Indonesian Journal of Law and Economics Review
Vol. 21 No. 4 (2026): November
DOI: 10.21070/ijler.v21i4.1655

ISSN 2598-9928 (online), https://ijler.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Indonesian Journal of Law and Economics Review
Vol. 21 No. 4 (2026): November
DOI: 10.21070/ijler.v21i4.1655

Table Of Contents

Indonesian Journal of Law and Economics Review
Vol. 21 No. 4 (2026): November
DOI: 10.21070/ijler.v21i4.1655

Originality Statement

The author[s] declare that this article is their own work and to the best of their knowledge it contains no materials previously published or written by another person, or substantial proportions of material which have been accepted for the published of any other published materials, except where due acknowledgement is made in the article. Any contribution made to the research by others, with whom author[s] have work, is explicitly acknowledged in the article.

Conflict of Interest Statement

The author[s] declare that this article was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Copyright Statement

Indonesian Journal of Law and Economics Review
Vol. 21 No. 4 (2026): November
DOI: 10.21070/ijler.v21i4.1655

EDITORIAL TEAM

Indonesian Journal of Law and Economics Review

Vol. 21 No. 4 (2026): November
DOI: 10.21070/ijler.v21i4.1655

Article information

Check this article update (crossmark)

Check this article impact (*)

Save this article to Mendeley

(*) Time for indexing process is various, depends on indexing database platform

Indonesian Journal of Law and Economics Review
Vol. 21 No. 4 (2026): November
DOI: 10.21070/ijler.v21i4.1655

Cybercrime Enforcement Remains Fragmented Despite Electronic Evidence Reform: Penegakan Hukum Kejahatan Siber Masih Terpecah-pecah Meskipun Telah Dilakukan Reformasi Bukti Elektronik

Amelia Firdausa Duana, duanaamelia047@gmail.com (*)
Program Studi Ilmu Hukum, Universitas Wahid Hasyim, Indonesia

Adityo Putro Prakoso, adityopp@unwahas.ac.id
Program Studi Ilmu Hukum, Universitas Wahid Hasyim, Indonesia

(*) Corresponding author

Abstract

General Background: Blockchain is reshaping transactions, ownership, verification, smart contracts, tokenization, and digital governance, creating new legal objects for Islamic jurisprudence. **Specific Background:** In fiqh al-nawāzil, these configurations cannotbe reduced to cryptocurrencies or productcompliancebecause their legal character varies with architecture, functions, actors, rights, risks, and governance. **Knowledge Gap:** Empirical integration between technical knowledge, taḥqīq al-manāṭ, uṣūl al-fiqh, maqāṣid, and maʾālāt remains limited, while product-centred reasoning does not adequately capture system-level characteristics and consequences. **Aims:** This qualitative multi-stakeholder case study examined 28 informants through semi-structured interviews, legal vignettes, and documentary analysis to reconstruct digital ijtihād for blockchain-related cases. **Results:** Blockchain emerged as a multidimensional nāzilah; taḥqīq al-manāṭ functioned as the epistemic gateway linking technical reality with legal characterization; reasoning shifted from product-based classification toward systemic analysis and from post-hoc maqāṣid justification toward maṣlaḥah–mafsadah and consequenceassessment. **Novelty:** Thestudy formulates Substantive Digital Fiqh al-Nawāzil Theory, sequencing taṣawwur al-nāzilah, taḥqīq al-manāṭ, taʿyīn al-waṣf al-muʾaṡṡir, uṣūlī reasoning, maqāṣid evaluation, maṣlaḥah–mafsadah, maʾālāt al-afʿāl, legal determination, Shariah governance, and continuous monitoring. **Implications:** The framework supports object-first, systemic, consequence-sensitive, and multidisciplinary digital ijtihād for fatwas and Shariah governance.

Highlights:

- Taḥqīq al-manāṭ linked technical facts with istinbāṭ al-ḥukm.
- Systemic legal characterization replaced product-centred classification across complex
- cases. Maqāṣid shifted toward maṣlaḥah–mafsadah and consequence-sensitive evaluation.

Keywords: Artificial Intelligence, Criminal Law, Cybercrime, Digital Evidence, Law Enforcement

Published date: 2026-09-25

Vol. 21 No. 4 (2026): November
DOI: 10.21070/ijler.v21i4.1655

Pendahuluan

Transformasi digital telah memperluas ruang aktivitas masyarakat Indonesia sekaligus memperbesar permukaan risiko kejahatan. Survei APJII 2026 menunjukkan penetrasi internet nasional mencapai 81,72% atau sekitar 235 juta pengguna, sehingga transaksi, komunikasi, penyimpanan data, layanan publik, dan aktivitas ekonomi semakin bergantung pada sistem digital [1]. Tingkat konektivitas yang tinggi meningkatkan manfaat sosial dan ekonomi, tetapi juga membuat lebih banyak individu dan institusi terpapar penipuan, pencurian data, peretasan, pemerasan digital, dan serangan terhadap sistem elektronik. Kondisi tersebut menempatkan cybercrime sebagai persoalan hukum pidana yang terkait langsung dengan keamanan masyarakat dan keandalan ekosistem digital.

Dampak ekonomi cybercrime juga semakin nyata. Kementerian Komunikasi dan Digital pada Juli 2026 menyebut kerugian akibat scam dan spam digital di Indonesia telah mencapai sekitar Rp7,5 triliun berdasarkan laporan Global Anti-Scam Alliance [2]. Modus penipuan kini memanfaatkan panggilan, pesan, tautan palsu, penyamaran identitas, dan teknologi kecerdasan artifisial untuk meniru suara atau karakter pihak yang dipercaya korban. Perkembangan ini memperlihatkan bahwa penegakan hukum tidak cukup berfokus pada serangan teknis terhadap komputer, karena pelaku juga mengeksploitasi perilaku pengguna dan arsitektur layanan digital.

Secara konseptual, cybercrime dapat dipahami sebagai kelompok perbuatan pidana yang memiliki hubungan substansial dengan komputer, jaringan, data, dan sistem elektronik [3]. Teknologi dapat menjadi sasaran kejahatan, misalnya akses tanpa hak atau gangguan terhadap sistem, dapat menjadi sarana kejahatan seperti penipuan daring dan pemerasan, atau menjadi lingkungan terjadinya perbuatan seperti penguntitan digital dan penyebaran konten manipulatif. Karakter tanpa batas geografis, kecepatan penyebaran, skalabilitas serangan, penggunaan identitas semu, serta ketergantungan pada jejak elektronik membedakan penanganan cybercrime dari banyak kejahatan konvensional. Kajian mengenai keamanan ruang siber Indonesia juga menempatkan koordinasi kelembagaan dan kerja sama lintas negara sebagai unsur penting dalam respons negara [4].

Kebijakan hukum pidana harus menyesuaikan perubahan tersebut tanpa meninggalkan asas legalitas. Pembaruan norma diperlukan ketika modus baru menghasilkan kerugian yang belum tertangani dengan memadai, tetapi kriminalisasi harus tetap dirumuskan secara jelas, terukur, dan proporsional. Kajian kebijakan hukum pidana Indonesia menekankan perlunya pembaruan yang adaptif, peningkatan kapasitas aparat, kerja sama internasional, dan pendidikan masyarakat untuk menghadapi intensitas cybercrime yang terus berubah [5], [6]. Dengan demikian, efektivitas penanggulangan tidak hanya diukur dari banyaknya ancaman pidana, tetapi juga dari ketepatan norma, kualitas pembuktian, dan kemampuan negara mencegah serta memulihkan kerugian.

