KEJAHATAN SIBER DAN PERDAGANGAN DATA GELAP (DARK WEB): TANTANGAN HUKUM INDONESIA DALAM KONTEKS BUDAPEST CONVENTION

Oleh
Moeso Novianto[1], Nur Arfiani[2]
[1,2]Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Mulia
E-mail: [1]novianto.moeso@gmail.com, [2]nur.arfiani@universitasmulia.ac.id

Article History:
Received: 04-11-2025
Revised: 23-11-2025
Accepted: 07-12-2025

Keywords:
Budapest Convention; Cybercrime, Dark Web, Data Protection, ITE Law

Abstract: *The rapid growth of digital technology has led to cybercrimes such as illegal data trade on the Dark Web, which are anonymous and transnational, posing serious threats to national data security. This study aims to analyze the roles of the Electronic Information and Transactions Law (ITE Law) and the Personal Data Protection Law (PDP Law) in addressing such crimes, as well as to examine the relevance of the Budapest Convention for Indonesia. Using a normative juridical method with statutory and conceptual approaches, the study finds that weak national legal implementation and the absence of Budapest Convention ratification hinder law enforcement, making stronger international cooperation urgently necessary.*

PENDAHULUAN

Latar Belakang Masalah

Perkembangan pesat teknologi informasi telah membuka dimensi baru dalam kehidupan manusia yang dikenal sebagai *cyberspace*, mengubah fundamental cara berinteraksi, bekerja, dan berinteraksi.[1] Namun, di balik kemajuan ini, muncul pula ancaman serius dalam bentuk kejahatan baru yang kompleks dan lintas batas, yang secara kolektif disebut *cybercrime*.[2] Salah satu bentuk kejahatan siber yang paling meresahkan adalah pencurian data indentitas (*identity theft*). Kejahatan ini dilakukan dengan mencuri informasi pribadi seperti nama, alamat email, nomor telepon, kata sandi dan data lainnya untuk disalahgunakan dalam berbagai aktivitas ilegal seperti penipuan (*fraud*), pemerasan, pembobolan akun, hingga pencucian uang.[3] Salah satu manifestasi paling berbahaya dari ancaman ini adalah penggunaan Dark Web sebagai pasar gelap untuk perdagangan data illegal, yang berpotensi

[1] Akbar K Putra, "Harmonisasi Konvensi Cyber Crime Dalam Hukum Nasional," *Jurnal Ilmu Hukum Jambi* 5, no. 2 (2014): 95–109.

[2] Agung Tri Wicaksono and Ikhsan Fatah Yasin, "Criminal Law Reformulation Through Omnibus Law as a Solution to Sectoral Cyber Protection (Reformulasi Hukum Pidana Melalui Omnibus Law Sebagai Solusi Perlindungan Siber Yang Bersifat Sektoral)," *Al-Jinayah: Jurnal Hukum Pidana Islam* 10, no. 2 (2024): 237–61, https://doi.org/10.15642/aj.2024.10.2.237-261.

[3] Deva Wira Pramudya and Hudi Yusuf, "Pencurian Data Identitas Sebagai Kejahatan Cyber Related Crime: Tinjauan Kriminologis Atas Kasus Pencurian Data Pada Akun Marketplace," *JIIC: Jurnal Intelek Insan Cendikia* 2, no. 7 (2025): 13469–78.

merusak keamanan data pribadi warga negara dan bahkan integritas nasional secara massif.[4]

Secara konseptual, Dark Web merupakan bagian tersembunyi dari internet yang tidak dapat diakses oleh mesin pencari biasa dan memerlukan perangkat lunak khusus untuk menjaga anonimitas pengguna. Anonimitas ini, yang ironisnya juga digunakan untuk tujuan yang sah seperti seperti melindungi jurnalis dari pengawasan pemerintah, menjadi pedang bermata dua yang efektif menyembunyikan identitas pelaku kejahatan. Pasar gelap di dark web beroperasi dengan mekanisme yang canggih, meniru platform e-commerce dengan sistem pembayaran mata uang kripto, ulasan penjual, dan layanan escrow, yang memfasilitasi penjualan data sensitif dalam skala besar dengan efisien. Data yang diperdagangkan mencakup berbagai informasi bernilai ekonomi tinggi, mulai dari kredensioal login, data kartu kredit, hingga malware dan alat peretasan.[5]

Di Indonesia, ancaman ini telah bermanifestasi dalam serangkaian insiden nyata yang menguji ketahanan siber nasional. Kasus-kasus kebocoran data berskala masif, seperti bocornya data Satu Data ASN dan Nomor Pokok Wajib Pajak (NPWP) oleh peretas dengan menggunakan nama alias Bjorka pada tahun 2024, menunjukkan bahwa data sensitif jutaan warga negara diperjualbelikan di forum-forum gelap seperti Breach Forums. Insiden-insiden ini tidak hanya mengakibatkan kerugian finansial dan ancaman terhadap privasi individu, tetapi juga secara serius merusak kepercayaan publik terhadap jaminan keamanan data oleh pemerintah dan lembaga swasta.[6] Meskipun Indonesia telah mengadopsi regulasi untuk menanggulangi ancaman ini, seperti Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU ITE dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), kerangka hukum yang ada masih dianggap belum memadai dan terfragmentasi. UU PDP, misalnya, meskipun telah memberikan landasan hukum yang lebih kuat untuk melindungi hak konstitusional warga negara atas data pribadi, tetap saja masih memerlukan peraturan pelaksana yang rinci untuk bisa diimplementasikan secara optimal. Sementara itu, UU ITE, meskipun mengkriminalisasi akses ilegal dan penyebaran konten terlarang, masih menghadapi kritik karena pasal-pasal yang multitafsir dan berpotensi disalahgunakan untuk membatasi kebebasan berekspresi.[7]

Namun, kesenjangan hukum yang paling krusial terletak pada dimensi transnasional dari kejahatan siber itu sendiri. Pasar gelap di Dark Web beroperasi lintas yurisdiksi, membuat penegakan hukum nasional menjadi sangat sulit ketika pelaku, server, atau bukti elektronik berada di luar negeri. Di sinilah peran kerja sama internasional menjadi sangat vital.[8] Konvensi Budapest (*Convention on Cybercrime*) yang merupakan perjanjian internasional pertama dan paling komprehensif tentang kejahatan siber, menawarkan kerangka kerja sama

[4] EC-Council University, "Exploring the Dark Web and Its Dangers," *EC-Council University*, Agustus 2025, https://www.eccu.edu/blog/the-dark-web-and-its-dangers/.

[5] Flare, "Top 5 Dark Web Marketplaces to Monitor," *Flare*, April 6, 2023, https://flare.io/learn/resources/blog/dark-web-marketplaces/.

[6] Faisal Aldiansyah, "Serangan Siber Terbesar Yang Pernah Terjadi Di Indonesia," *Netmarks*, April 14, 2024, https://www.netmarks.co.id/post/serangan-siber-terbesar-yang-pernah-terjadi-di-indonesia.

[7] Ghufron Rosadi Hidayah, Ha. Djazim Ma'shum, and Muhammad Awaluddin, "Studi Komparatif Perlindungan Data Pribadi Dalam UU ITE 2024 Dan UU PDP 2022," *Jurnal Riset Rumpun Ilmu Sosial, Politik Dan Humaniora* 4, no. 4 (2025): 61–70, https://doi.org/10.55606/jurrish.v4i4.6341.

[8] Yuniar A, "Collaboration Is the Key to Indonesia Cyber Resilience: BSSN," *Gov Insider*, September 8, 2025, https://govinsider.asia/intl-en/article/collaboration-is-the-key-to-indonesia-cyber-resilience-bssn.

hukum timbal balik yang terstruktur dan jaringan kontak 24/7 untuk mempercepat investigasi lintas batas.[9] Meskipun konvensi ini diakui sebagai ”standar emas” di tingkat global, Indonesia hingga saat ini belum meratifikasinya. Keputusan ini didasari oleh berbagai pertimbangan, termasuk kekhawatiran adanya tumpang tindih dengan regulasi domestik yang ada, isu kedaulatan, serta potensi pelanggaran hak asasi manusia. Ketiadaan ratifikasi ini secara nyata membatasi kemampuan ini untuk berkolaborasi secara efektif dengan lebih dari 75 negara pihak dalam menindak kejahatan siber transnasional.[10]

Dengan demikian, terbentangnya jurang antara ancaman kejahatan siber di Dark Web yang terus berevolusi dan kerangka hukum Indonesia yang reaktif dan terfragmentasi, ditambah lagi dengan posisi pasif Indonesia dalam kerangka kerja sama internasional seperti Konvensi Budapest, menciptakan urgensi mendalam untuk sebuah analisis yang komprehensif. Penelitian ini hadir untuk membahas permasalahan tersebut secara kritis, menganalisis tantangan hukum yang ada, dan merumuskan rekomendasi kebijakan yang adaptif dan terintegrasi untuk menciptakan ruang digital yang lebih aman dan terpercaya bagi masyarakat Indonesia.

Oleh karena itu, berdasarkan latar belakang di atas, rumusan masalah yang diangkat pada penelitian ini adalah 1) Bagaimana Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Perlindungan Data Pribadi (UU PDP) mengatur dan menangani kejahatan siber terkait perdagangan data ilegal di dark web?, 2) Apa mekanisme utama Budapest Convention yang krusial untuk penanganan kejahatan siber transnasional? 3) Bagaimana implikasi hukum dari status Indonesia yang belum meratifikasi konvensi tersebut terhadap kemampuan penegak hukum dalam menangani kasus perdagangan data ilegal di Dark Web?

METODE PENELITIAN

Penelitian dengan judul “Kejahatan Siber dan Perdagangan Data Gelap (Dark Web): Tantangan Hukum Indonesia Dalam Konteks Budapest Convention» ini memakai jenis penelitian yuridis normatif (*legal research*).[11] yaitu penelitian yang difokuskan untuk mengkaji penerapan-penerapan kaidah atau norma-norma dalam hukum positif yang berlaku.[12] Terkhusus yang berkaitan dengan kejahatan siber dan perdagangan data gelap. Setelah itu, peneliti selanjutnya melakukan penelusuran untuk mencari bahan-bahan hukum yang relevan. Karena peneliti menggunakan pendekatan perundang-undangan dan pendekatan konseptual, maka peneliti akan mencari peraturan perundang-undangan yang berkaitan dengan isu hukum yang dihadapi, mengumpulkan buku dan jurnal dan kemudian diklasifikasi menurut sumber dan hierarkinya.[13] Adapun jenis data yang digunakan pada penelitian ini adalah data sekunder yang terdapat di dalam kepustakaan, berupa undang-undang, buku, jurnal, dan artikel lainnya.

