ULIL ALBAB : Jurnal Ilmiah Multidisiplin
Vol.5, No.11, Oktober 2026

Problematika Hukum Pidana dalam Era Digital di Indonesia: Tantangan, Kesenjangan Regulasi, dan Arah Pembaharuan

Muhammad Anggil Setiadi
Magister Hukum/ Universitas Widya Mataram, Indonesia
E-mail: muhammadanggil010@gmail.com

Article History:
Received: 23 Juli 2026
Revised: 20 September 2026
Accepted: 08 Oktober 2026

Keywords: *Kejahatan, Siber, Pidana, UU ITE, KUHP.*

Abstrak: *Perkembangan teknologi informasi dan komunikasi telah mengubah lanskap kriminalitas di Indonesia. Kejahatan konvensional kini bermutasi menjadi kejahatan siber (cybercrime) yang bersifat lintas batas (transnational), anonim, dan cepat. Jurnal ini menganalisis problematika penegakan hukum pidana materiil dan pidana formil di Indonesia dalam menghadapi era digital. Masalah utama terletak pada lambatnya adaptasi regulasi (seperti UU ITE dan KUHP Baru UU 1/2023) terhadap modus kejahatan baru seperti deepfake, crypto-scam, dan cyberbullying, serta kendala pembuktian digital (digital evidence). Dengan metode penelitian yuridis-normatif, jurnal ini menyimpulkan perlunya rekonstruksi hukum acara pidana digital dan penguatan kapasitas aparat penegak hukum guna mewujudkan keadilan yang progresif.*

PENDAHULUAN

Memasuki dekade ketiga abad ke-21, umat manusia berada dalam pusaran revolusi industri 4.0 dan menuju era Society 5.0. Transformasi ini ditandai dengan integrasi ruang fisik dan ruang siber (*cyber space*) yang digerakkan oleh lompatan teknologi informasi, seperti kecerdasan buatan (*Artificial Intelligence*), internet untuk segala (*Internet of Things*), komputasi awan (*cloud computing*), dan teknologi rantai blok (*blockchain*). Di Indonesia, fenomena digitalisasi ini berkembang sangat masif. Berdasarkan data penetrasi internet yang terus meroket, mayoritas masyarakat kini menggantungkan aktivitas ekonomi, sosial, hingga pemenuhan hak informasi pada ekosistem digital.

Namun, sebagaimana dua sisi mata uang, akselerasi teknologi tidak hanya membawa daya guna bagi peradaban, melainkan juga melahirkan ancaman baru yang destruktif. Dunia virtual menjelma menjadi ruang inkubasi baru bagi kejahatan. Karakteristik ruang siber yang asimetris, tanpa batas (*borderless*), anonim (*anonymity*), dan beroperasi dalam hitungan detik, telah mendematerialisasi konsep kejahatan konvensional. Tindak pidana yang dahulu membutuhkan kehadiran fisik, interaksi tatap muka, dan lokus yang jelas, kini telah bermutasi menjadi kejahatan berbasis digital (*cybercrime* atau *cyber-enabled crime*).

Kondisi tersebut menempatkan hukum pidana Indonesia dalam posisi yang dilematis. Secara sosiologis dan yuridis, hukum pidana dituntut untuk menjalankan fungsinya sebagai *otonom* (menjaga kepastian hukum) sekaligus *responsif* (mengikuti perkembangan masyarakat). Hukum pidana Indonesia, yang fondasi klasiknya berakar dari sistem kodifikasi kontinental warisan kolonial, dibangun berdasarkan asumsi-asumsi fisik: pelaku yang terlihat, barang bukti yang kasat

mata, serta batas yurisdiksi teritorial yang rigid. Ketika dihadapkan pada realitas digital, pilar-pilar hukum klasik ini mengalami guncangan hebat.