Kerangka hukum Indonesia saat ini tersebar dalam beberapa rezim. Undang-Undang Nomor 1 Tahun 2024 sebagai perubahan kedua atas Undang-Undang Informasi dan Transaksi Elektronik tetap menjadi instrumen penting untuk perbuatan yang berkaitan langsung dengan sistem dan informasi elektronik. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi mengatur hak subjek data, kewajiban pengendali dan prosesor, larangan tertentu, serta sanksi terhadap penyalahgunaan data. Undang-Undang Nomor 1 Tahun 2023 tentang KUHP mulai berlaku pada 2 Januari 2026 dan berinteraksi dengan ketentuan pidana khusus dalam UU ITE, sehingga penegak hukum perlu menentukan norma yang tepat berdasarkan unsur konkret setiap perbuatan. Analisis mengenai cybercrime dalam KUHP Nasional menunjukkan perlunya pembacaan sistematis terhadap hubungan antara KUHP dan UU ITE agar tidak terjadi tumpang tindih atau kekosongan penerapan.

Pembaruan yang sangat penting juga terjadi pada hukum acara pidana. Undang-Undang Nomor 20 Tahun 2025 tentang KUHAP berlaku sejak 2 Januari 2026 dan menggantikan Undang-Undang Nomor 8 Tahun 1981. KUHAP baru secara tegas memasukkan bukti elektronik ke dalam jenis alat bukti, sehingga posisi formal bukti digital tidak lagi hanya bergantung pada perluasan melalui undang-undang sektoral. Perubahan tersebut relevan bagi perkara cybercrime karena sebagian besar hubungan antara pelaku, korban, perangkat, akun, transaksi, dan akibat tindak pidana direkonstruksi melalui data elektronik. Namun, pengakuan formal belum otomatis menyelesaikan persoalan teknis mengenai perolehan, autentikasi, integritas, penyimpanan, dan penilaian bukti.

Literatur sebelum berlakunya KUHAP baru telah menunjukkan kelemahan tata kelola bukti digital. Penelitian mengenai akuisisi dan penyajian bukti digital menegaskan bahwa karakter data elektronik menuntut metode pengamanan dan evaluasi yang berbeda dari bukti fisik biasa. Kajian forensik komputer juga menunjukkan bahwa keaslian dokumen elektronik perlu dibangun melalui proses teknis yang dapat menjelaskan sumber, integritas, dan perubahan data [7], [8]. Penelitian mengenai ius constituendum alat bukti elektronik sebelumnya menyoroti fragmentasi aturan pembuktian antara KUHAP lama dan berbagai undang-undang khusus [9]. Setelah reformasi 2025, persoalan bergeser dari sekadar pengakuan formal menuju konsistensi prosedur dan kualitas tata kelola bukti digital.

Kajian terbaru pada 2026 memperlihatkan bahwa pengakuan bukti elektronik dalam KUHAP baru masih menyisakan persoalan arsitektur pembuktian. Samudra, Basu, dan Sáenz Pérez menilai kerangka Indonesia masih terfragmentasi dan belum cukup rinci mengenai pengumpulan, autentikasi, penanganan, preservasi, dan evaluasi bukti elektronik [10]. Temuan ini penting karena bukti digital mudah disalin, diubah, dihapus, disinkronkan lintas perangkat, atau disimpan pada infrastruktur cloud di luar yurisdiksi penyidik. Artinya, reformasi prosedural harus diikuti standar operasional dan mekanisme audit yang dapat diuji di pengadilan.

Perkembangan artificial intelligence menambah lapisan persoalan. Generative AI dapat membantu pelaku membuat pesan phishing yang lebih meyakinkan, meniru suara, menghasilkan identitas palsu, mengotomasi percakapan penipuan, dan

Vol. 21 No. 4 (2026): November
DOI: 10.21070/ijler.v21i4.1655

membuat deepfake. Kajian hukum Indonesia menunjukkan bahwa social engineering berbasis generative AI menimbulkan persoalan atribusi pertanggungjawaban dan standar pembuktian, sementara penyalahgunaan deepfake juga dapat menimbulkan pelanggaran privasi yang tidak selalu cocok dimasukkan ke dalam satu rumusan pidana yang sama [11], [12]. Karena itu, penegakan hukum harus menilai perbuatan, niat, metode, kerugian, dan objek hukum yang dilanggar, bukan sekadar penggunaan teknologi AI itu sendiri.

Penelitian terdahulu cenderung membahas cybercrime dari sudut yang terpisah, yaitu kebijakan kriminal, keamanan siber, pembuktian elektronik, perlindungan data, atau penyalahgunaan AI. Kesenjangan analitis muncul setelah KUHP Nasional dan KUHAP baru berlaku bersamaan pada 2026 karena penegakan cybercrime kini harus membaca hukum pidana materiil, hukum acara pidana, hukum teknologi, dan perlindungan data dalam satu kerangka. Pembaruan hukum pidana nasional juga perlu dinilai dari hubungannya dengan demokratisasi, kepastian hukum, dan perlindungan hak agar perluasan kriminalisasi tetap terukur [13]. Penelitian ini mengisi kesenjangan tersebut dengan menghubungkan karakter cybercrime, bentuk perbuatan, pertanggungjawaban pidana, tata kelola bukti digital, koordinasi kelembagaan, dan strategi penal serta non-penal. Tujuan penelitian adalah menganalisis cybercrime sebagai bentuk kejahatan modern, memetakan bentuk perbuatan dan kerangka hukumnya, mengidentifikasi tantangan penegakan hukum di Indonesia, serta merumuskan arah penguatan kebijakan hukum pidana yang relevan setelah reformasi hukum pidana 2026.

Metode

Penelitian ini menggunakan penelitian hukum normatif dengan sifat deskriptif-analitis. Penelitian berfokus pada norma, asas, konsep, dan konstruksi hukum yang mengatur cybercrime, pertanggungjawaban pidana, bukti elektronik, perlindungan data pribadi, serta penegakan hukum di ruang digital. Karena penelitian bersifat normatif, penelitian tidak menggunakan populasi dan sampel responden. Unit analisis berupa bahan hukum primer dan bahan hukum sekunder yang dipilih berdasarkan keterkaitan langsung dengan empat fokus penelitian.

Pendekatan penelitian terdiri atas pendekatan perundang-undangan, pendekatan konseptual, dan pendekatan kasus. Pendekatan perundang-undangan digunakan untuk menelaah Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Nomor 1 Tahun 2023 tentang KUHP, Undang-Undang Nomor 20 Tahun 2025 tentang KUHAP, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahan terakhir melalui Undang-Undang Nomor 1 Tahun 2024, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, dan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Pendekatan konseptual digunakan untuk membahas ontologi cybercrime, pertanggungjawaban pidana, yurisdiksi, bukti elektronik, digital forensics, chain of custody, kebijakan penal, dan kebijakan non-penal. Pendekatan kasus digunakan untuk menganalisis Putusan PN Surabaya Nomor 2574/Pid.Sus/2022/PN Sby mengenai akses tanpa hak dengan tujuan memperoleh informasi elektronik dan Putusan PN Jakarta Selatan Nomor 616/Pid.Sus/2023/PN JKT.SEL mengenai distribusi konten elektronik yang melanggar kesusilaan. Kedua putusan dipilih secara purposif karena memperlihatkan dua persoalan yang menjadi fokus penelitian, yaitu penerapan unsur tindak pidana siber dan penggunaan bukti elektronik dalam pembuktian.