Teknik analisis pengolahan terhadap bahan hukum yang telah terkumpul dilakukan dengan

[9] The Convention on Cybercrime (2024).

[10] Pradnya Wicaksana, “Pakar Hukum Suber Unair: Indonesia Harus Meratifikasi Budapest Convention,” *Universitas Airlangga*, September 12, 2022, https://unair.ac.id/pakar-hukum-siber-unair-indonesia-harus-meratifikasi-budapest-convention/.

[11] Johny Ibrahim, *Teori Dan Metodologi Penelitian Hukum Normatif* (Sumatera Utara: Bayumedia, 2008).

[12] Peter Mahmud Marzuki, *Penelitian Hukum (Edisi Revisi)* (Jakarta: Kencana, 2014).

[13] Ibrahim, *Teori Dan Metodologi Penelitian Hukum Normatif*.

tahapan: inventarisasi, identifikasi, klasifikasi, dan melakukan sistematisasi. Tahap sistematisasi dilakukan agar tidak terjadi kontradiksi antara bahan hukum yang satu dengan yang lain. Bahan hukum yang telah dikumpulkan kemudian dikelompokkan dan ditelaah dengan menggunakan pendekatan konseptual dan pendekatan perundang-undangan untuk memperoleh gambaran atau jawaban terhadap permasalahan yang menjadi fokus kajian dalam penelitian.[14] Kemudian penulis dalam menganalisis penelitian ini menggunakan metode kualitatif, yaitu dengan cara melakukan interpretasi (penafsiran) terhadap bahan-bahan hukum yang telah diolah.

HASIL DAN PEMBAHASAN

1. Pengaturan dan Penanganan Kejahatan Siber Terkait Perdagangan Data Ilegal di Dark Web menurut Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Perlindungan Data Pribadi (UU PDP)

Secara teknis, Dark Web merupakan sebuah komponen dari internet yang tidak dapat diakses melalui mesin pencari konvensional seperti Google atau Bing. Ia memerlukan perangkat lunak khusus, seperti Tor (*The Onion Router*) atau 12P (*Invisible Internet Project*), untuk diakses.[15] Fenomena ini seringkali disalahartikan sebagai Deep Web, yaitu bagian internet yang tersembunyi di balik otentikasi atau *paywall*. Namun, Dark Web adalah subset yang lebih kecil dari Deep Web yang secara spesifik dirancang untuk menjaga anonimitas pengguna.[16] Anonimitas yang ditawarkan oleh Dark Web memiliki fungsi ganda. Di satu sisi, ia menyediakan sarana bagi individu yang berada di bawah rezim sensor ketat, seperti Jurnalis atau aktivis politik, untuk berkomunikasi secara aman tanpa pengawasan pemerintah.[17] Di sisi lain, sifat anonim ini menjadikannya tempat ideal bagi para pelaku kejahatan siber untuk menyembunyikan identitas dan aktivitas ilegal mereka dari penegak hukum. Sifat tersembunyi dan anonim ini secara fundamental menyulitkan upaya investigasi, pelacakan, dan penuntutan, yang secara signifikan memperbesar tantangan bagi otoritas penegak hukum di seluruh dunia.[18]

Pasar gelap di Dark Web, yang dikenal sebagai darknet markets, beroperasi dengan model bisnis yang mengejutkan serupa dengan platform e-commerce konvensional. Pasar-pasar ini menawarkan berbagai jenis data sensitif yang memiliki nilai ekonomi tinggi.[19] Data yang diperdagangkan mencakup informasi pribadi yang sangat berharga seperti Nomor Pokok Wajib Pajak (NPWP), kredensial (nama pengguna dan kata sandi), informasi kartu kredit, data sensitif lainnya, dan bahkan alat-alat peretasan seperti malware dan ransomware.[20] Untuk menjamin anonimitas, transaksi di pasar gelap ini biasanya dilakukan menggunakan mata uang kripto, seperti Bitcoin atau Monero. Selain itu, banyak dari platform ini mengadopsi

[14] Muhaimin, *Metode Penelitian Hukum* (Mataram: Mataram University Press, 2020).
[15] EC-Council University, "Exploring the Dark Web Dan Its Dangers," *EC-Council University*, Agustus 2025, https://www.eccu.edu/blog/the-dark-web-and-its-dangers/.
[16] Ellie Farrier, "What Is the Dark Web?," *AVG*, March 5, 2025, https://www.avg.com/en/signal/what-is-the-dark-web.
[17] Sindy Ariyaningsih et al., "Korelasi Kejahatan Siber Dengan Percepatan Digitalisasi Di Indonesia," *Justisia: Jurnal Ilmu Hukum* 1, no. 1 (2023): 1–11, https://doi.org/10.56457/jjih.v1i1.38.
[18] EC-Council University, "Exploring the Dark Web Dan Its Dangers."
[19] Wikipedia, "Darkent Markets," *Wikipedia*, Agustus 2025, https://en.wikipedia.org/wiki/Darknet_market.
[20] Aldiansyah, "Serangan Siber Terbesar Yang Pernah Terjadi Di Indonesia."

fitur-fitur yang dirancang untuk membangun kepercayaan di antara para pelaku kejaahtan, termasuk penggunaan sistem escrow untuk melindungi pembeli dan penjual, serta sistem ulasan atau peringkat penjual yang mirip dengan platform seperti Ebay. Model bisnis yang terstruktur ini memungkinkan perdagangan data ilegal berlangsung secara efisien dan dalam skala yang sangat besar. [21]

Ancaman teoretis yang ditimbulkan oleh Dark Web telah menjadi kenyataan empiris di Indonesia. Kasus-kasus kebocoran data besar telah membuktikan bahwa data sensitif warga negara dijual secara masif di forum-forum gelap.[22] Salah satu contoh paling mencolok adalah kebocoran data oleh Satu Data ASN dan data NPWP oleh peretas dengan alias Bjorkan pada tahun 2024. Kasus ini menunjukkan bahwa data sensitif milik 4.7 juta Pegawai Negeri Sipil (PNS) dan 6.6 juta wajib pajak Indonesia telah bocor dan diperdagangkan di forum-forum gelap seperti Breach Forums.[23] Data yang bocor mencakup informasi yang sangat pribadi, termasuk nomor identitas, alamat, dan data jabatan. Dampak dari kasus-kasus ini jauh melampaui kerugian finansial individu. Mereka secara serius merusak citra keamanan siber pemerintah dan mengungkap kerentanan yang signifikan dalam sistem perlindungan data nasional. Kasus-kasus ini menegaskan bahwa kejahatan siber yang terkait dengan Dark Web bukan lagi ancaman abstrak, melainkan tantangan nyata yang membutuhkan respons hukum dan strategis yang kuat.[24]

Meskipun otoritas penegak hukum global telah berhasil menutup beberapa darknet markets terkemuka seperti Silk Road dan Dream Market, fenomena ini tidak secara efektif memberantas perdagangan ilegal. Data menunjukkan bahwa pasar gelap masih menghasilkan miliaran dolar setiap tahunnya dan terus beradaptasi. Salah satu perkembangan signifikan adalah migrasi para pelaku ke platform baru yang lebih tersembunyi dan terdesentralisasi, seperti saluran dan grup telegram.[25] Perkembangan ini menggarisbawahi sebuah hubungan kausal yang penting. Upaya penegakan hukum yang bersifat reaktif, seperti menutup platform ilegal, tidak mengeliminasi kejahatan siber, tetapi justru memaksa para pelaku untuk berinovasi dan menemukan cara baru yang lebih sulit dilacak. Ini menciptakan tantangan berkelanjutan bagi indonesia, di mana penegak hukum tidak hanya terus memburu pasar ilegal, tetapi juga harus berhadapan dengan ekosistem kejahatan yang terus bergerak dan beradaptasi.[26]

---

[21] Flare, "Top 5 Dark Web Marketplaces to Monitor."

[22] Asoke Nath and Romita Mondal, "Dark Web: The Uniluminated Side of the World Wide Web," *International Journal of Computer Science and Engineering* 7, no. 1 (2019): 296–305, https://doi.org/10.26438/ijcse/v7i1.296305.

[23] Muhammad Naufal Bahreisy, "Analisis Halaman-Halaman Dark Web Untuk Mendukung Investigasi Kejehatan" (Skripsi, Universitas Islam Indonesia, 2020), https://dspace.uii.ac.id/bitstream/handle/123456789/28362/16917113%20M%20Naufal%20Bahreisy.pdf?sequence=1.

[24] Aldiansyah, "Serangan Siber Terbesar Yang Pernah Terjadi Di Indonesia."

[25] Muhammad Prakoso Aji, "Sistem Keamanan Siber Dan Kedaulatan Data Di Indonesia Dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) (Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective)," *Jurnal Politica* 13, no. 2 (2022): 222–38, http://dx.doi.org/10.22212/jp.v13i2.3299.

[26] Yedija Otniel Purba and Agus Mauluddin, "Kejahatan Siber Dan Kebijakan Identitas Kependudukan Digital: Sebuah Studi Tentang Potensi Pencurian Data Online," *Jurnal CIC Lembaga Riset Dan Konsultan Sosial* 5, no. 2 (2023): 55–66, https://doi.org/10.51486/jbo.v5i2.113.

