu dan tempat yang cermat, jelas, dan lengkap. Pasal 165 sampai dengan Pasal 167 memberi dasar forum. Dalam perkara multi-lokus, dakwaan harus menjelaskan fungsi setiap tempat dan tidak cukup menggunakan formula wilayah hukum secara abstrak.

Ketiga, bukti elektronik tidak otomatis membuktikan waktu, tempat, dan pelaku. Pembuktian perlu memisahkan *tempus normatif*, *tempus teknis*, dan *tempus evidensial*, serta memetakan simpul pelaku/perangkat, jaringan/sistem, data/objek, dan korban/akibat. Satu *timestamp*, alamat IP, tangkapan layar, lokasi server, rekening, atau identitas pelanggan harus dikorelasikan dengan sumber independen.

Keempat, uji empat tahap legalitas perolehan, autentikasi-integritas, atribusi, serta relevansi-kausalitas memberi struktur penilaian yang selaras dengan Pasal 235 dan Pasal 242 KUHAP. Model tersebut menjaga efektivitas penegakan hukum sekaligus mencegah atribusi dan perluasan forum secara spekulatif.

Kelima, ketidakpastian awal mengenai *tempus*, *locus*, identitas, atau keberadaan terduga pelaku dalam perkara siber tidak dapat dijadikan alasan untuk menolak laporan atau pengaduan. Informasi tersebut harus dicatat dan ditindaklanjuti melalui penyelidikan sesuai Pasal 13 ayat (1) dan Pasal 14 KUHAP serta Pasal 12 huruf a dan huruf f Peraturan Kepolisian Negara Republik Indonesia Nomor 7 Tahun 2022; kepastian forum dan atribusi pelaku ditentukan setelah korelasi bukti. Penerimaan laporan harus dibedakan dari keputusan akhir mengenai ada atau tidaknya tindak pidana.

DAFTAR PUSTAKA

Buku

International Organization for Standardization. *ISO/IEC 27037:2012 Information Technology Security Techniques Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*. Geneva: ISO, 2012.

Kent, Karen, Suzanne Chevalier, Tim Grance, dan Hung Dang. *Guide to Integrating Forensic Techniques into Incident Response*. NIST Special Publication 800-86. Gaithersburg: National Institute of Standards and Technology, 2006.

Peraturan Perundang-Undangan

Council of Europe. *Convention on Cybercrime*, ETS No. 185, Budapest, 23 November 2001.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana sebagaimana telah diubah dengan Undang-Undang Nomor 1 Tahun 2026 tentang Penyesuaian Pidana.

United Nations. *United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes*. New York, 24 December 2024.

Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor I1 Tahun 2008 tentang Informasi Dan Transaksi Elektronik.

Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana.

Peraturan Kepolisian Negara Nomor 7 Tahun 2022 tentang Kode Etik Profesi dan Komisi Kode Etik Kepolisian Negara Republik Indonesia.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

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

Jurnal

Marsudianto, dkk. "Uncertainty of Locus Delicti and Tempus Delicti as an Obstacle to Law Enforcement against *Cybercrime*". *Greenation International Journal of Law and Social Sciences* 3, no. 2 (2025): 114 -121.

Rahmawati. "Penentuan Tempus dan Locus Delicti dalam Cyber Crime". *Sol Justicia* 3, no. 1 (2020): 94 -104.

Simada, Arthur, Syafruddin Kalo, Mohammad Ekaputra, dan Jelly Leviza. "Penentuan Locus Delictie dalam Tindak Pidana Cyber Crime (Merusak dan Mengganggu Sistem Elektronik dan Komunikasi Milik Orang Lain)". *Locus Journal of Academic Literature Review* 3, no. 4 (2024): 349 -361. https://doi.org/10.56128/ljoalr.v3i4.314.