Bahan hukum primer meliputi peraturan perundang-undangan yang telah disebutkan dan dua putusan pengadilan terpilih. Bahan hukum sekunder diprioritaskan pada artikel ilmiah terbitan 2022-2026 agar pembahasan mencerminkan kondisi regulasi dan teknologi yang mutakhir. Artikel ditelusuri melalui SciSpace dan portal jurnal penerbit dengan kombinasi istilah pencarian dalam bahasa Indonesia dan Inggris yang mencakup cybercrime Indonesia, electronic evidence, digital forensics, cybercrime regulation, artificial intelligence, deepfake, dan institutional coordination. Metadata, tahun publikasi, dan DOI diverifikasi melalui laman penerbit dan resolver DOI. Literatur dimasukkan apabila bersifat ilmiah, relevan langsung dengan fokus penelitian, dan memiliki metadata yang dapat ditelusuri. Publikasi duplikat, sumber tanpa keterkaitan langsung, serta metadata yang tidak dapat diverifikasi dikeluarkan. Sumber resmi APJII dan Kementerian Komunikasi dan Digital digunakan secara terbatas untuk memberikan konteks faktual mengenai skala penggunaan internet dan perkembangan penipuan digital.

Pengumpulan bahan hukum dilakukan melalui studi kepustakaan dengan teknik inventarisasi, verifikasi, klasifikasi, dan pencatatan. Instrumen penelitian berupa matriks inventarisasi dan analisis bahan hukum. Matriks memuat identitas sumber, jenis bahan hukum, isu hukum, norma atau pertimbangan yang relevan, konsep utama, posisi bukti elektronik, keterkaitan dengan pertanyaan penelitian, serta catatan analitis. Tahap inventarisasi memetakan norma berdasarkan jenis perbuatan, subjek hukum, objek perlindungan, dan kewenangan penegak hukum. Tahap verifikasi memeriksa status berlaku peraturan, identitas putusan, dan metadata publikasi. Tahap klasifikasi memisahkan persoalan hukum materiil, hukum acara, kelembagaan, teknis forensik, dan pencegahan. Penggunaan matriks menjaga konsistensi perbandingan antarsumber dan membuat alur seleksi bahan hukum dapat ditelusuri kembali.

Analisis dilakukan secara kualitatif dengan penafsiran gramatikal dan sistematis. Penafsiran gramatikal digunakan untuk membaca unsur norma, sedangkan penafsiran sistematis digunakan untuk menilai hubungan KUHP, KUHAP, UU ITE, UU Pelindungan Data Pribadi, dan aturan sistem elektronik. Pada pendekatan kasus, fakta hukum, konstruksi pasal, alat bukti, amar putusan, dan relevansi pertimbangan hakim dibandingkan dengan kerangka normatif yang berlaku. Analisis juga menerapkan prinsip legalitas, kesalahan, proporsionalitas, due process of law, dan perlindungan hak sebagai parameter normatif. Hasil analisis disusun secara deduktif untuk menjawab hubungan antara perkembangan modus cybercrime dan kapasitas sistem hukum Indonesia dalam menentukan perbuatan pidana, membuktikan keterlibatan pelaku, dan menjatuhkan konsekuensi hukum yang dapat dipertanggungjawabkan.

ISSN 2598-9928 (online), https://ijler.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Indonesian Journal of Law and Economics Review
Vol. 21 No. 4 (2026): November
DOI: 10.21070/ijler.v21i4.1655

Hasil dan Pembahasan

A. Cybercrime sebagai bentuk kejahatan modern dan karakteristik pertanggungjawaban pidana

Secara ontologis, cybercrime bukan satu jenis tindak pidana yang memiliki unsur tunggal, melainkan kategori yang menunjuk pada perbuatan manusia ketika teknologi digital mempunyai hubungan substantif dengan objek, sarana, atau ruang terjadinya perbuatan. Objek materialnya dapat berupa tindakan terhadap data, sistem elektronik, identitas digital, harta, privasi, atau kepentingan hukum lain yang direpresentasikan dan diproses secara digital. Objek formalnya terletak pada penilaian hukum terhadap sifat tanpa hak atau melawan hukum, kesalahan, hubungan kausal, kerugian, serta pertanggungjawaban pelaku. Phillips et al. menunjukkan bahwa belum terdapat satu definisi universal cybercrime dan bahwa klasifikasi yang berguna harus mampu membedakan relasi teknologi dengan perbuatan serta objek yang diserang [14]. Kerangka ontologis ini penting agar istilah cybercrime tidak diperlakukan sebagai delik mandiri, melainkan selalu dikembalikan pada unsur pasal yang konkret.

Pada tataran konseptual, cybercrime dapat dibedakan antara cyber-dependent crime, yaitu perbuatan yang keberadaannya bergantung pada sistem digital, dan cyber-enabled crime, yaitu kejahatan yang telah dikenal tetapi skala, kecepatan, atau jangkauannya diperbesar oleh teknologi. Lusthaus menekankan bahwa cybercrime lebih tepat dipahami sebagai kejahatan yang menggunakan teknologi digital secara signifikan [15]. Model ontologis digital crime juga dapat menghubungkan jenis perbuatan, bukti digital, dan pertanggungjawaban pidana secara sistematis [16]. Dalam penelitian ini, posisi teknologi dianalisis melalui tiga relasi, yaitu sebagai sasaran, sebagai sarana, atau sebagai lingkungan terjadinya perbuatan. Pembedaan tersebut menentukan norma materiil, bentuk kesalahan, jenis bukti, dan subjek yang dapat dimintai pertanggungjawaban.

Karakter pertama cybercrime adalah skalabilitas. Seorang pelaku dapat mengirim ribuan pesan, membuat banyak akun, atau menjalankan perangkat lunak otomatis dalam waktu singkat sehingga jumlah calon korban meningkat tanpa kenaikan biaya yang sebanding. Skala tersebut membuat kerugian kumulatif dapat jauh lebih besar daripada kejahatan konvensional yang membutuhkan kontak fisik satu per satu. Sistem otomatis juga memungkinkan serangan berjalan terus saat pelaku tidak aktif secara langsung. Karena itu, penilaian keseriusan perkara perlu memperhitungkan skala, jumlah korban, nilai kerugian, dan dampak terhadap sistem, bukan hanya satu transaksi yang terlihat dalam laporan awal.

Karakter kedua adalah penggunaan identitas digital yang tidak selalu sama dengan identitas hukum. Nama pengguna, alamat surat elektronik, nomor telepon, alamat IP, akun media sosial, perangkat, atau dompet digital hanya merupakan titik awal atribusi. Semua indikator tersebut dapat dipinjam, dijual, diretas, dipalsukan, dialihkan, atau digunakan melalui jaringan perantara. Pertanggungjawaban pidana tetap mensyaratkan pembuktian hubungan antara subjek hukum dengan perbuatan dan keadaan batin yang dipersyaratkan oleh delik. Penetapan tersangka tidak seharusnya hanya didasarkan pada kepemilikan akun atau perangkat tanpa rangkaian bukti yang menunjukkan siapa yang mengendalikan aktivitas pada waktu relevan.