Permasalahan ini semakin diperparah oleh dimensi transnasional kejahatan siber. Kasus-kasus kebocoran data di Indonesia sering kali melibatkan peretas yang beroperasi dari luar negeri. Keterbatasan kerangka hukum nasional, seperti UU ITE dan UU PDP, menjadi sangat nyata dalam situasi ini. Meskipun UU PDP memiliki cakupan ekstrateritorial yang memungkinkan penuntutan terhadap entitas asing yang memproses data warga negara Indonesia, implementasinya di lapangan terbentur pada kendala yurisdiksi dan kesulitan untuk memperoleh bukti elektronik yang berada di luar negeri. Tanpa adanya kerangka kerja sama internasional yang efektif, Indonesia kesulitan untuk melakukan investigasi lintas batas, memperoleh data dari Penyedia Layanan Internet (ISP) asing, atau mengekstradisi pelaku yang bersembunyi di negara lain. Keterbatasan ini menjelaskan mengapa penuntasan kasus-kasus siber transnasional sering kali menjadi proses yang lambat dan penuh hambatan.[27]

Pembahasan mengenai perlindungan data pribadi tidak bisa dilepaskan dari konsep privasi. Hukum telah mengenal konsep privasi dalam kaitannya dengan gangguan secara fisik berupa *trespass* (memasuki pekarangan orang lain tanpa ijin) yang dikenal dalam hukum pidana. Dalam perkembangannya, hukum memberikan pula perlindungan terhadap emosional dan intelektual manusia. Samuel D. Waren dan Louis D. Brandeis mengemukakan bahwa privasi merupakan pengembangan perlindungan hukum terhadap emosi manusia.[28] Lebih lanjut menurut Holvast, privasi identik dengan kebebasan (*freedom*), kontrol dan self-determination (menentukan nasib sendiri). Namun demikian, sampai dengan saat ini belum ada kesatuan pendapat mengenai makna definitif dari privasi. Solove mengemukakan setidaknya ada 6 (enam) rumusan privasi, yakni: 1) *the right to be let alone* (hak untuk menyendiri), 2) *limited access to the self* (hak untuk menutup diri), 3) *secrecy* (hak untuk menutup hal-hal tertentu dari orang lain), 4) *control over the personal information* (hak untuk mengendalikan informasi pribadi), 5) *personhood* (hak untuk melindungi kepribadian), 6) *intimacy* (hak untuk berhubungan dengan orang lain).[29]

Menurut General Assembly United Nation dalam The Right of Privacy in the Digital Age mengakui bahwa perkembangan teknologi komunikasi membuat orang dapat terkoneksi ke seluruh dunia, namun di sisi lain perkembangan tersebut juga meningkatkan kemampuan pemerintah, perusahaan-perusahaan dan individu-individu untuk melakukan pengawasan (surveillance), penyadapan dan pengumpulan data yang berpotensi mengancam hak asasi manusia. Oleh karenanya diperlukan perlindungan privasi baik terhadap aktivitas secara online maupun offline.[30] Walaupun perlindungan data pribadi pada setiap negara dapat berbeda, pada umumnya pengaturan merujuk pada prinsip-prinsip perlindungan data yang serupa. Umumnya rezim perlindungan data terinspirasi dari OECD tahun 1980 tentang Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data yang menerapkan prinsip-prinsip pertama privasi yang diakui secara internasional. Berikut adalah

[27] Muhammad Yudistira and Ramadani Ramadani, "Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang Nomor 27 Tahun 2022 Oleh Kominfo," *Unes Law Review* 5, no. 4 (2023): 3917–29, https://doi.org/10.31933/unesrev.v5i4.698.

[28] Brandeis and Warren, "The Right to Privacy," *Harvard Law Review* IV, no. 5 (1890): 193–220.

[29] Dewi Sulistianingsih et al., "Tata Kelola Perlindungan Data Pribadi Di Era Metaverse (Telaah Yuridis Undang-Undang Perlindungan Data Pribadi)," *Masalah-Masalah Hukum* 52, no. 1 (2023): 97–106, https://doi.org/10.14710/mmh.52.1.2023.97-106.

[30] Sinta Dewi Rosadi, "Protecting Privacy on Personal Data in Digital Economic Era: Legal Framework in Indonesia," *Brawijaya Law Journal* 5, no. 1 (2018): 143–57, https://doi.org/10.21776/ub.blj.2018.005.01.09.

prinsip perlindungan data pribadi menurut OECD:[31]

Tabel 1

Prinsip	Penjelasan
Prinsip Pembatasan Pengumpulan (*Collection Limitation Principle*)	Harus ada batasan untuk pengumpulan data pribadi dan data semacam itu harus diperoleh dengan cara yang sah dan adil dan dengan sepengetahuan atau persetujuan dari subjek data
Prinsip Kualitas Data (*Data Quality Principle*)	Data pribadi harus relevan dengan tujuan penggunaannya, dan sejauh yang diperlukan untuk tujuan tersebut, harus akurat, lengkap dan terus diperbarui
Prinsip Spesifikasi Tujuan (*Use Limitation Principle*)	Tujuan pengumpulan data pribadi harus ditentukan selambat-lambatnya pada saat pengumpulan data dan penggunaan selanjutnya terbatas pada pemenuhan tujuan tersebut atau tujuan lainnya yang tidak sesuai dan ditentukan untuk setiap perubahan tujuan
Prinsip Perlindungan Keamanan (*Security Safeguards Principle*)	Data pribadi tidak boleh diungkapkan, tersedia atau digunakan untuk tujuan selain yang ditentukan kecuali: a) dengan persetujuan subjek data; atau b) oleh otoritas hukum
Prinsip Keterbukaan (*Openness Principle*)	Adanya kebijakan keterbukaan tentang perkembangan, praktik, dan policy berkenaan dengan data pribadi. Sarana tersebut harus tersedia untuk menetapkan keberadaan dan sifat data pribadi, dan tujuan utama penggunaannya, serta identitas dan lokasi pengontrol data (*data controller*)
Prinsip Partisipasi Individu (*Individual Participation Principle*)	Individu berhak: a. Untuk memperoleh dari pengontrol data (*data controller*) atau konfirmasi, apakah pengontrol data memiliki data terkait atau tidak; b. Untuk berkomunikasi dengan mereka, data yang berkaitan dengan mereka: i) dalam waktu yang wajar, ii) dengan biaya, jika ada, iii) alasan yang cukup, dan iv) diberikan dalam bentuk yang dapat dipahami; c. Diberikan alasan jika permintaan dibuat berdasarkan huruf a) dan b) ditolak, dan dapat diargumentasikan penolakan tersebut; d. Untuk melawan data terkait mereka, dan seandainya perlawanan tersebut besar, untuk menghapus data, memperbaiki, melengkapi atau mengubah.
Prinsip Akuntabilitas (*Accountability Principle*)	Pengontrol data (*data controller*) harus bertanggung jawab untuk mematuhi langkah-langkah yang berdampak pada prinsip-prinsip yang disebutkan di atas

Meskipun hak atas privasi dan data pribadi ini sudah dikategorikan sebagai sebagai hak

[31] OECD, "The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines," *OECD Publishing* 1, no. 176 (2011): 1–50, https://doi.org/10.1787/5kgf09z90c31-en.

dasar dan sudah dinyatakan untuk menjadi fokus utama sebagai bentuk implementasi HAM baik secara internasional oleh komite-komite di U*nited Nations High Commissioner for Human Rights* (UHCHR) dalam berbagai laporan dan resolusi *General Assembly* untuk memberikan urgensi pada negara – negara internasional. Salah satu negara yang dituju pada laporan dan resolusi itu adalah kepada Indonesia melalui pemerintah sebagai pemangku kewajiban untuk melakukan regulasi dan peraturan perundang – undangan terkait hak atas privasi dan perlindungan data pribadi. Kendati demikian kasus – kasus terkait pelanggaran hak atas privasi dan perlindungan data pribadi seperti kebocoran, jual beli, hingga penyalahgunaan data masih terjadi. [32]

Ketentuan mengenai perlindungan hak atas privasi dan perlindungan data pribadi sudah diakui oleh berbagai aspek ketentuan peraturan perundang – undangan di Indonesia baik dari konstitusi yaitu UUD 1945, berbagai peraturan perundang – undangan turunannya seperti UU HAM, UU PDP, UU ITE dan undang – undang ratifikasi instrumen HAM internasional. Perlindungan atas hak privasi dan data pribadi tidak hanya selesai dengan pengaturan terkait definisinya, ruang lingkup dan kewajiban negara saja, perlu juga adanya ketentuan penegakan hukum jika terjadi pelanggaran atas hak tersebut. Penegakan hukum dilakukan dengan mengatur sanksi dan memastikan penegakannya. UU ITE mengatur mengenai pasal – pasal larangan untuk melakukan tindakan yang dapat melanggar hak atas privasi dan perlindungan data pribadi. Pasal 30 mengatur mengenai larangan untuk mengakses komputer dan/atau sistem elektronik secara melawan hukum atau dikenal dengan istilah akses ilegal, Adapun ketentuan pidananya adalah penjara maksimal 6 tahun dengan adanya ancaman penjara lebih lama yaitu 7 tahun bagi yang melakukan akses ilegal dengan tujuan memperoleh informasi atau dokumen elektronik dan ancaman penjara hingga 8 tahun bagi yang melakukan akses ilegal dengan cara – cara melawan hukum. Lalu Pasal 31 mengatur mengenai intervensi dan/atau penyadapan atas informasi dan/atau dokumen elektronik atau untuk menghapusnya diancam dengan pidana penjara paling lama hingga 10 tahun. Pasal 32 ayat (1) mengatur larangan untuk merubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan sebuah informasi dan/atau dokumen elektronik secara melawan hukum. Adapun ancaman pidana bagi orang yang melakukan hal tersebut adalah pidana penjara paling lama 8 tahun. Pasal 32 ayat (2) mengatur mengenai larangan untuk memindahkan atau mentransfer kepada pihak yang tidak berhak dan diancam dengan pidana penjara paling lama hingga 9 tahun. Pasal 32 ayat (3) mengatur larangan membuka informasi dan/atau dokumen elektronik bersifat rahasia, diancam dengan pidana penjara maksimal 10 tahun.[33]

Pelanggaran sebagaimana diatur dalam UU PDP dapat diberikan juga sanksi administrasi sebagaimana diatur dalam Pasal 57 ayat (1). Sanksi administratif diberikan kepada setiap pelanggaran yang dilakukan sebagaimana dikualifikasikan dan diatur berbagai ketentuan seperti pada Pasal 20 ayat (l), Pasal 21, Pasal 24 UU PDP dan lainnya yang mana dapat dijatuhi sanksi administratif oleh pihak/instansi yang berwenang. Bentuk-bentuk dari sanksi administratif diatur dalam pasal 57 ayat (2) UU PDP yang dapat berbentuk peringatan tertulis,

[32] Djafar Wahyudi, *Privasi 101: Panduan Memahami Privasi, Perlindungan Data Dan Surveilans* (Jakarta: Elsam, 2015).