Di ranah hukum materiil, perundang-undangan Indonesia sering kali gagap dan terlambat dalam merespons modus operandi kejahatan digital yang kian canggih. Meskipun Indonesia telah memiliki Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang telah beberapa kali direvisi, serta Kitab Undang-Undang Hukum Pidana (KUHP) Nasional baru, kesenjangan regulasi (*regulatory gap*) tetap menganga. Sebagai contoh, kriminalisasi terhadap pemanfaatan teknologi manipulasi digital seperti *deepfake* untuk tindakan pornografi balas dendam (*revenge porn*) atau penipuan, masih sulit dijerat karena biasnya subjek hukum dan pertanggungjawaban pidana (*criminal liability*) pada sistem kecerdasan buatan. Begitu pula dengan kejahatan kerah putih di sektor keuangan digital yang memanfaatkan aset kripto terdesentralisasi (*Decentralized Finance*), yang kerap lolos dari jerat pasal penipuan konvensional.

Di sisi lain, problematika pada aspek hukum formil (hukum acara pidana) tidak kalah krusial. Kitab Undang-Undang Hukum Acara Pidana (KUHAP) yang ada saat ini dirancang pada tahun 1981, sebuah era di mana data digital belum dikenal. Akibatnya, timbul ketidakpastian hukum mengenai standarisasi penanganan alat bukti elektronik (*digital evidence*). Proses penemuan, penyitaan, pemeliharaan rantai penjagaan (*chain of custody*), hingga digital forensik sering kali terhambat oleh keterbatasan regulasi pembuktian dan ketidakmerataan infrastruktur teknologi di berbagai wilayah kepolisian di Indonesia. Akibatnya, tidak sedikit kasus-kasus kejahatan siber yang kandas di persidangan akibat orisinalitas bukti digital yang diragukan atau gagal diverifikasi secara sahih.

Tantangan ini semakin diperumit oleh disparitas kompetensi aparat penegak hukum (hakim, jaksa, polisi) dalam memahami arsitektur teknologi. Celah pemahaman (*knowledge gap*) antara pelaku kejahatan siber yang *tech-savvy* dengan aparat hukum kerap memicu fenomena salah sasar pidana (*miscarriage of justice*), atau sebaliknya, pembiaran kejahatan akibat ketidakmampuan membuktikan elemen pidana siber secara logis-ilmiah.

Mengingat daya rusak kejahatan digital yang bersifat lintas batas negara (*transnational crime*) dan mampu melumpuhkan infrastruktur kritis nasional dalam sekejap, reposisi dan pembaharuan hukum pidana Indonesia menjadi agenda yang mendesak. Pembaharuan hukum pidana tidak boleh lagi bersifat parsial atau sekadar "tambal sulam" aturan sektoral. Diperlukan sebuah arah pembaharuan yang holistik, progresif, dan visioner demi mewujudkan keadilan substantif di era digital.

Oleh karena itu, penelitian dalam jurnal ini menjadi penting untuk memetakan secara komprehensif letak simpul-simpul kelemahan hukum pidana Indonesia—baik dari aspek materiil, formil, maupun struktural aparat penegaknya. Melalui pendekatan yuridis-normatif, artikel ini bertujuan untuk menguraikan problem-problem krusial tersebut sekaligus merumuskan cetak biru (*blueprint*) rekonstruksi hukum acara pidana siber, harmonisasi pasal materiil, serta penguatan institusi penegak hukum di Indonesia. Upaya ini dilakukan semata-mata agar hukum tidak melulu berjalan tertatih-tatih di belakang dinamika teknologi, melainkan mampu hadir sebagai instrumen rekayasa sosial (*tool of social engineering*) yang menjamin kepastian hukum dan melindungi hak-hak digital warga negara Indonesia.

METODE PENELITIAN

Penelitian yuridis-normatif berfokus pada pengkajian hukum yang dikonsepkan sebagai norma, kaidah, asas, maupun doktrin yang terdapat dalam peraturan perundang-undangan. Fokus utama dari metode ini adalah menguji sinkronisasi, konsistensi, serta kesenjangan (*regulatory gap*)

antara regulasi hukum pidana yang ada saat ini dengan realitas perkembangan kejahatan di era digital.