Karakter ketiga adalah sifat lintas batas. Pelaku, korban, server, penyedia platform, rekening penerima, dan penyimpanan data dapat berada pada yurisdiksi yang berbeda. Keadaan ini menimbulkan masalah kewenangan penyidikan, kecepatan permintaan data, retensi log, perbedaan standar privasi, dan pelaksanaan permintaan bantuan hukum. Kerja sama bilateral dan multilateral menjadi penting karena risiko digital tidak berhenti pada batas negara. Dalam hukum pidana, kerja sama tersebut tetap harus mengikuti dasar kewenangan yang sah agar data yang diperoleh dapat dipertanggungjawabkan dalam proses peradilan.

Karakter keempat adalah volatilitas bukti. Data digital dapat berubah karena sinkronisasi otomatis, pembaruan aplikasi, penghapusan jarak jauh, rotasi log, atau tindakan pengguna. Satu salinan tangkapan layar dapat memberi petunjuk awal, tetapi tidak selalu cukup membuktikan autentisitas, sumber, konteks, atau integritas data. Akuisisi dan penyajian bukti digital karena itu perlu memperhatikan cara bukti diperoleh, disimpan, diverifikasi, dan dinilai agar hakim dapat menguji keabsahannya. Pencatatan proses penyitaan, pencitraan forensik, nilai hash, waktu akuisisi, perangkat yang digunakan, petugas yang menangani, dan setiap perpindahan penguasaan mempunyai arti penting dalam menjaga reliabilitas.

Karakter kelima adalah kecepatan perubahan modus. Pelaku dapat berpindah platform, mengganti domain, memanfaatkan layanan cloud, menggunakan enkripsi, atau mengotomasi interaksi dengan korban dalam waktu singkat. Generative AI mempercepat perubahan ini karena dapat menghasilkan pesan yang disesuaikan dengan profil korban, meniru karakter komunikasi, dan membuat konten visual atau suara yang meyakinkan. Perubahan tersebut memperbesar kesulitan pada standar bukti dan atribusi pertanggungjawaban. Artinya, hukum pidana harus cukup teknologi-netral untuk bertahan terhadap perubahan alat, tetapi rumusan delik tetap harus jelas agar tidak menimbulkan perluasan pidana tanpa batas.

Pertanggungjawaban pidana dalam cybercrime tetap mengikuti prinsip dasar hukum pidana. Aparat harus membuktikan perbuatan yang memenuhi unsur delik, hubungan pelaku dengan perbuatan, bentuk kesalahan yang disyaratkan, serta tidak adanya alasan pembenar atau pemaaf yang relevan. Teknologi tidak menghapus kebutuhan tersebut. Dalam perkara akses ilegal, misalnya, fakta bahwa sistem berhasil dimasuki belum otomatis menjawab siapa yang melakukan, apakah akses dilakukan tanpa hak, apa tujuan dan pengetahuan pelaku, serta apakah data yang disajikan berasal dari aktivitas yang sama. Oleh karena itu, analisis teknis dan analisis yuridis harus bergerak bersama.

Pertanggungjawaban juga dapat menjadi lebih kompleks ketika tindak pidana melibatkan beberapa aktor. Satu pihak dapat membuat infrastruktur, pihak lain memperoleh data korban, pihak lain mengirim pesan, dan pihak berikutnya menerima atau memindahkan hasil kejahatan. Generative AI bahkan memungkinkan sebagian tindakan dilakukan oleh sistem otomatis yang dikonfigurasi manusia. Pembuktian perlu memetakan kontribusi tiap pihak dan tidak menyamakan penggunaan

Vol. 21 No. 4 (2026): November
DOI: 10.21070/ijler.v21i4.1655

teknologi dengan kepemilikan niat pidana. Kajian reformulasi cybercrime berbasis AI mengingatkan bahwa struktur pertanggungjawaban perlu menjawab risiko penggunaan AI tanpa mengorbankan kepastian hukum [17].

Temuan utama subbagian ini adalah bahwa persoalan cybercrime tidak cukup dijelaskan melalui klasifikasi jenis kejahatan. Dibandingkan literatur yang terutama memetakan definisi, tipologi, atau risiko teknologi, penelitian ini menunjukkan bahwa titik penentu pertanggungjawaban berada pada keselarasan antara posisi teknologi dalam perbuatan, atribusi subjek, unsur kesalahan, dan rantai bukti digital. Kerangka ini menghubungkan ontologi cybercrime langsung dengan kebutuhan pembuktian pidana.

B. Bentuk-bentuk cybercrime dan kerangka hukum pidana Indonesia

Bentuk pertama adalah akses tanpa hak terhadap komputer atau sistem elektronik. Pasal 30 ayat (1) UU ITE melarang akses tanpa hak terhadap komputer atau sistem elektronik milik orang lain. Ayat (2) menambahkan tujuan memperoleh Informasi Elektronik atau Dokumen Elektronik, sedangkan ayat (3) mencakup akses dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan. Sanksinya diatur secara berjenjang dalam Pasal 46. Penerapan pasal karena itu harus membuktikan bentuk akses, tujuan, sifat tanpa hak, serta hubungan pelaku dengan aktivitas digital yang terjadi, bukan sekadar menunjukkan bahwa suatu akun atau sistem pernah diakses.

Bentuk kedua mencakup gangguan terhadap data atau sistem melalui malware dan ransomware. Pasal 32 jo. Pasal 48 UU ITE relevan ketika pelaku tanpa hak mengubah, merusak, menghilangkan, memindahkan, atau menyembunyikan Informasi Elektronik atau Dokumen Elektronik milik orang lain. Pasal 33 jo. Pasal 49 berlaku ketika perbuatan tanpa hak menyebabkan sistem elektronik terganggu atau tidak bekerja sebagaimana mestinya. Ransomware dapat sekaligus memuat akses tanpa hak, gangguan data, dan tuntutan pembayaran. Karena itu, konstruksi pidana harus bertumpu pada perbuatan dan akibat yang terbukti, bukan pada nama perangkat lunak yang digunakan.

Bentuk ketiga adalah phishing dan social engineering. Pelaku merekayasa komunikasi agar korban menyerahkan kredensial, kode verifikasi, data pribadi, atau uang. Pasal 30 UU ITE dapat diterapkan apabila kredensial kemudian digunakan untuk mengakses sistem tanpa hak. Pasal 65 UU Pelindungan Data Pribadi relevan terhadap perolehan, pengungkapan, atau penggunaan data pribadi secara melawan hukum. Pasal 35 jo. Pasal 51 ayat (1) UU ITE dapat diuji jika terdapat manipulasi data agar tampak autentik. AI memperbesar risiko karena pesan, suara, atau identitas palsu dapat dibuat lebih meyakinkan, tetapi penerapan pidana tetap bergantung pada unsur konkret yang terbukti.

Bentuk keempat adalah penipuan daring melalui perdagangan elektronik, media sosial, aplikasi pesan, investasi palsu, lowongan kerja, atau layanan keuangan. Karakter digital memperluas jangkauan pelaku dan mempersulit korban memverifikasi identitas lawan transaksi. Penegakan hukum perlu merekonstruksi representasi palsu, hubungan kausal dengan penyerahan uang atau data, serta aliran hasil kejahatan. Rekening penampung, dompet elektronik, riwayat percakapan, metadata transaksi, dan data perangkat dapat saling menguatkan. Namun, keberadaan transaksi ke suatu rekening saja belum otomatis membuktikan bahwa pemilik rekening adalah pengendali utama skema.