[33] Hikmal Yusuf Argiansyah and M. Rizki Yudha Prawira, "Analisis Hukum Hak Atas Privasi Dan Perlindungan Data Pribadi Berdasarkan Perspektif Hak Asasi Manusia," *Jurnal Hukum Pelita* 5, no. 1 (2024): 61–75.

penghentian sementara kegiatan pemrosesan data pribadi, penghapusan atau pemusnahan data pribadi, dan/atau denda dengan nominal tertentu. Denda yang dimaksud adalah denda secara administratif, yakni paling besar dua persen dari pendapatan/penerimaan tahunan terhadap variabel pelanggaran.[34]

UU Perlindungan Data Pribadi memberikan serangkaian hak yang eksplisit dan tidak ambigu kepada subjek data, yang mencerminkan pendekatan modern yang berpusat pada individu. Hak-hak ini mencakup: 1) hak untuk mengakses dan memperbaiki data, setiap individu memiliki hak untuk meminta akses dan salinan data pribadinya, serta hak untuk melengkapi atau memperbaiki kesalahan dalam data tersebut, 2) hak untuk menghapus dan memusnahkan data, subjek data berhak untuk mengakhiri pemrosesan, menghapus, dan/atau memusnahkan data pribadi yang tidak relevan atau yang tidak lagi diperlukan, sesuai dengan ketentuan yang berlaku, 3) hak untuk menarik persetujuan, subjek data berhak untuk menarik kembali persetujuan pemrosesan data yang telah diberikan kepada pengendali data pribadi.

Meskipun ketentuan hukumnya kuat, efektivitas UU Perlindungan Data Pribadi sangat bergantung pada implementasinya, yang hingga saat ini masih terhambat oleh beberapa faktor seperti: 1) ketiadaan otoritas independen, salah satu tantangan terbesar adalah belum terbentuknya otoritas perlindungan data pribadi yang independen dan berwenang penuh untuk mengawasi pelaksanaan undang-undang, menjatuhkan sanksi, dan menerima pengaduan dari masyarakat, 2) kekosongan aturan turunan, hingga kini, peraturan pelaksana yang rinci sebagai turunan dari UU PDP belum sepenuhnya diterbitkan. Keterlambatan ini menciptakan kekosongan normatif dan membuat perlindungan data pribadi belum berjalan secara optimal, 3) fragmentasi regulasi, naskah-naskah hukum yang ada menunjukkan adanya tumpang tindih kewenangan antara UU PDP dan UU ITE. UU ITE yang juga mengatur tentang kejahatan siber dan perlindungan data, memiliki beberapa pasal yang multitafsir dan berpotensi menimbulkan dualisme hukum, yang mempersulit penegakan hukum yang kohesif.

Selain itu, UU ITE dirancang sebagai kerangka hukum yang komprehensif untuk mengatur berbagai aspek transaksi dan informasi elektronik, sekaligus mengkriminalisasi tindakan-tindakan ilegal di dunia maya.[35] Untuk menindak kejahatan siber, UU ITE menetapkan sejumlah pasal yang menjadi landasan hukum utama. Pasal yang paling relevan untuk kejahatan data adalah Pasal 30 ayat (1), (2) dan (3) yang mengkriminalisasi "akses ilegal" (*illegal access*). Pasal ini secara khusus melarang seseorang untuk mengakses sistem elektronik milik orang lain tanpa hak atau dengan cara melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.[36]

Beberapa poin penting terkait pasal ini adalah: a) delik formil, Pasal 30 ayat (3) dikategorikan sebagai delik formil. Artinya, tindak pidana dianggap selesai saat pelaku

[34] Diah Puspitasari, Sintia Kartini Haniandaresta, and Dalila Afif, "Urgensi Undang-Undang Perlindungan Data Pribadi Dalam Mengatasi Masalah Keamanan Data Penduduk," *Journal of Administrative and Social Science* 4, no. 2 (2023): 195–205, https://doi.org/10.55606/jass.v4i2.403.

[35] Rini Retno Winarni, "Efektivitas Penerapan Undang-Undang ITE Dalam Tindak Pidana Cyber Crime," *Hukum Dan Dinamika Masyarakat* 14, no. 1 (2016): 16–27.

[36] Addin Aditya, "Upaya Preventif Cegah Kejahatan Siber Dan Penyalahgunaan Transaksi Elektronik Melalui Sosialisasi UU ITE," *Jurnal Abdimas Nusa Mandiri* 6, no. 1 (2024): 22–27, https://doi.org/10.33480/abdimas.v6i1.5370.

melakukan perbuatan yang dilarang, yaitu mengakses sistem elektronik secara ilegal, tanpa harus menunggu adanya akibat seperti kerugian finansial atau keberhasilan pencurian data. Hal ini mempermudah proses penyidikan karena fokusnya pada tindakan akses ilegal itu sendiri, b) unsur tindak pidana, unsur menjebol sistem pengamanan dapat ditafsirkan secara luas, mencakup tindakan teknis seperti brute force attack untuk menebak kata sandi yang dienkripsi, hingga tindakan manipulatif seperti menipu korban agar terhubung ke jaringan palsu dalam kasus evil twin.[37] Selain itu, Pasal 27B ayat (2) juga relevan karena melarang distribusi informasi dengan ancaman pencemaran atau pembukaan rahasia, yang seringkali menjadi modus dalam perdagangan data ilegal di Dark Web.

Meskipun memiliki landasan hukum yang jelas, implementasi UU ITE dalam menanggulangi kejahatan siber yang terhubung dengan Dark Web masih menghadapi berbagai tantangan signifikan di mana tantangan tersebut berupa anonimitas pelaku, anonimitas yang melekat pada dark web membuat identifikasi dan pelacakan pelaku menjadi sangat sulit. Peretas sering menggunakan teknologi enkripsi, VPN dan server asing untuk menyamarkan jejak mereka, yang secara fundamental menghambat upaya investigasi dan keterbatasan yurisdiksi, UU ITE beroperasi dalam batasan yurisdiksi teritorial, yang menjadi tidak relevan ketika pelaku dan bukti elektronik berada di luar negeri. Ketiadaan kerangka kerjasama internasional yang kuat, seperti Konvensi Budapest, membuat Indonesia kesulitan memperoleh data dari Penyedia Layanan Internet (ISP) asing atau mengekstradisi pelaku.

Analisis terhadap UU ITE menunjukkan bahwa fokus undang-undang ini cenderung pada apsek penindakan dan penghukuman pelaku, dengan sanksi pidana yang berat seperti denda dan/atau penjara. Namun, perlindungan terhadap hak-hak korban, seperti ganti rugi materiil dan imateriil, masih bersifat umum dan belum implementatif. Mekanisme perlindungan yang ada seringkali tidak memadai. Korban kejahatan siber, seperti yang terjadi dalam kasus-kasus penipuan daring, seringkali tidak mengetahui cara mengajukan ganti rugi dan harus melalui proses yang rumit untuk mendapatkan kembali aset mereka. Selain itu, banyak korban juga mengalami viktimisasi sekunder, yaitu penderitaan tambahan yang timbul dari respons negatif sistem hukum, media, dan masyarakat, seperti sikap menyalahkan korban atau kurangnya pendampingan hukum dan psikologis.

2. Mekanisme Utama Budapest Convention dalam Penanganan Kejahatan Siber Transnasional

Penanganan kejahatan siber, terutama yang bersifat transnasional, menghadapi serangkaian tantangan yang unik dan kompleks yang tidak ditemukan dalam kasus kejahatan konvensional. Karakteristik bawaan dari dunia maya, seperti anonimitas dan volatilitas, secara fundamental melemahkan efektivitas penegakan hukum yang hanya mengandalkan kerangka hukum domestik.[38] Salah satu tantangan terbesar adalah anonimitas pelaku. Para peretas dan pelaku kejahatan siber sering kali memanfaatkan teknologi enkripsi, *Virtual Private Network* (VPN) dan jaringan tersembunyi seperti TOR (*The Onion Router*) untuk menyamarkan identitas dan lokasi mereka. Penggunaan teknologi ini membuat identifikasi dan pelacakan pelaku menjadi sangat sulit, bahkan hampir mustahil, karena jejak digital

[37] Yusuf Daeng et al., "Analisis Penerapan Sistem Keamanan Siber Terhadap Kejahatan Siber Di Indonesia," *Innovative: Journal of Social Network Science Research* 3, no. 6 (2023): 1135–45.

[38] Nurul Aini and Fauziah Lubis, "Tantangan Pembuktian Dalam Kasus Kejahatan Siber," *Judge: Jurnal Hukum* 5, no. 2 (2024): 55–63, https://doi.org/doi.org/10.54209/judge.v5i02.566.

ISSN 2798-3471 (Cetak)
ISSN 2798-3641 (Online)

mereka tersembunti dan tidak dapat dilacak kembali ke sumber aslinya dengan mudah.[39]

Tantangan kedua adalah volatilitas bukti digital. Bukti elektronik, seperti log server, data lalu lintas atau data yang disimpan dalam sistem komputer, bersifat sangat rapuh (ephemeral). Bukti-bukti ini dapat diubah, dihapus, atau dimusnahkan secara permanen hanya dalam hitungan detik. Sifat ini sangat kontrak dengan bukti fisik konvensional, yang memungkinkan penyelidik memiliki waktu yang lebih lama untuk mengumpulkan dan menganalisisnya. Dalam konteks lintas batas, di mana proses permintaan bantuan hukum antarnegara seringkali memakan waktu berbulan-bulan, bukti digital yang dibutuhkan dapat hilang jauh sebelum permintaan tersebut ditindaklanjuti.[40] Yang ketiga dan mungkin yang paling signifikan, adalah permasalahan yurisdiksi lintas batas. Pelaku dapat melakukan kejahatan dari satu negara, sementara server yang menyimpan bukti dan korban berada di negara lain yang berbeda. Situasi ini menimbulkan pertanyaan fundamendal mengenai yurisdiksi dan hukum mana yang berlaku. Tanpa kerangka kerja sama internasional yang kuat, otoritas penegak hukum suatu negara tidak memiliki kewenangan untuk melakukan investigasi atau menyita bukti di luat batas teritorialnya, yang secara efektif menciptakan "zona aman" atau *safe havens* bagi para pelaku kejahatan.