Untuk membedah problematika hukum secara komprehensif, penelitian ini menerapkan 4 (empat) pendekatan hukum (*legal approach*), yaitu:

1. **Pendekatan Perundang-undangan (*Statute Approach*):** Dilakukan dengan menelaah seluruh regulasi yang berkaitan dengan hukum pidana digital di Indonesia, antara lain Kitab Undang-Undang Hukum Pidana (KUHP) Nasional (UU No. 1 Tahun 2023), Kitab Undang-Undang Hukum Acara Pidana (KUHAP), UU Informasi dan Transaksi Elektronik (UU ITE), serta UU Pelindungan Data Pribadi (UU PDP).
2. **Pendekatan Konseptual (*Conceptual Approach*):** Bergerak dari doktrin, konsep, dan asas-asas hukum pidana (seperti asas legalitas, pertanggungjawaban pidana/*criminal liability*, dan teori pembuktian) untuk menjawab tantangan hukum siber yang belum diatur secara eksplisit dalam undang-undang.
3. **Pendekatan Komparatif (*Comparative Approach*):** Melakukan perbandingan secara terbatas dengan instrumen hukum internasional—seperti *Budapest Convention on Cybercrime*—guna melihat arah standardisasi hukum acara pidana digital global yang dapat diadopsi di Indonesia.
4. **Pendekatan Kasus (*Case Approach*):** Menganalisis beberapa yurisprudensi atau preseden putusan pengadilan terkait kejahatan siber di Indonesia untuk melihat bagaimana hakim menginterpretasikan alat bukti digital di persidangan.

Data yang digunakan dalam penelitian ini sepenuhnya berasal dari data sekunder yang diklasifikasikan ke dalam tiga jenis bahan hukum, yaitu:

1. **Bahan Hukum Primer:** Bahan hukum yang memiliki kekuatan hukum mengikat secara formal, meliputi:
   a. Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP Nasional).
   b. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta seluruh perubahannya (UU ITE).
   c. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP).
   d. Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (KUHAP).
2. **Bahan Hukum Sekunder:** Bahan hukum yang memberikan penjelasan mengenai bahan hukum primer, terdiri dari buku teks hukum pidana siber, jurnal ilmiah terakreditasi (nasional maupun internasional), tesis, naskah akademik rancangan undang-undang, serta laporan hasil riset lembaga kajian hukum (*think tank*).
3. **Bahan Hukum Tersier:** Bahan hukum yang memberikan petunjuk maupun penjelasan terhadap bahan hukum primer dan sekunder, seperti kamus besar bahasa Indonesia (KBBI), kamus hukum (*black's law dictionary*), dan ensiklopedia digital.

Teknik pengumpulan bahan hukum dalam penelitian ini dilakukan melalui **studi kepustakaan** (*library research*), yaitu dengan mengidentifikasi, menginventarisasi, membaca, dan mencatat bahan-bahan hukum yang relevan dengan isu hukum pidana digital.

Bahan hukum yang telah terkumpul kemudian diseleksi dan dianalisis menggunakan metode **analisis kualitatif** dengan penalaran logika deduktif. Metode deduktif bergerak dari premis mayor (aturan hukum pidana, asas hukum, dan teori-teori universal) menuju premis minor (fakta mengenai kejahatan digital baru, ketidaksiapan KUHAP, dan kendala penegakan hukum). Hasil dari analisis ini ditarik konklusi objektif guna menjawab rumusan masalah mengenai peta problematika hukum pidana materiil dan formil, sekaligus merumuskan rekomendasi arah

pembaruan hukum pidana di Indonesia secara komprehensif.

HASIL DAN PEMBAHASAN

A. Problematika Hukum Pidana Materiil dalam Menjerat Modus Operandi Kejahatan Digital Baru

Hukum pidana materiil berkaitan erat dengan substansi larangan perbuatan (kriminalisasi) dan syarat pertanggungjawaban pidana (*criminal liability*). Di era digital, doktrin hukum pidana klasik menghadapi tantangan berat akibat munculnya kejahatan yang tidak lagi melibatkan interaksi fisik antarmanusia, melainkan interaksi antar-sistem atau manipulasi data digital. Penelitian ini menemukan tiga area krusial yang mengalami kesenjangan regulasi (*regulatory gap*) di Indonesia:

1. Kebuntuan Hukum Pertanggungjawaban Pidana Kecerdasan Buatan (Artificial Intelligence) dan Deepfake

   Teknologi kecerdasan buatan, khususnya *deepfake* (manipulasi berbasis kecerdasan buatan untuk meniru wajah atau suara manusia), telah digunakan untuk memproduksi konten pornografi balas dendam (*revenge porn*), penipuan daring, hingga penyebaran disinformasi politik.