Bentuk kelima adalah pencurian identitas dan penyalahgunaan data pribadi. Pasal 65 UU Pelindungan Data Pribadi melarang perolehan atau pengumpulan, pengungkapan, dan penggunaan data pribadi milik orang lain secara melawan hukum, dengan sanksi pada Pasal 67. Pasal 66 melarang pembuatan atau pemalsuan data pribadi untuk memperoleh keuntungan yang dapat menimbulkan kerugian, dan Pasal 68 mengatur sanksinya. Tantangan implementasi tetap berkaitan dengan koordinasi kelembagaan, kapasitas keamanan siber, dan efektivitas perlindungan subjek data [18]. Karena itu, istilah pencurian identitas harus diterjemahkan ke dalam tindakan yang sesuai dengan unsur pasal, bukan diperlakukan sebagai label pidana yang berdiri sendiri.

Bentuk keenam adalah pemerasan digital. Pelaku dapat mengancam akan menyebarkan data, foto, rekaman, dokumen, atau materi manipulatif apabila korban tidak memberikan uang atau keuntungan lain. Unsur pemerasan perlu dibedakan dari sekadar ancaman atau perselisihan digital. Ketika materi diperoleh melalui peretasan, perkara juga dapat mengandung pelanggaran terhadap sistem elektronik atau data pribadi. Pendekatan berbasis perbuatan memungkinkan penegak hukum menggunakan norma yang tepat tanpa menciptakan istilah kejahatan baru yang tidak memiliki unsur jelas.

Bentuk ketujuh adalah cyberstalking dan cyberbullying. Kedua istilah sering digunakan sebagai kategori sosial, tetapi tidak setiap tindakan yang disebut stalking atau bullying otomatis memenuhi unsur tindak pidana. Penilaian harus melihat bentuk ancaman, pelecehan, penguntitan, penyebaran informasi, intensitas tindakan, konteks, dan akibat yang ditentukan undang-undang. Pemisahan antara kategori sosial dan rumusan delik penting untuk menjaga asas legalitas. Jika suatu tindakan tidak memenuhi unsur pidana, mekanisme platform, perlindungan perdata, administratif, atau pencegahan dapat tetap relevan.

Bentuk kedelapan adalah deepfake dan manipulasi konten berbasis AI. Deepfake dapat digunakan untuk penipuan finansial, pencemaran reputasi, pornografi non-konsensual, manipulasi identitas, atau penyebaran informasi palsu. Teknologinya sendiri tidak bersifat terlarang. Pasal 35 jo. Pasal 51 ayat (1) UU ITE dapat relevan apabila terdapat manipulasi, penciptaan, perubahan, penghilangan, atau pengrusakan Informasi Elektronik atau Dokumen Elektronik dengan tujuan agar tampak autentik. Penilaian tetap harus memeriksa tujuan, objek, akibat, dan kesalahan. Literatur menunjukkan bahwa kekosongan definisi teknis, ketidakjelasan konstruksi pidana, dan kesulitan pembuktian masih mengurangi kepastian hukum [19], [20].

Masalah kriminalisasi deepfake menjadi lebih tajam ketika perbuatan sulit dimasukkan ke dalam kategori lama. Ketiadaan definisi teknis, kelemahan standar pembuktian forensik, dan keterbatasan kapasitas aparat menunjukkan bahwa respons hukum tidak cukup hanya mengandalkan penamaan teknologi. Kondisi tersebut tidak berarti setiap deepfake memerlukan delik baru. Pembentuk kebijakan perlu terlebih dahulu memetakan kerugian yang belum terlindungi, menilai kecukupan

ISSN 2598-9928 (online), https://ijler.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Vol. 21 No. 4 (2026): November
DOI: 10.21070/ijler.v21i4.1655

norma yang ada, dan memastikan rumusan baru tidak mengkriminalisasi ekspresi atau penggunaan AI yang sah. Prinsip lex certa tetap menjadi batas dalam pembaruan hukum.

Hubungan antara KUHP Nasional dan UU ITE membutuhkan perhatian khusus. KUHP berfungsi sebagai hukum pidana umum, sedangkan UU ITE memuat sejumlah ketentuan khusus yang berkaitan dengan sistem dan informasi elektronik. Keduanya perlu dibaca secara harmonis ketika suatu rangkaian tindakan memenuhi unsur dari lebih dari satu ketentuan. Dalam praktik, pilihan pasal harus ditentukan oleh unsur perbuatan, waktu kejadian, objek yang dilindungi, aturan khusus yang berlaku, dan prinsip hubungan antara ketentuan umum serta khusus. Pendekatan ini mencegah duplikasi penuntutan yang tidak perlu sekaligus menghindari kekosongan perlindungan.

UU Pelindungan Data Pribadi menambah lapisan penting karena banyak serangan siber menjadikan data sebagai komoditas, alat penipuan, atau sarana pengambilalihan identitas. Pencegahan juga menjadi kewajiban penyelenggara sistem. Pasal 3 ayat (1) PP Nomor 71 Tahun 2019 mewajibkan sistem diselenggarakan secara andal dan aman, sedangkan Pasal 4 menekankan perlindungan atas ketersediaan, keutuhan, keautentikan, kerahasiaan, dan keteraksesan Informasi Elektronik. Kewajiban ini harus dibedakan dari pertanggungjawaban pidana pelaku serangan. Tidak setiap insiden keamanan merupakan tindak pidana, sehingga penegakan perlu memisahkan pelanggaran administratif, kelalaian yang relevan, dan perbuatan pidana yang memenuhi unsur.

Kerangka hukum cybercrime Indonesia karena itu bersifat multi-rezim. KUHP, KUHAP, UU ITE, UU Pelindungan Data Pribadi, dan peraturan sistem elektronik membentuk lapisan yang berbeda tetapi saling berhubungan. Hermanto, Nur, dan Zulfa menekankan bahwa hukum siber Indonesia perlu dibenahi secara komprehensif agar pengaturan mengikuti perkembangan teknologi dan putusan konstitusional [21]. Tantangan utamanya bukan sekadar menambah aturan, melainkan memastikan batas antaraturan, unsur tindak pidana, kewenangan, prosedur pembuktian, dan perlindungan hak dapat diterapkan secara konsisten.

Temuan baru pada subbagian ini adalah bahwa fragmentasi penegakan bukan terutama disebabkan oleh ketiadaan norma. Masalah yang lebih mendasar terletak pada pemetaan fakta yang sama ke beberapa rezim hukum dengan unsur, subjek, dan konsekuensi berbeda. Dibandingkan kajian yang menilai kecukupan satu undang-undang secara terpisah, penelitian ini menempatkan pemilihan norma dan pemetaan unsur sebagai persoalan inti harmonisasi cybercrime di Indonesia.

C. Analisis putusan dalam penegakan hukum cybercrime

Pendekatan kasus dalam penelitian ini digunakan untuk menguji bagaimana konsep dan norma yang dibahas bekerja pada perkara konkret. Dua putusan dipilih secara purposif karena mewakili dua karakter yang berbeda. Putusan PN Surabaya Nomor 2574/Pid.Sus/2022/PN Sby menampilkan cybercrime yang bersifat cyber-dependent melalui akses tanpa hak terhadap sistem elektronik, sedangkan Putusan PN Jakarta Selatan Nomor 616/Pid.Sus/2023/PN JKT.SEL memperlihatkan penggunaan sarana digital untuk mendistribusikan konten elektronik serta persoalan pembuktian dengan jejak digital. Analisis tidak dimaksudkan untuk menggeneralisasi seluruh praktik peradilan, tetapi untuk menilai hubungan antara unsur pasal, atribusi pelaku, dan bukti elektronik.