Meskipun Indonesia telah berupaya mengadopsi regulasi untuk menanggulangi ancaman siber, seperti Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU ITE dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, kerangka hukum yang ada masih dianggap belum memadai dan terfragmentasi. UU PDP, misalnya, meskipun memiliki cakupan ekstrateritorial yang memungkinkan penuntutan terhadap entitas asing yang memproses data warga negara Indonesia, implementasinya di lapangan terbentur pada kendala yurisdiksi dan kesulitan untuk memperoleh bukti elektronik yang berada di luar negeri. Tanpa adanya kerangka kerja sama internasional yang efektif, penuntasan kasus-kasus siber transnasional sering kali menjadi proses yang lambat dan penuh hambatan. Tantangan teoretis yang dihadapi telah menjadi kenyataan empiris di Indonesia.

Konvensi Budapest mengatasi tantangan penegakan hukum siber yang unik ini melalui tiga pilar mekanisme utama yang saling terintegrasi, yaitu: harmonisasi hukum, kewenangan prosedural, dan kerangka kerja sama internasional. Pilar pertama, harmonisasi hukum substantif, konvensi budapest mewajibkan negara-negara pihak untuk mengkriminalisasi serangkaian perilaku siber melalui undang-undang domestik mereka, ketentuan tersebut mencakup: 1) pelanggaran terhadap kerahasiaan, integritas, dan ketersediaan data dan sistem komputer, seperti akses ilegal (*illegal access*), intersepsi ilegal (*illegal interception*), gangguan data (*data interface*), gangguan sistem (*system interface*), 2) pelanggaran terkait komputer, seperti pemalsuan terkait komputer (*computer related forgery*) dan penipuan terkait komputer (*computer related fraud*), 3) pelanggaran terkait konten, seperti ponografi anak, 4) pelanggaran terkait hak cipta dan hak terkait. Peran krusial dari mekanisme ini

[39] Aldi Ferdiansyah, Berdi Adityas Wiryawan Wahyono, and Almansyah Harahap, "Pengaruh Penerapan Undang-Undang ITE Terhadap Tingkat Kejahatan Siber Di Indonesia," *Jurnal Kajian Hukum Dan Kebijakan Publik* 2, no. 2 (2025): 924–30, https://doi.org/10.62379/bza49768.

[40] Dede Mercy Rolando, Hanna Hilyati Aulia, and Mutia Tanseba Andini, "Transformasi Digital Dan Ancaman Cybercrime," *Siyasah: Jurnal Hukum Tata Negara* 3, no. 1 (2023): 68–84, https://doi.org/10.32332/siyasah.v3i1.7441.

adalah menciptakan landasan hukum yang seragam di antara negara-negara pihak. Dengan memiliki definisi kejahatan yang serupa, penegak hukum dapat berkolaborasi lebih mudah tanpa terhambat oleh perbedaan hukum atau persyaratan dual criminality yang ketat dalam mekanisme bantuan hukum timbal balik konvensional. Harmonisasi ini memungkinkan investigasi dan penuntutan lintas batas berjalan lebih mulus dan efisien.[41]

Adapun pilar kedua adalah kewenangan prosedural yang efektif dan dipercepat, pilar ini mensyaratkan negara pihak untuk memiliki serangkaian kewenangan investigas yang diperlukan untuk menghadapi sifat unik dari bukti digital.[42] Kewenangan ini secara langsung menargetkan masalah volatilitas bukti dan anonimitas pelaku. Mekanisme yang paling krusial adalah preservasi data tersimpan yang di dalam wilayahnya. Permintaan ini dapat dilakukan tanpa memerlukan persyaratan dual criminality yang ketat. Tujuan utamanya adalah untuk mengamankan bukti digital yang rapuh sebelum bukti tersebut hilang. Setelah data berhasil dipreservasi, konvensi memberikan waktu minimal 60 hari bagi negara penerima untuk menyiapkan dan mengirimkan permohonan bantuan hukum timbal balik (*Mutual Legal Asistance*) formal untuk memperoleh akses penuh atau penyitaan data tersebut.[43] Kewenangan ini berfungsi sebagai tindakan pencegahan yang sangat vital dalam rantai investigasi siber, di mana waktu adalah faktor penentu keberhasilan. Selain itu, konvensi juga mengatur kewenangan prosedural lain seperti akses dan penyitaan data tersimpan (*search and seizure*), serta pengumpulan data lalu lintas secara real time. Kewenangan-kewenangan ini memberikan otoritas penegak hukum instrumen yang kuat untuk mengikuti jejak digital pelaku dan mengumpulkan bukti yang sah di pengadilan.

Pilar ketiga adalah kerangka kerja sama internasional yang cepat dan responsif, pilar ini merupakan jantung dari konvensi dalam konteks penanganan kejahatan siber transnasional. Konvensi ini tidak hanya menyederhanakan prosedur MLA konvensional, tetapi juga mendirikan sebuah kerangka kerja sama yang lebih efisien. Inti dari mekanisme adalah setiap negara pihak wajib menunjuk sebuah poin kontak yang tersedia 24 jam sehari, 7 har iseminggu. Untuk memberikan bantuan real time dan memfasilitasi investigasi siber. Jaringan ini merupakan jaringan khusus yang berfokus pada kejahatan siber dan bukti elektronik, dan terdiri dari tim-tim multidisiplin yang terpercaya. Jaringan 24/7 memungkinkan penegak hukum dari berbagai negara untuk berkomunikasi dan berkoordinasi secara instan, memotong birokrasi yang melekat pada saluran diplomatik tradisional. Kecepatan ini sangat penting untuk menangkap bukti yang cepat hilang dan melacak pelaku yang bergerak cepat melintasi yurisdiksi. Data yang dipreservasi melalui jaringan ini nantinya dapat digunakan sebagai bukti dalam kasus pidana melalui prosedur MLA yang lebih lanjut.[44]

Peran krusial Konvensi Budapest tidak hanya terletak pada fitur-fitur individualnya, tetapi pada cara mekanisme-mekanisme tersebut bekerja sama untuk menciptakan sebuah *rantai nilai penegakan hukum siber terintegrasi*. Konvensi ini secara kolektif mengatasi setiap hambatan yang ada dalam penanganan kasus siber transnasional. Pertama, hambatan yurisdiksi yang muncul akibat pelaku dan bukti yang tersebar di berbagai negara diatasi oleh

[41] Bisdan Sigalingging, "Bantuan Hukum Timbal Balik Dalam Perampasan Aset Korupsi Antar Lintas Batas Negara," *Luris Studia: Jurnal Kajian Hukum* 2, no. 3 (2021): 387–98.

[42] Rolando, Aulia, and Andini, "Transformasi Digital Dan Ancaman Cybercrime."

[43] Aini and Lubis, "Tantangan Pembuktian Dalam Kasus Kejahatan Siber."

[44] Meyse Stevely Sisilia Wuwungan, "Perlindungan Hukum Terhadap Pemilik Data Pribadi Pengguna Teknologi Informasi Akibat Tindak Pidana Peretasan," *Lex Privatum* 13, no. 4 (2024): 1–12.

ISSN 2798-3471 (Cetak)
ISSN 2798-3641 (Online)

harmonisasi hukum substantif dan Jaringan 24/7. Harmonisasi menciptakan dasar hukum yang sama, memastikan suatu tindakan yang dianggap ilegal di satu negara juga ilegal di negara lain yang menjadi anggota Konvensi. Sementara itu, Jaringan 24/7 memfasilitasi komunikasi instan antara aparat penegak hukum, meniadakan batas-batas geografis yang menghambat investigasi. Kedua, hambatan bukti digital yang volatil diatasi secara efektif oleh kewenangan prosedural yang dipercepat, khususnya mekanisme *expedited preservation*. Mekanisme ini memastikan bahwa bukti yang paling rapuh dapat diamankan segera, memberikan waktu yang cukup bagi negara yang bersangkutan untuk melakukan prosedur hukum yang lebih formal. Tanpa mekanisme ini, proses MLA konvensional yang lambat akan membuat bukti tersebut hilang sebelum sempat digunakan dalam penuntutan. Ketiga, hambatan birokrasi dalam proses MLA konvensional digantikan oleh efisiensi dan responsivitas Jaringan 24/7. Mekanisme ini mengganti korespondensi diplomatik yang bertele-tele dengan jalur komunikasi langsung yang efisien, memungkinkan penegak hukum untuk berkolaborasi secara real-time. Kecepatan ini sangat penting untuk menangkap pelaku yang bergerak cepat melintasi yurisdiksi.[45]

Dengan demikian, dapat disimpulkan bahwa setiap pilar Konvensi Budapest secara langsung menargetkan dan menetralisir salah satu karakteristik yang paling sulit dari kejahatan siber, yaitu kecepatan, anonimitas, dan sifat lintas batas. Konvensi ini menyediakan sebuah sistem yang sinergis, di mana setiap komponennya saling melengkapi untuk mencapai tujuan bersama: penegakan hukum yang efektif di dunia siber yang tidak terikat oleh batas fisik.[46]

Meskipun Konvensi Budapest diakui sebagai kerangka kerja yang komprehensif, Indonesia hingga saat ini belum meratifikasinya. Keputusan ini didasari oleh berbagai pertimbangan, termasuk kekhawatiran adanya tumpang tindih dengan regulasi domestik yang ada, isu kedaulatan, serta potensi pelanggaran hak asasi manusia. Kekhawatiran kedaulatan, misalnya, berfokus pada potensi pengikisan kedaulatan data dan hukum nasional jika otoritas asing diberikan akses ke data warga negara Indonesia. Namun, posisi non-ratifikasi ini menciptakan sebuah dilema keamanan dan kedaulatan.[47] Secara teori, Indonesia berupaya melindungi kedaulatan dengan tidak meratifikasi perjanjian internasional yang berpotensi membatasinya. Namun, secara praktik, tindakan ini justru membuat negara menjadi lebih rentan terhadap ancaman siber yang tidak dapat dijangkau oleh hukum domestik. Ketiadaan ratifikasi secara nyata membatasi kemampuan Indonesia untuk berkolaborasi secara efektif dengan lebih dari 75 negara pihak dalam menindak kejahatan siber transnasional. Aparat penegak hukum Indonesia kesulitan untuk melakukan investigasi lintas batas, memperoleh bukti dari penyedia layanan internet (ISP) asing, atau mengekstradisi pelaku yang bersembunyi di negara lain.