   Dalam doktrin hukum pidana Indonesia, subjek hukum pidana yang utama adalah orang perorangan (*natuurlijke persoon*) yang bertumpu pada asas tiada pidana tanpa kesalahan (*geen straf zonder schuld* / *mens rea*). Ketika teknologi *deepfake* merugikan korban, muncul problematika atribusi kesalahan:

   Siapa yang harus bertanggung jawab secara pidana?

   a. Apakah *developer* yang membuat algoritma awal?
   b. Pengguna (*user*) yang mengoperasikan aplikasi tersebut?
   c. Atau sistem kecerdasan buatan itu sendiri yang bertindak secara otonom?

   Meskipun KUHP Nasional (UU No. 1 Tahun 2023) telah memperluas cakupan subjek hukum korporasi, regulasi kita belum mengenal konsep *electronic personhood* (subjek hukum elektronik). Hukum pidana materiil Indonesia saat ini hanya mampu menjerat pengguna (*user*) akhir dengan pasal-pasal konvensional (seperti pasal pencemaran nama baik atau pornografi dalam UU ITE), namun gagal menyentuh akar permasalahan penyalahgunaan teknologi penyedia algoritmanya.

2. Kejahatan Kripto dan Desentralisasi Keuangan (DeFi)

   Kesenjangan regulasi materiil juga terlihat jelas pada maraknya kasus *crypto-scam* (penipuan berbasis aset kripto) dan pemanfaatan platform *decentralized finance* (DeFi) untuk pencucian uang. Pasal penipuan tradisional dalam Pasal 378 KUHP Lama atau Pasal 492 KUHP Baru mensyaratkan adanya unsur "menggerakkan orang lain dengan memakai nama palsu atau martabat palsu."

   Dalam skema penipuan kripto (seperti *rug pull*—di mana pengembang membawa kabur dana investor), tidak ada interaksi personal langsung. Pelaku berlindung di balik *smart contract* (kontrak pintar otomatis) yang terdesentralisasi. Hukum pidana materiil Indonesia masih kesulitan merumuskan batas-batas melawan hukum (*wederrechtelijkheid*) dalam transaksi manipulatif berbasis kode komputer (*code is law*), sehingga banyak korban penipuan digital jenis ini tidak mendapatkan perlindungan hukum pidana yang memadai.

B. **Problematika** Hukum Pidana Formil: Tantangan Alat Bukti Elektronik (*Digital Evidence*) dan Yurisdiksi

Hukum pidana formil (hukum acara) berfungsi menegakkan hukum pidana materiil. Realitas menunjukkan bahwa secanggih apa pun pasal hukum materiil dibuat, ia akan lumpuh jika hukum acaranya tidak adaptif terhadap karakteristik bukti digital yang bersifat volatil (mudah berubah/dihapus) dan tidak kasat mata.

1. Kerapuhan Rantai Penjagaan (*Chain of Custody*) dan Keterbatasan KUHAP

Alat bukti elektronik secara formal telah diakui dalam Pasal 5 UU ITE dan diperkuat dalam UU Pelindungan Data Pribadi (UU PDP). Namun, Kitab Undang-Undang Hukum Acara Pidana (KUHAP) tahun 1981 yang menjadi tulang punggung hukum acara di Indonesia belum pernah direvisi secara komprehensif untuk mengatur tata cara penanganan bukti digital.

Problematika utama terletak pada prosedur *chain of custody* (mata rantai penjagaan alat bukti). Berbeda dengan barang bukti fisik seperti pisau atau uang tunai, bukti digital seperti *log file*, riwayat obrolan WhatsApp, atau metadata server sangat rentan dimanipulasi tanpa meninggalkan jejak kasat mata.