Dalam Putusan PN Surabaya Nomor 2574/Pid.Sus/2022/PN Sby, pengadilan menyatakan KGS Egi Pratama terbukti secara bersama-sama melakukan akses tanpa hak terhadap komputer dan/atau sistem elektronik dengan tujuan memperoleh Informasi Elektronik dan/atau Dokumen Elektronik. Konstruksi tersebut sesuai dengan karakter Pasal 30 ayat (2) UU ITE jo. Pasal 46 ayat (2). Pengadilan menjatuhkan pidana penjara 10 bulan dan denda Rp15.000.000,00 dengan pidana pengganti apabila denda tidak dibayar [22]. Daftar barang bukti dalam putusan mencakup riwayat transaksi perbankan, perangkat komputer, telepon seluler, serta data akun pada layanan aset digital. Secara analitis, perkara ini menunjukkan bahwa atribusi tidak berhenti pada keberadaan akun atau perangkat. Rangkaian bukti perlu menghubungkan subjek, akses, waktu, transaksi, dan tujuan memperoleh informasi sehingga unsur tanpa hak dan keterlibatan pelaku dapat dinilai secara utuh.

Putusan PN Jakarta Selatan Nomor 616/Pid.Sus/2023/PN JKT.SEL diputus pada 18 Januari 2024 atas perbuatan yang terjadi ketika ketentuan UU ITE sebelum perubahan 2024 masih menjadi dasar perkara. Pengadilan menyatakan Bayu Firlen terbukti melakukan distribusi, transmisi, atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan melanggar kesusilaan berdasarkan Pasal 27 ayat (1) jo. Pasal 45 ayat (1) Undang-Undang Nomor 19 Tahun 2016, dengan pidana penjara 4 tahun dan denda Rp1.000.000.000,00 [23]. Bukti yang digunakan antara lain flashdisk berisi tangkapan layar, telepon seluler dan kartu SIM, data transaksi pelanggan atau anggota, akun dan tautan media sosial, serta video. Kajian Billah dan Saragih terhadap putusan tersebut menegaskan pentingnya kombinasi bukti digital dan bukti konvensional serta persoalan autentikasi dalam penilaian hakim [24]. Perkara ini relevan untuk menunjukkan bahwa bentuk digital bukti tidak menghapus kebutuhan akan konteks, keaslian, dan keterkaitan dengan perbuatan terdakwa.

Perbandingan kedua putusan memperlihatkan dua titik penting. Putusan Surabaya menekankan unsur akses tanpa hak dan atribusi terhadap aktivitas pada sistem, sedangkan Putusan Jakarta Selatan menekankan distribusi konten elektronik serta hubungan antara perangkat, akun, transaksi, dan materi digital. Keduanya diputus sebelum berlakunya KUHAP 2025, tetapi persoalan yang muncul tetap relevan setelah 2 Januari 2026. Pasal 235 ayat (3) sampai ayat (5) KUHAP baru kini memberikan dasar yang lebih tegas untuk menguji autentikasi dan legalitas perolehan alat bukti, sementara Pasal 242 memperjelas ruang lingkup bukti elektronik. Dengan demikian, pendekatan kasus menguatkan temuan normatif bahwa efektivitas penegakan cybercrime bergantung pada kecocokan antara unsur pasal, proses memperoleh bukti, integritas data, dan kemampuan menghubungkan jejak digital dengan subjek hukum.

Vol. 21 No. 4 (2026): November
DOI: 10.21070/ijler.v21i4.1655

Kontribusi analisis kasus ini terletak pada pembacaan dua putusan pra-KUHAP 2025 menggunakan standar prosedural yang berlaku setelah reformasi. Kedua perkara menunjukkan titik yang kini menjadi lebih terukur, yaitu legalitas perolehan bukti, autentikasi, integritas, dan hubungan bukti dengan subjek hukum. Dengan demikian, reformasi KUHAP tidak mengubah unsur tindak pidana pada putusan tersebut, tetapi menaikkan standar pengujian atas kualitas bukti elektronik untuk perkara sejenis pada masa kini.

D. Tantangan penegakan hukum cybercrime di Indonesia

Tantangan pertama adalah atribusi pelaku. Aktivitas digital menghasilkan banyak indikator teknis, tetapi indikator tersebut tidak selalu identik dengan pelaku. Alamat IP dapat dipakai bersama, perangkat dapat dikendalikan jarak jauh, akun dapat diretas, kartu SIM dapat disalahgunakan, dan kredensial dapat berpindah tangan. Penyidik karena itu perlu membangun rangkaian bukti yang menghubungkan akun, perangkat, lokasi, waktu, transaksi, komunikasi, dan perilaku pengguna. Kesalahan atribusi dapat mengancam hak tersangka sekaligus merusak keandalan pembuktian di pengadilan.

Tantangan kedua adalah perolehan bukti dari layanan digital. Data penting sering disimpan oleh penyelenggara sistem elektronik, platform global, penyedia cloud, lembaga keuangan, atau operator telekomunikasi. Nilai pembuktian data dapat hilang jika permintaan terlambat dan data sudah melewati masa retensi. Sebaliknya, permintaan yang terlalu luas dapat melanggar privasi dan prinsip proporsionalitas. Karena itu, prosedur memperoleh data harus memiliki dasar hukum, ruang lingkup yang spesifik, dokumentasi yang jelas, dan mekanisme pengawasan agar kebutuhan penegakan hukum seimbang dengan perlindungan hak.

Tantangan ketiga adalah integritas dan autentisitas bukti elektronik. Monique, Yuliati, dan Sulistio menempatkan digital forensics sebagai unsur penting untuk menjaga dan menguji bukti elektronik dalam proses peradilan pidana Indonesia [25]. Proses pembuktian seharusnya dapat menjawab dari mana data berasal, bagaimana data diperoleh, apakah data berubah, siapa yang menguasai data pada setiap tahap, dan metode apa yang digunakan untuk memeriksanya. Chain of custody perlu diperlakukan sebagai rekam proses yang dapat ditelusuri, bukan sekadar formulir administratif. Ketika tahapan tersebut tidak terdokumentasi, pihak lain sulit menguji reliabilitas dan kemungkinan kontaminasi bukti.

KUHAP baru memperkuat dasar formal bukti elektronik. Pasal 235 ayat (1) huruf f Undang-Undang Nomor 20 Tahun 2025 menempatkan bukti elektronik sebagai alat bukti, sedangkan Pasal 235 ayat (3) sampai ayat (5) menegaskan autentikasi dan perolehan yang sah. Pasal 242 mencakup Informasi Elektronik, Dokumen Elektronik, dan/atau sistem elektronik yang berkaitan dengan tindak pidana. Ketentuan ini perlu dibaca bersama Pasal 5 ayat (1) UU ITE dan Pasal 64 ayat (3) UU Pelindungan Data Pribadi. Dengan demikian, isu utama setelah reformasi bukan lagi pengakuan formal bukti elektronik, tetapi konsistensi autentikasi, legalitas perolehan, chain of custody, dan kualitas pemeriksaan forensik.