[45] Miko Aditya Suharto and Maria Novita Apriyani, "Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional," *Risalah Hukum* 17, no. 2 (2021): 98–107, https://doi.org/10.30872/risalah.v17i2.705.

[46] Wahyu Rifqi Febrian, Raden Mohammad Rangga Faturrahman, and Hannah Syahida Rahmadina, "The Role of International Law in Handling Cyber Crime Cases," *Jurnal Sahid Da'watii* 3, no. 2 (2024): 1–7, https://doi.org/10.56406/jurnalsahiddawatii.v3i02.481.

[47] Ermanto Fahamsyah et al., "Penerapan Prinsip Aut Dedere Aut Judicare Terhadap Pelaku Cybercrime Lintas Negara Melalui Ratifikasi Budapest Convention," *De Jure: Jurnal Hukum Dan Syariah* 14, no. 1 (2022): 140–59, http://dx.doi.org/10.18860/j-fsh.v14i1.15731.

Kegagalan ini sangat terlihat dalam kasus-kasus kebocoran data skala masif. Data sensitif jutaan warga negara Indonesia, yang seharusnya dilindungi oleh kedaulatan nasional, kini diperdagangkan di forum-forum gelap di luar negeri, di luar jangkauan yurisdiksi Indonesia. Keputusan untuk tidak meratifikasi, yang dimaksudkan untuk menjaga kontrol nasional, justru menghasilkan hilangnya kontrol atas keamanan data di era global. Posisi ini secara ironis menciptakan "zona aman" bagi para pelaku kejahatan, yang memanfaatkan celah birokrasi dan hukum untuk menghindari penuntutan.

3. Implikasi Hukum dari Status Indonesia yang Belum Meratifikasi Konvensi Tersebut Terhadap Kemampuan Penegak Hukum dalam Menangani Kasus Perdagangan Data Ilegal di Dark Web?

Dalam teori hukum internasional, hubungan antara hukum internasional dan hukum nasional telah lama menjadi subjek perdebatan yang intens, melahirkan dua doktrin utama: monisme dan dualisme. Paham monisme didasarkan pada pemikiran kesatuan dari seluruh hukum yang mengatur kehidupan manusia. Menurut pandangan ini, hukum internasional adalah konsekuensi langsung dari norma dasar seluruh hukum, sehingga mengikat setiap individu secara kolektif tanpa perlu tindakan legislasi tambahan. Dalam aliran monisme, terdapat dua sub-aliran: monisme dengan primat hukum nasional, yang menganggap hukum nasional lebih utama, dan monisme dengan primat hukum internasional, yang menempatkan hukum internasional pada kedudukan hierarki yang lebih tinggi.[48]

Berbeda dengan monisme, paham dualisme menganggap hukum internasional dan hukum nasional sebagai dua sistem hukum yang terpisah satu sama lain. Menurut para pendukung teori ini, seperti Triepel dan Anzilotti, kedua sistem hukum tersebut memiliki subjek, sumber, dan hakikat yang berbeda. Oleh karena itu, hukum internasional tidak dapat secara otomatis berlaku di dalam lingkungan hukum nasional. Untuk dapat diberlakukan, ketentuan hukum internasional harus melalui proses yang disebut "transformasi," di mana perjanjian internasional diubah menjadi bagian dari hukum nasional melalui proses legislasi domestik. Konsep ini memberi supremasi pada kedaulatan negara, yang berarti hukum internasional tidak dapat memaksa suatu negara untuk patuh tanpa persetujuan eksplisit melalui hukum domestiknya.[49]

Adapun Indonesia tidak secara tegas dan konsisten menganut satu aliran hukum internasional, baik monisme maupun dualisme. Sebaliknya, praktik ratifikasi dan penerapan hukum internasional di Indonesia menunjukkan adanya pendekatan hibrida atau "campuran". Posisi ini merupakan konsekuensi langsung dari rumusan konstitusional yang tidak secara eksplisit menetapkan kedudukan hukum internasional dalam sistem hukum nasional. Ketiadaan kejelasan ini menciptakan ambiguitas yang berujung pada inkonsistensi dalam praktik peradilan dan legislasi. Pada praktiknya, Indonesia sering kali menerapkan doktrin dualisme melalui mekanisme "delegasi" dan "transformasi". Proses ini mengharuskan perjanjian internasional, terutama yang tergolong sebagai *law-making treaties* yang bertujuan untuk mengubah hukum domestik, untuk melalui proses legislasi di DPR dan diubah menjadi

[48] Miftakhul Nur Arista, "Hubungan Hukum Internasional Dan Hukum Nasional," *Ma'mal: Jurnal Laboratorium Syariah Dan Hukum* 1, no. 4 (2020): 365–76.

[49] Hasanudin Hasim, "Hubungan Hukum Internasional Dan Hukum Nasional Perspektif Teori Monisme Dan Teori Dualisme," *Mazahibuna: Jurnal Perbandingan Mazhab* 1, no. 2 (2019): 166–79, https://doi.org/10.24252/mh.v1i2.10623.

undang-undang atau peraturan presiden sebelum dapat diberlakukan. Dengan kata lain, hukum internasional tidak secara otomatis berlaku di Indonesia; penerapannya bergantung pada persetujuan organ-organ negara yang berwenang, yaitu eksekutif dan legislatif. Pendekatan ini mencerminkan fokus pada kepentingan nasional dan kedaulatan, di mana negara memiliki kewenangan untuk menentukan ketentuan hukum internasional mana yang akan diberlakukan.[50]

Proses ratifikasi di Indonesia bukan sekadar prosedur formalitas, melainkan sebuah mekanisme yang berfungsi sebagai saringan politik dan hukum. [1] Sebelum suatu perjanjian diratifikasi, diperlukan kajian yang mendalam untuk memastikan bahwa materi muatan konvensi tidak bertentangan dengan asas, nilai, dan norma yang telah berlaku dalam sistem hukum nasional. [2] Proses ini, yang dikenal sebagai "harmonisasi hukum," bertujuan untuk menciptakan keselarasan antara hukum internasional dan hukum domestik.[51] Keputusan untuk meratifikasi atau tidak meratifikasi suatu konvensi sangat erat kaitannya dengan "kehendak politik" (*political will*) pemerintah dan pertimbangan kepentingan nasional. Faktor-faktor ini menjadi penentu utama dalam pengambilan keputusan, mencerminkan sifat pragmatis dalam kebijakan luar negeri Indonesia. Dengan demikian, proses ratifikasi berfungsi sebagai alat yang memungkinkan pemerintah untuk secara selektif mengadopsi norma-norma internasional yang sejalan dengan kepentingan nasional, sekaligus menolak yang dianggap dapat mengganggu kedaulatan, keamanan, atau stabilitas domestik.[52]

Kejahatan siber terutama yang terkait dengan perdagangan data ilegal di Dark Web, secara inheren bersifat transnasional. Pelaku dapat beroperasi dari satu negara, sementara korban dan bukti digital berada di negara lain yang berbeda. Sifat lintas batas ini menciptakan tantangan fundamental bagi sistem hukum yang didasarkan pada yurisdiksi teritorial. Meskipun Indonesia telah memiliki kerangka hukum nasional seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Perlindungan Data Pribadi (UU PDP), efektivitasnya dalam menangani kasus lintas batas sangat terbatas. Di sinilah Konvensi Budapest, sebagai perjanjian internasional paling komprehensif tentang kejahatan siber, menawarkan solusi yang terintegrasi. Namun, karena Indonesia belum meratifikasi konvensi ini, implikasi hukumnya sangat signifikan dan secara langsung memengaruhi kemampuan penegak hukum untuk beroperasi secara efektif di ranah global.[53]

Implikasi paling mendasar dari status non-ratifikasi adalah terhambatnya mekanisme kerja sama internasional yang cepat dan efisien. Konvensi budapest didasarkan pada tiga pilar utama, yaitu: harmonisasi hukum, kewenangan prosedural, dan kerangka kerja sama internasional yang responsif. Indonesia sebagai negara non pihak, tidak dapat secara otomatis memanfaatkan mekanisme canggih yang dirancang khusus untuk mengatasi sifat unik

[50] Hikmahanto Juwana, "Kewajiban Negara Dalam Proses Ratifikasi Perjanjian Internasional: Memastikan Keselarasan Dengan Konstitusi Dan Mentransformasikan Ke Hukum Nasional," *Undang: Jurnal Hukum* 2, no. 1 (2019): 1–32, https://doi.org/10.22437/ujh.2.1.1-32.

[51] Juwana, "Kewajiban Negara Dalam Proses Ratifikasi Perjanjian Internasional: Memastikan Keselarasan Dengan Konstitusi Dan Mentransformasikan Ke Hukum Nasional."

[52] Glendi G Tambajong, Donald Albert Rumokoy, and Stefan Obaja Voges, "Tinjauan Yuridis Ratifikasi Perjanjian Internasional Berdasarkan Undang-Undang Nomor 24 Tahun 2000," *Lex Privatum* 13, no. 4 (2024): 1–12.

[53] Jansen Chandra, Vincent Tanaka, and Ricky Banke, "Peran Interpol Dalam Menangani Dan Menanggulangi Kejahatan Siber Di Indonesia," *Peshum: Jurnal Pendidikan, Sosial Dan Humaniora* 4, no. 3 (2025): 4710–19, https://doi.org/10.56799/peshum.v4i3.9028.

kejahatan siber[54]. Pertama, ketiadaan jaringan kontak 24/7, Konvensi Budapest mensyaratkan pembentukan Jaringan Poin Kontak 24/7 di setiap negara pihak, yang memungkinkan penegak hukum untuk berkomunikasi dan berkoordinasi secara instan untuk melacak pelaku dan mengamankan bukti digital yang volatil. Indonesia, tanpa keanggotaan dalam jaringan ini, harus bergantung pada saluran Bantuan Hukum Timbal Balik (*Mutual Legal Assistance*) konvensional. Proses MLA tradisional ini dikenal lambat dan penuh birokrasi, yang sangat tidak efektif untuk kejahatan siber di mana bukti digital dapat dimusnahkan dalam hitungan detik. Kesenjangan ini menciptakan "zona aman" atau *safe havens* bagi para pelaku kejahatan di luar negeri.