Apabila penyidik kepolisian di lapangan melakukan kesalahan kecil saat menyita gawai—misalnya tidak memasukkannya ke dalam *faraday bag* sehingga gawai tersebut dapat diakses atau dihapus datanya dari jarak jauh oleh pelaku—maka nilai otentisitas bukti tersebut gugur di persidangan. Ketiadaan standar operasional baku yang mengikat dalam KUHAP menimbulkan disparitas putusan hakim dalam menilai sah atau tidaknya suatu bukti elektronik.

2. Konflik Yurisdiksi Lintas Batas (*Transnational Jurisdiction*)

Karakteristik kejahatan digital adalah *borderless* (tanpa batas). Sebagai contoh, dalam banyak kasus judi online, *phishing*, atau peretasan situs pemerintah di Indonesia, pelaku atau server utamanya berada di luar negeri (misalnya di Asia Tenggara atau Eropa Timur).

Asas teritorialitas yang dianut dalam Pasal 2 KUHP mengalami disorientasi di ruang siber. Ketika penyidik Indonesia ingin melacak alamat IP (*IP Address*) pelaku, mereka membentur tembok yurisdiksi negara lain. Mekanisme *Mutual Legal Assistance* (MLA) yang bersifat birokratis antarpemerintah memakan waktu berbulan-bulan bahkan bertahun-tahun. Padahal, dalam hukum acara pidana siber, keterlambatan hitungan menit saja dapat membuat pelaku menghapus seluruh data digital secara permanen (*anti-forensics*).

3. Arah Pembaharuan Hukum Pidana Indonesia di Era Digital

Menghadapi kompleksitas di atas, Indonesia tidak bisa lagi mengandalkan regulasi "tambal sulam". Diperlukan rekonstruksi hukum pidana yang bersifat progresif melalui tiga pilar pembaharuan:

a. **Harmonisasi Regulasi Materiil:** Mempercepat pembentukan undang-undang khusus atau aturan turunan KUHP Baru yang secara eksplisit mengkriminalisasi penyalahgunaan teknologi AI, manipulasi sintetis (*deepfake*), serta mendefinisikan ulang subjek hukum peretas otonom.

b. **Kodifikasi KUHAP Baru (Hukum Acara Siber):** Mendesak dilakukannya amandemen KUHAP dengan menyisipkan bab khusus mengenai *Cyber Procedure*. Bab ini harus mengatur standardisasi forensik digital, kewenangan penyitaan data di awan (*cloud data seizure*), dan perlindungan hak privasi warga negara agar tidak terjadi penyalahgunaan wewenang oleh aparat.

c. **Restorative Justice di Ruang Siber:** Mengingat masifnya kasus-kasus pelanggaran UU ITE skala kecil (seperti penghinaan di media sosial), hukum pidana harus memprioritaskan keadilan restoratif (*restorative justice*) guna mencegah kepadatan berlebih di lembaga pemasyarakatan (*overcrowding*), sekaligus memfokuskan sumber daya penegak hukum untuk memburu pelaku kejahatan siber kerah putih berskala besar.

KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang telah diuraikan sebelumnya, maka dapat ditarik kesimpulan sebagai berikut:

1. **Problematika Hukum Pidana Materiil (Substansi Hukum):**

   Dinamika teknologi digital telah melahirkan modus operandi kejahatan baru yang memicu terjadinya kesenjangan regulasi (*regulatory gap*) di Indonesia. Doktrin hukum pidana klasik mengalami kebuntuan dalam mengatribusikan pertanggungjawaban pidana (*criminal liability*) pada teknologi kecerdasan buatan (*Artificial Intelligence*) seperti *deepfake* dan penipuan berbasis aset kripto/DeFi. Regulasi yang ada saat ini (termasuk KUHP Nasional dan UU ITE) belum mengadopsi konsep *electronic personhood*, sehingga penegakan hukum materiil cenderung hanya mampu menyentuh pengguna akhir (*end-user*) dan gagal menjerat aktor utama atau penyedia sistem algoritmanya.
2. **Problematika Hukum Pidana Formil (Hukum Acara):**