Tantangan keempat adalah kualitas dan pemerataan kapasitas digital forensik. Penelitian systematic review mengenai perkembangan forensik digital di Indonesia menunjukkan kebutuhan penguatan metode dan kapasitas untuk mendukung penyidikan cybercrime [26]. Unit penegak hukum di wilayah berbeda dapat memiliki akses yang tidak sama terhadap laboratorium, perangkat, ahli, dan pelatihan. Ketimpangan tersebut berpengaruh pada kecepatan akuisisi, kualitas analisis, dan kemampuan menjelaskan temuan teknis di persidangan. Peningkatan kapasitas perlu mencakup penyidik, jaksa, hakim, dan tenaga ahli agar bahasa teknis dapat diterjemahkan menjadi fakta hukum yang dapat diuji.

Tantangan kelima adalah yurisdiksi dan kerja sama internasional. Ketika penyedia layanan berada di luar negeri, penyidik mungkin membutuhkan saluran kerja sama yang lebih lambat daripada masa retensi data. Perbedaan aturan privasi dan standar permintaan data juga dapat menghambat. Upaya penanggulangan perlu memanfaatkan mekanisme bantuan hukum, kerja sama kepolisian, kontak langsung yang sah dengan penyedia, dan pengembangan standar nasional yang kompatibel dengan praktik internasional. Kecepatan harus tetap disertai akuntabilitas karena bukti yang diperoleh secara tidak sah dapat dipersoalkan dalam proses peradilan.

Tantangan keenam adalah tumpang tindih kelembagaan. Keamanan siber, penegakan hukum, pelindungan data, telekomunikasi, pertahanan, dan keamanan nasional memiliki titik pertemuan tetapi tidak selalu identik. Ananta dan kolega menemukan potensi konflik kewenangan antar lembaga dalam perlindungan terhadap ancaman siber dan menekankan pentingnya pembagian peran serta prosedur koordinasi yang jelas [27]. Dalam perkara pidana, garis kewenangan harus membedakan respons insiden, mitigasi keamanan, penyidikan, intelijen, dan kebijakan regulasi. Koordinasi yang kabur dapat menunda penanganan, menggandakan permintaan data, atau menimbulkan sengketa kewenangan.

Tantangan ketujuh adalah hak atas proses hukum yang adil. Digital evidence dapat sangat persuasif karena terlihat objektif, padahal data tetap membutuhkan konteks, interpretasi, dan metode pengumpulan yang dapat diuji. Stoykova menempatkan equality of arms dan presumption of innocence sebagai kerangka penting dalam pengaturan bukti digital [28]. Terdakwa perlu memiliki kesempatan yang memadai untuk mengetahui sumber bukti, memeriksa metode analisis, dan menguji kesimpulan ahli, sejauh tidak bertentangan dengan perlindungan yang sah. Penegakan cybercrime yang efektif tidak boleh mengorbankan due process karena keandalan putusan bergantung pada prosedur yang dapat dipertanggungjawabkan.

Tantangan kedelapan adalah kejahatan berbasis AI dan deepfake. Konten sintetis membuat pembedaan antara data asli, data yang dimodifikasi, dan data yang sepenuhnya dihasilkan mesin menjadi lebih rumit. Penilaian tidak cukup hanya menggunakan pemeriksaan visual, sebab kualitas manipulasi terus meningkat. Regulasi yang terfragmentasi dapat mempersulit penentuan risiko, akuntabilitas, dan standar pembuktian pada penyalahgunaan AI. Pada level pembuktian, aparat membutuhkan metode verifikasi, provenance data, log proses, alat deteksi yang dapat diuji, serta ahli yang mampu menjelaskan tingkat kepastian tanpa menyatakan hasil teknis sebagai kebenaran absolut.

ISSN 2598-9928 (online), https://ijler.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Vol. 21 No. 4 (2026): November
DOI: 10.21070/ijler.v21i4.1655

Tantangan kesembilan adalah hubungan antara penegakan hukum dan kesadaran masyarakat. Banyak skema penipuan memanfaatkan keputusan korban, misalnya memberikan kode OTP, mengklik tautan, atau mengirim dana setelah menerima komunikasi palsu. Rendahnya pemahaman mengenai verifikasi informasi dan keamanan akun memperbesar peluang keberhasilan serangan. Nono, Janggur, dan Thene menunjukkan bahwa kesadaran hukum digital perlu dikembangkan secara preventif untuk menghadapi disinformasi dan cybercrime [29]. Karena itu, keberhasilan penegakan hukum juga dipengaruhi kemampuan masyarakat mengenali, melaporkan, dan mempertahankan bukti awal ketika menjadi korban.

Kesembilan tantangan tersebut saling berkaitan. Atribusi yang lemah dapat diperparah oleh data yang terlambat diperoleh; data yang lengkap dapat kehilangan nilai jika integritasnya tidak terjaga; laboratorium yang baik dapat tetap tidak efektif jika koordinasi antarinstansi lambat; dan norma yang jelas dapat sulit diterapkan ketika modus AI berkembang lebih cepat dari kapasitas pemeriksaan. Masalah penegakan hukum cybercrime karena itu bersifat sistemik. Solusinya perlu menyentuh aturan materiil, prosedur, kelembagaan, teknologi, sumber daya manusia, dan pencegahan pada saat yang sama.

Temuan penelitian ini berbeda dari pembacaan yang melihat setiap kendala secara terpisah. Hambatan penegakan membentuk rantai ketergantungan: keterlambatan memperoleh data melemahkan atribusi, atribusi yang lemah mengurangi nilai pembuktian, dan bukti yang baik tetap tidak efektif tanpa kapasitas forensik serta koordinasi kelembagaan. Karena itu, perbaikan tunggal pada regulasi atau teknologi tidak cukup apabila mata rantai lain tetap lemah.

E. Upaya penanggulangan cybercrime dalam perspektif kebijakan hukum pidana

Kebijakan penanggulangan cybercrime perlu menggabungkan pendekatan penal dan non-penal. Pendekatan penal berfungsi menentukan perbuatan terlarang, menetapkan pertanggungjawaban, memproses perkara, menjatuhkan sanksi, dan melindungi kepentingan hukum korban. Pendekatan non-penal berfungsi mengurangi peluang kejahatan melalui keamanan sistem, literasi, tata kelola data, desain layanan, dan mitigasi risiko. Kombinasi tersebut perlu disertai peningkatan kapasitas aparat, kerja sama internasional, koordinasi, dan edukasi masyarakat. Pendekatan terpadu lebih sesuai dengan karakter cybercrime yang dapat dicegah sebelum kerugian terjadi.

Pada sisi penal, langkah pertama adalah harmonisasi norma. Aparat penegak hukum membutuhkan pedoman yang menjelaskan hubungan KUHP Nasional, UU ITE, UU Pelindungan Data Pribadi, dan undang-undang sektoral lain ketika satu rangkaian perbuatan memenuhi beberapa ketentuan. Pedoman tidak boleh menggantikan undang-undang, tetapi dapat membantu pemetaan unsur, lex specialis, bentuk kesalahan, subjek hukum, dan sanksi. Kajian kebijakan hukum siber menilai bahwa kekosongan, disharmoni, dan perubahan teknologi menuntut reformasi regulasi yang adaptif sekaligus menjaga keseimbangan antara kebutuhan penegakan hukum dan perlindungan privasi. Tujuannya adalah kepastian penerapan, bukan memperluas kriminalisasi.