Kedua, Sifat bukti digital yang mudah diubah, dihapus, atau disembunyikan menuntut prosedur investigasi yang dipercepat. Konvensi Budapest menyediakan kewenangan prosedural seperti "*expedited preservation of stored data*", yang memungkinkan satu negara meminta negara lain untuk segera mengamankan data sebelum hilang, tanpa harus melalui proses MLA yang panjang. Ketiadaan mekanisme ini secara signifikan melemahkan kemampuan penegak hukum Indonesia untuk mengamankan bukti krusial yang berada di server asing, sehingga mempersulit penuntutan. Ketiga, sistem hukum yang terfragmentasi, Non-ratifikasi Konvensi Budapest juga mengakibatkan Indonesia tidak memiliki kerangka hukum siber yang terharmonisasi dengan standar global. Meskipun UU ITE dan UU PDP mengkriminalisasi banyak perbuatan siber, perbedaan definisi dan standar hukum antarnegara tetap menjadi hambatan utama dalam kerja sama lintas batas.[55]

Keterbatasan hukum yang timbul dari non-ratifikasi ini memiliki konsekuensi nyata, yang terlihat jelas dalam kasus-kasus kebocoran data di Indonesia. Perdagangan data sensitif di Dark Web, seperti data Satu Data ASN dan NPWP yang diklaim oleh peretas Bjorka, seringkali melibatkan pelaku yang tidak berada di wilayah hukum Indonesia. Dalam kasus seperti ini, aparat penegak hukum Indonesia menghadapi dilema akut. Mereka memiliki landasan hukum domestik untuk menindak kejahatan tersebut (seperti Pasal 30 UU ITE tentang akses ilegal dan sanksi dari UU PDP), namun eksekusi hukumnya terhenti di perbatasan. Tanpa adanya Konvensi Budapest atau perjanjian bilateral yang setara, penegak hukum kesulitan untuk:[56] 1) melacak pelaku yang anonim, peretas sering menggunakan teknologi enkripsi, VPN dan server asing untuk menyamarkan jejak mereka, yang secara fundamental menghambat upaya investigasi, 2) memperoleh bukti dari luar negeri, data yang dijual di Dark Web seringkali disimpan di server di luar Indonesia. Permintaah untuk mendapatkan data ini dari penyedia layanan internet (ISP) sering menjadi sangat rumit dan lambat, sehingga bukti bisa hilang sebelum diamankan. 3) Mengekstradisi pelaku, jika pelaku berhasil diidentifikasi di negara lain, proses ekstradisi menjadi sangat sulit tanpa adanya perjanjian internasional yang mengikat, seperti yang disediakan oleh Konvensi Budapest. Dengan demikian, meskipun UU

[54] Wicaksono and Yasin, "Criminal Law Reformulation Through Omnibus Law as a Solution to Sectoral Cyber Protection (Reformulasi Hukum Pidana Melalui Omnibus Law Sebagai Solusi Perlindungan Siber Yang Bersifat Sektoral)."

[55] Joni Laksito, Maulana Fahmi Idris, and Agus Waryanto, "Hak Dan Kewajiban Negara Dalam Mengatasi Kejahatan Lintas Batas Di Era Digital: Pendekatan Anlisis Normatif," *Hakim: Jurnal Ilmu Hukum Dan Sosial* 2, no. 4 (2024): 774–90, https://doi.org/10.51903/hakim.v2i4.2154.

[56] Ayman Hammam Abdurrohman, Cahyo Nurul Uzmawi, and Ridwan Khoiruddin, "Cybersecurity Dan Pancasila: Harmonisasi Regulasi Hukum Internasional Dengan Kepentingan Nasional," *JDHI: Jurnal Dinamika Hukum Indonesia* 1, no. 1 (2025): 23–29.

PDP memiliki klausa ekstrateritorial yang progresif, implementasinya di lapangan menjadi kurang efektif karena kurangnya instrumen kerja sama yang mendukungnya.

Adapun alasan Indonesia belum meratifikasi Konvensi Budapest tidak hanya bersifat yuridis, tetapi juga politis, terkait dengan isu kedaulatan dan potensi pelanggaran hak asasi manusia. Beberapa pihak mengkhawatirkan bahwa ratifikasi akan mengharuskan Indonesia untuk mengorbankan sebagian kedaulatan hukumnya dan memberikan kewenangan yang luas kepada otoritas asing untuk mengakses data. Kekhawatiran ini mirip dengan posisi Indonesia terhadap konvensi internasional lainnya, seperti Konvensi Pengungsi 1951, di mana Indonesia menganggap instrumen hukum nasional sudah cukup dan tidak ingin terikat oleh kewajiban internasional yang dianggap berat. Namun, penolakan yang didasarkan pada pertimbangan kedaulatan ini justru menimbulkan ironi: dengan tidak meratifikasi Konvensi Budapest, Indonesia secara ironis menjadi lebih rentan. Negara kehilangan kontrol atas keamanan datanya di ranah global, dan kedaulatan digitalnya dapat tergerus oleh serangan siber yang tidak dapat ditindak secara efektif. Keputusan ini, yang dimaksudkan untuk melindungi kedaulatan, justru menghasilkan hilangnya kontrol atas keamanan data warga negara di pasar ilegal yang tidak memiliki batas.

KESIMPULAN

Kejahatan siber khususnya perdagangan data ilegal di Dark Web telah menjadi ancaman nyata yang kompleks, bersifat lintas batas, dan terus berkembang. Indonesia memang telah memiliki landasan hukum berupa UU ITE dan UU PDP untuk melindungi data pribadi serta menindak kejahatan siber, namun implementasinya masih menghadapi banyak hambatan, seperti anonimitas pelaku, keterbatasan yurisdiksi, kekosongan aturan turunan, dan belum terbentuknya otoritas pengawas independen. Ketiadaan ratifikasi terhadap *Budapest Convention* semakin memperlemah kemampuan Indonesia dalam melakukan penegakan hukum lintas negara karena tidak dapat memanfaatkan mekanisme kerja sama cepat seperti jaringan kontak 24/7, harmonisasi hukum, serta prosedur preservasi data yang dipercepat. Akibatnya, Indonesia kesulitan melacak pelaku, mengamankan bukti digital, dan menuntut kejahatan siber yang melibatkan pelaku dan infrastruktur di luar negeri. Oleh karena itu, untuk memperkuat ketahanan siber nasional, Indonesia perlu memperbaiki implementasi hukum nasional yang ada, membentuk otoritas perlindungan data yang independen, serta mempertimbangkan ratifikasi *Budapest Convention* agar mampu berkolaborasi secara efektif dalam menanggulangi kejahatan siber transnasional.

DAFTAR PUSTAKA

[1] A, Yuniar. “Collaboration Is the Key to Indonesia Cyber Resilience: BSSN.” *Gov Insider*, September 8, 2025. https://govinsider.asia/intl-en/article/collaboration-is-the-key-to-indonesia-cyber-resilience-bssn.

[2] Abdurrohman, Ayman Hammam, Cahyo Nurul Uzmawi, and Ridwan Khoiruddin. “Cybersecurity Dan Pancasila: Harmonisasi Regulasi Hukum Internasional Dengan Kepentingan Nasional.” *JDHI: Jurnal Dinamika Hukum Indonesia* 1, no. 1 (2025): 23–29.

[3] Aditya, Addin. “Upaya Preventif Cegah Kejahatan Siber Dan Penyalahgunaan Transaksi Elektronik Melalui Sosialisasi UU ITE.” *Jurnal Abdimas Nusa Mandiri* 6, no. 1 (2024): 22–27. https://doi.org/10.33480/abdimas.v6i1.5370.

[4] Aini, Nurul, and Fauziah Lubis. "Tantangan Pembuktian Dalam Kasus Kejahatan Siber." *Judge: Jurnal Hukum* 5, no. 2 (2024): 55–63. https://doi.org/doi.org/10.54209/judge.v5i02.566.

[5] Aji, Muhammad Prakoso. "Sistem Keamanan Siber Dan Kedaulatan Data Di Indonesia Dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) (Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective)." *Jurnal Politica* 13, no. 2 (2022): 222–38. http://dx.doi.org/10.22212/jp.v13i2.3299.

[6] Aldiansyah, Faisal. "Serangan Siber Terbesar Yang Pernah Terjadi Di Indonesia." *Netmarks*, April 14, 2024. https://www.netmarks.co.id/post/serangan-siber-terbesar-yang-pernah-terjadi-di-indonesia.

[7] Argiansyah, Hikmal Yusuf, and M. Rizki Yudha Prawira. "Analisis Hukum Hak Atas Privasi Dan Perlindungan Data Pribadi Berdasarkan Perspektif Hak Asasi Manusia." *Jurnal Hukum Pelita* 5, no. 1 (2024): 61–75.

[8] Arista, Miftakhul Nur. "Hubungan Hukum Internasional Dan Hukum Nasional." *Ma'mal: Jurnal Laboratorium Syariah Dan Hukum* 1, no. 4 (2020): 365–76.

[9] Ariyaningsih, Sindy, A. Ari Andrianto, Adri Surya Kusuma, and Rina Arum Prastyanti. "Korelasi Kejahatan Siber Dengan Percepatan Digitalisasi Di Indonesia." *Justisia: Jurnal Ilmu Hukum* 1, no. 1 (2023): 1–11. https://doi.org/10.56457/jjih.v1i1.38.

[10] Bahreisy, Muhammad Naufal. "Analisis Halaman-Halaman Dark Web Untuk Mendukung Investigasi Kejehatan." Skripsi, Universitas Islam Indonesia, 2020. https://dspace.uii.ac.id/bitstream/handle/123456789/28362/16917113%20M%20Naufal%20Bahreisy.pdf?sequence=1.

[11] Brandeis and Warren. "The Right to Privacy." *Harvard Law Review* IV, no. 5 (1890): 193–220.