   Hukum acara pidana Indonesia mengalami disorientasi di ruang siber karena masih bertumpu pada Kitab Undang-Undang Hukum Acara Pidana (KUHAP) tahun 1981 yang bercorak konvensional-fisik. Masalah krusial terletak pada ketiadaan kodifikasi baku mengenai hukum acara siber (*cyber procedure*), khususnya terkait standardisasi penanganan mata rantai penjagaan (*chain of custody*) alat bukti elektronik yang bersifat volatil. Hal ini diperumit oleh benturan yurisdiksi lintas batas (*transnational jurisdiction*) dan birokrasi MLA yang lambat, sehingga sering kali menyebabkan hilangnya bukti digital dan kegagalan penegakan hukum (*miscarriage of justice*).

B. Saran (Rekomendasi Kebijakan)

Guna mengatasi problematika di atas, maka arah pembaharuan hukum pidana Indonesia ke depan harus difokuskan pada tiga poin rekomendasi berikut:

1. **Pembaruan Legislasi Materiil:** Pemerintah dan DPR perlu segera menyusun regulasi turunan dari KUHP Nasional (UU No. 1 Tahun 2023) atau merevisi UU ITE secara berkala untuk melegislasi perluasan subjek hukum berbasis teknologi, merumuskan batasan sifat melawan hukum dalam pemanfaatan AI, serta memberikan perlindungan hukum pidana yang komprehensif bagi korban kejahatan finansial digital.
2. **Akselerasi Amandemen KUHAP Baru:** Indonesia mendesak untuk memiliki KUHAP baru yang menyisipkan bab khusus mengenai tata cara penyidikan tindak pidana siber. Regulasi ini wajib memuat aturan rigid mengenai legalitas penyitaan data berbasis awan (*cloud data*), standardisasi pengujian forensik digital nasional, serta mekanisme kerja sama penegakan hukum lintas negara yang lebih taktis dan cepat.
3. **Peningkatan Kapasitas Struktural:** Diperlukan komitmen dari lembaga penegak hukum (Polri, Kejaksaan, dan Mahkamah Agung) untuk menyelenggarakan pelatihan forensik digital dan sertifikasi khusus hukum siber bagi para penyidik, jaksa, dan hakim secara merata hingga ke tingkat daerah. Hal ini krusial demi memangkas kesenjangan

pemahaman teknologi (*knowledge gap*) antara aparat dan pelaku kejahatan siber yang semakin *tech-savvy*.

DAFTAR REFERENSI

Aditya, Z. F., & Al-Fatih, S. (2021). Perlindungan Hukum terhadap Korban Kejahatan Siber (*Cybercrime*) dalam Sistem Peradilan Pidana Indonesia. *Jurnal Hukum Pembangunan*, 51(3), 612-628.

Fajriansyah, A., Siregar, R. A., & Panggabean, M. L. (2025). *Reformasi Hukum Pidana di Era Digital: Analisis terhadap KUHP Baru*. Jurnal Hukum Mimbar Justitia, 11(1).

Flora, H. S., Rinaldi, K., Mudjrimin, J., dkk. (2024). Hukum Pidana di Era Digital**.** Batam: Rey Media Grafika.

Kiki, & Baihaki, R. (2025). Tindak Pidana Siber di Indonesia: Regulasi, Tantangan, dan Penegakan Hukum**.** Medan: PT Media Penerbit Indonesia.

Prakoso, A. B. (2022). Karakteristik Bukti Digital dan Problematika *Chain of Custody* dalam Hukum Acara Pidana Indonesia. *Jurnal Konstitusi*, 19(4), 810-832.

Sitompul, J. (2021). Rekonstruksi Asas Teritorialitas Hukum Pidana Indonesia Menghadapi Karakteristik Kejahatan Siber Lintas Batas. *Jurnal Legislasi Indonesia*, 18(2), 145-159.

Wahyudi, S. (2023). Pertanggungjawaban Pidana (*Criminal Liability*) Berbasis Kecerdasan Buatan: Sebuah Tantangan Dogmatika Hukum Pidana Masa Depan. *Jurnal Ius Quia Iustum*, 30(1), 89-112.