[12] Chandra, Jansen, Vincent Tanaka, and Ricky Banke. "Peran Interpol Dalam Menangani Dan Menanggulangi Kejahatan Siber Di Indonesia." *Peshum: Jurnal Pendidikan, Sosial Dan Humaniora* 4, no. 3 (2025): 4710–19. https://doi.org/10.56799/peshum.v4i3.9028.

[13] Daeng, Yusuf, Jimmy Levin, Karolina Karolina, and Muhammad Razzaq Prayudha. "Analisis Penerapan Sistem Keamanan Siber Terhadap Kejahatan Siber Di Indonesia." *Innovative: Journal of Social Network Science Research* 3, no. 6 (2023): 1135–45.

[14] EC-Council University. "Exploring the Dark Web and Its Dangers." *EC-Council University*, Agustus 2025. https://www.eccu.edu/blog/the-dark-web-and-its-dangers/.

[15] ———. "Exploring the Dark Web Dan Its Dangers." *EC-Council University*, Agustus 2025. https://www.eccu.edu/blog/the-dark-web-and-its-dangers/.

[16] Fahamsyah, Ermanto, Vicko Taniady, Kania Venisa Rachim, and Novi Wahyu Riwayanti. "Penerapan Prinsip Aut Dedere Aut Judicare Terhadap Pelaku Cybercrime Lintas Negara Melalui Ratifikasi Budapest Convention." *De Jure: Jurnal Hukum Dan Syariah* 14, no. 1 (2022): 140–59. http://dx.doi.org/10.18860/j-fsh.v14i1.15731.

[17] Farrier, Ellie. "What Is the Dark Web?" *AVG*, March 5, 2025. https://www.avg.com/en/signal/what-is-the-dark-web.

[18] Febrian, Wahyu Rifqi, Raden Mohammad Rangga Faturrahman, and Hannah Syahida Rahmadina. "The Role of International Law in Handling Cyber Crime Cases." *Jurnal*

ISSN 2798-3471 (Cetak)
ISSN 2798-3641 (Online)

Sahid Da'watii 3, no. 2 (2024): 1–7. https://doi.org/10.56406/jurnalsahiddawatii.v3i02.481.

[19] Ferdiansyah, Aldi, Berdi Adityas Wiryawan Wahyono, and Almansyah Harahap. "Pengaruh Penerapan Undang-Undang ITE Terhadap Tingkat Kejahatan Siber Di Indonesia." *Jurnal Kajian Hukum Dan Kebijakan Publik* 2, no. 2 (2025): 924–30. https://doi.org/10.62379/bza49768.

[20] Flare. "Top 5 Dark Web Marketplaces to Monitor." *Flare*, April 6, 2023. https://flare.io/learn/resources/blog/dark-web-marketplaces/.

[21] Hasim, Hasanudin. "Hubungan Hukum Internasional Dan Hukum Nasional Perspektif Teori Monisme Dan Teori Dualisme." *Mazahibuna: Jurnal Perbandingan Mazhab* 1, no. 2 (2019): 166–79. https://doi.org/10.24252/mh.v1i2.10623.

[22] Hidayah, Ghufron Rosadi, Ha. Djazim Ma'shum, and Muhammad Awaluddin. "Studi Komparatif Perlindungan Data Pribadi Dalam UU ITE 2024 Dan UU PDP 2022." *Jurnal Riset Rumpun Ilmu Sosial, Politik Dan Humaniora* 4, no. 4 (2025): 61–70. https://doi.org/10.55606/jurrish.v4i4.6341.

[23] Ibrahim, Johny. *Teori Dan Metodologi Penelitian Hukum Normatif*. Sumatera Utara: Bayumedia, 2008.

[24] Juwana, Hikmahanto. "Kewajiban Negara Dalam Proses Ratifikasi Perjanjian Internasional: Memastikan Keselarasan Dengan Konstitusi Dan Mentransformasikan Ke Hukum Nasional." *Undang: Jurnal Hukum* 2, no. 1 (2019): 1–32. https://doi.org/10.22437/ujh.2.1.1-32.

[25] Laksito, Joni, Maulana Fahmi Idris, and Agus Waryanto. "Hak Dan Kewajiban Negara Dalam Mengatasi Kejahatan Lintas Batas Di Era Digital: Pendekatan Anlisis Normatif." *Hakim: Jurnal Ilmu Hukum Dan Sosial* 2, no. 4 (2024): 774–90. https://doi.org/10.51903/hakim.v2i4.2154.

[26] Marzuki, Peter Mahmud. *Penelitian Hukum (Edisi Revisi)*. Jakarta: Kencana, 2014.

[27] Muhaimin. *Metode Penelitian Hukum*. Mataram: Mataram University Press, 2020.

[28] Nath, Asoke, and Romita Mondal. "Dark Web: The Uniluminated Side of the World Wide Web." *International Journal of Computer Science and Engineering* 7, no. 1 (2019): 296–305. https://doi.org/10.26438/ijcse/v7i1.296305.

[29] OECD. "The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines." *OECD Publishing* 1, no. 176 (2011): 1–50. https://doi.org/10.1787/5kgf09z90c31-en.

[30] Pramudya, Deva Wira, and Hudi Yusuf. "Pencurian Data Identitas Sebagai Kejahatan Cyber Related Crime: Tinjauan Kriminologis Atas Kasus Pencurian Data Pada Akun Marketplace." *JIIC: Jurnal Intelek Insan Cendikia* 2, no. 7 (2025): 13469–78.

[31] Purba, Yedija Otniel, and Agus Mauluddin. "Kejahatan Siber Dan Kebijakan Identitas Kependudukan Digital: Sebuah Studi Tentang Potensi Pencurian Data Online." *Jurnal CIC Lembaga Riset Dan Konsultan Sosial* 5, no. 2 (2023): 55–66. https://doi.org/10.51486/jbo.v5i2.113.

[32] Puspitasari, Diah, Sintia Kartini Haniandaresta, and Dalila Afif. "Urgensi Undang-Undang Perlindungan Data Pribadi Dalam Mengatasi Masalah Keamanan Data Penduduk." *Journal of Administrative and Social Science* 4, no. 2 (2023): 195–205. https://doi.org/10.55606/jass.v4i2.403.

[33] Putra, Akbar K. "Harmonisasi Konvensi Cyber Crime Dalam Hukum Nasional." *Jurnal*

Ilmu Hukum Jambi 5, no. 2 (2014): 95–109.
[34] Rolando, Dede Mercy, Hanna Hilyati Aulia, and Mutia Tanseba Andini. "Transformasi Digital Dan Ancaman Cybercrime." *Siyasah: Jurnal Hukum Tata Negara* 3, no. 1 (2023): 68–84. https://doi.org/10.32332/siyasah.v3i1.7441.
[35] Rosadi, Sinta Dewi. "Protecting Privacy on Personal Data in Digital Economic Era: Legal Framework in Indonesia." *Brawijaya Law Journal* 5, no. 1 (2018): 143–57. https://doi.org/10.21776/ub.blj.2018.005.01.09.
[36] Sigalingging, Bisdan. "Bantuan Hukum Timbal Balik Dalam Perampasan Aset Korupsi Antar Lintas Batas Negara." *Luris Studia: Jurnal Kajian Hukum* 2, no. 3 (2021): 387–98.
[37] Suharto, Miko Aditya, and Maria Novita Apriyani. "Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional." *Risalah Hukum* 17, no. 2 (2021): 98–107. https://doi.org/10.30872/risalah.v17i2.705.
[38] Sulistianingsih, Dewi, Miftakhul Ihwan, Andry Setiawan, and Muchammad Shidqon Prabowo. "Tata Kelola Perlindungan Data Pribadi Di Era Metaverse (Telaah Yuridis Undang-Undang Perlindungan Data Pribadi)." *Masalah-Masalah Hukum* 52, no. 1 (2023): 97–106. https://doi.org/10.14710/mmh.52.1.2023.97-106.
[39] Tambajong, Glendi G, Donald Albert Rumokoy, and Stefan Obaja Voges. "Tinjauan Yuridis Ratifikasi Perjanjian Internasional Berdasarkan Undang-Undang Nomor 24 Tahun 2000." *Lex Privatum* 13, no. 4 (2024): 1–12.
[40] The Convention on Cybercrime (2024).
[41] Wahyudi, Djafar. *Privasi 101: Panduan Memahami Privasi, Perlindungan Data Dan Surveilans*. Jakarta: Elsam, 2015.
[42] Wicaksana, Pradnya. "Pakar Hukum Suber Unair: Indonesia Harus Meratifikasi Budapest Convention." *Universitas Airlangga*, September 12, 2022. https://unair.ac.id/pakar-hukum-siber-unair-indonesia-harus-meratifikasi-budapest-convention/.
[43] Wicaksono, Agung Tri, and Ikhsan Fatah Yasin. "Criminal Law Reformulation Through Omnibus Law as a Solution to Sectoral Cyber Protection (Reformulasi Hukum Pidana Melalui Omnibus Law Sebagai Solusi Perlindungan Siber Yang Bersifat Sektoral)." *Al-Jinayah: Jurnal Hukum Pidana Islam* 10, no. 2 (2024): 237–61. https://doi.org/10.15642/aj.2024.10.2.237-261.
[44] Wikipedia. "Darkent Markets." *Wikipedia*, Agustus 2025. https://en.wikipedia.org/wiki/Darknet_market.
[45] Winarni, Rini Retno. "Efektivitas Penerapan Undang-Undang ITE Dalam Tindak Pidana Cyber Crime." *Hukum Dan Dinamika Masyarakat* 14, no. 1 (2016): 16–27.
[46] Wuwungan, Meyse Stevely Sisilia. "Perlindungan Hukum Terhadap Pemilik Data Pribadi Pengguna Teknologi Informasi Akibat Tindak Pidana Peretasan." *Lex Privatum* 13, no. 4 (2024): 1–12.
[47] Yudistira, Muhammad, and Ramadani Ramadani. "Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang Nomor 27 Tahun 2022 Oleh Kominfo." *Unes Law Review* 5, no. 4 (2023): 3917–29. https://doi.org/10.31933/unesrev.v5i4.698.

ISSN 2798-3471 (Cetak)
ISSN 2798-3641 (Online)