Langkah kedua adalah memperkuat tata kelola bukti elektronik setelah KUHAP baru. Pengakuan bukti elektronik harus diikuti standar akuisisi, preservasi, verifikasi, dokumentasi, dan penyajian di persidangan. Standar tersebut sebaiknya mempertimbangkan prinsip forensik yang dapat diaudit, penggunaan hash saat relevan, dokumentasi perangkat dan perangkat lunak, pencatatan chain of custody, serta pemisahan data asli dan salinan kerja. Pedoman nasional yang konsisten akan meningkatkan reliabilitas, membantu pengujian silang, dan memudahkan hakim menilai bobot bukti.

Langkah ketiga adalah memperkuat kapasitas lintas profesi. Pelatihan tidak cukup hanya diberikan kepada unit cybercrime kepolisian karena bukti yang kompleks akan melewati penyidik, jaksa, ahli, dan hakim. Setiap aktor perlu memahami fungsi dan batas bukti digital, termasuk kemungkinan false positive, keterbatasan alat, serta kebutuhan dokumentasi. Penguatan sumber daya juga harus menjangkau wilayah di luar pusat agar kualitas penanganan tidak terlalu bergantung pada lokasi perkara. Standar kompetensi yang terukur diperlukan agar hasil pemeriksaan teknis dapat diterjemahkan secara konsisten ke dalam fakta hukum.

Langkah keempat adalah membangun koordinasi kelembagaan yang jelas. Respons insiden keamanan dapat melibatkan penyelenggara sistem, BSSN, Komdigi, Polri, lembaga keuangan, dan lembaga lain sesuai sektor. Setiap pihak perlu mengetahui kapan insiden berubah menjadi dugaan tindak pidana, siapa yang harus menjaga bukti, dan saluran apa yang digunakan untuk berbagi data. Protokol koordinasi perlu menetapkan tujuan, batas akses, dokumentasi, serta akuntabilitas agar pembagian peran tidak menimbulkan keterlambatan atau tumpang tindih kewenangan. Koordinasi tersebut tetap harus berjalan dalam batas dasar hukum masing-masing lembaga.

Langkah kelima adalah memperkuat kerja sama lintas negara dan dengan penyedia layanan. Banyak data penting berada pada perusahaan global yang memiliki prosedur permintaan hukum sendiri. Negara perlu memastikan permintaan data disusun secara spesifik, cepat, dan memenuhi syarat yurisdiksi tujuan. Kerja sama juga penting untuk pelacakan aset, rekening, domain, infrastruktur, dan pelaku yang berpindah negara. Pada saat yang sama, setiap mekanisme perlu menjaga hak privasi dan mencegah permintaan data yang terlalu luas. Kepastian prosedur akan meningkatkan peluang bukti dapat digunakan dalam persidangan.

Pada sisi non-penal, security by design perlu ditempatkan sejak tahap perancangan sistem. Pasal 3 ayat (1) PP Nomor 71 Tahun 2019 mewajibkan sistem diselenggarakan secara andal, aman, dan bertanggung jawab, sedangkan Pasal 4 menuntut perlindungan atas ketersediaan, keutuhan, keautentikan, kerahasiaan, dan keteraksesan Informasi Elektronik. Pengendalian akses, autentikasi yang kuat, pembaruan sistem, pemantauan anomali, segmentasi, cadangan data, dan rencana respons insiden dapat menekan peluang serta dampak serangan. Pencegahan teknis ini melengkapi, bukan menggantikan, penegakan hukum pidana.

Vol. 21 No. 4 (2026): November
DOI: 10.21070/ijler.v21i4.1655

Pencegahan scam memerlukan kombinasi teknologi, desain layanan, dan edukasi. Fitur anti-scam pada layanan telekomunikasi, verifikasi identitas, deteksi pola komunikasi berisiko, peringatan transaksi, dan mekanisme laporan cepat dapat menekan peluang pelaku memindahkan hasil kejahatan. Namun, desain pencegahan perlu memperhatikan perlindungan data dan risiko salah pemblokiran. Evaluasi berkala harus mengukur efektivitas kebijakan berdasarkan penurunan kerugian, waktu respons, dan keberhasilan memutus aliran dana, bukan hanya jumlah akun atau nomor yang diblokir.

Literasi digital juga perlu difokuskan pada perilaku konkret. Kampanye umum tentang bahaya internet sering tidak cukup mengubah keputusan pengguna pada saat menerima tekanan atau bujukan. Materi edukasi perlu mengajarkan verifikasi identitas, pengelolaan kata sandi, penggunaan autentikasi multifaktor, larangan membagikan kode verifikasi, pemeriksaan alamat situs, serta prosedur cepat ketika akun atau rekening disalahgunakan. Pendidikan yang berulang dan berbasis skenario lebih relevan untuk menghadapi modus yang cepat berubah. Literasi tersebut perlu dihubungkan dengan saluran pelaporan yang mudah agar korban dapat bertindak sebelum kerugian meluas.

Khusus pada AI dan deepfake, kebijakan harus berbasis risiko dan perbuatan. Indonesia membutuhkan norma yang cukup jelas untuk mengatasi penggunaan AI yang menimbulkan kerugian konkret tanpa mempidanakan teknologi atau konten sintetis secara umum. Kebijakan perlindungan data juga perlu menyesuaikan kemampuan AI memproses data dalam skala besar, karena regulasi yang terlalu umum dapat menyisakan celah pada pengumpulan, pemrosesan, dan penyalahgunaan data pribadi berbasis AI [30]. Arah kebijakan yang proporsional dapat memprioritaskan penipuan, pemerasan, pencurian identitas, pornografi non-konsensual, atau manipulasi lain ketika unsur kerugian dan kesalahan telah dapat dirumuskan secara pasti.

Aspek korban juga perlu masuk ke dalam desain kebijakan. Penegakan cybercrime sering berfokus pada identifikasi pelaku, sementara korban membutuhkan penghentian penyebaran konten, pemulihan akses akun, pembekuan transaksi, koreksi data, atau informasi mengenai perkembangan perkara. Mekanisme pelaporan yang terintegrasi antara penyelenggara layanan dan penegak hukum dapat mempercepat pengamanan bukti sekaligus membatasi kerugian lanjutan. Pendekatan ini tidak mengubah hukum pidana menjadi mekanisme kompensasi semata, tetapi menempatkan efektivitas penanganan dari sudut dampak nyata pada korban.

Kebijakan penanggulangan juga harus menjaga batas penggunaan hukum pidana. Cybercrime yang berkembang cepat sering mendorong tuntutan untuk membuat delik baru segera setelah muncul teknologi atau istilah baru. Respons semacam itu berisiko menghasilkan norma yang terlalu luas, tumpang tindih, atau cepat usang. Pembaruan hukum sebaiknya dimulai dari identifikasi kerugian, evaluasi kecukupan norma yang ada, analisis kebutuhan kriminalisasi, dan pengujian proporsionalitas. Prinsip legalitas dan due process harus tetap menjadi batas karena efektivitas penegakan hukum tidak hanya diukur dari kemampuan menghukum, tetapi juga dari ketepatan menentukan siapa yang dapat dipertanggungjawabkan dan berdasarkan bukti apa.

Secara keseluruhan, kebijakan yang paling relevan adalah kebijakan yang mengintegrasikan norma pidana, prosedur bukti elektronik, kapasitas forensik, koordinasi, keamanan sistem, kerja sama lintas negara, dan literasi. Pembaruan hukum pidana tetap perlu dinilai dari dampaknya terhadap kepastian hukum, perlindungan hak, dan proporsionalitas intervensi negara, bukan hanya dari kemampuan memperluas kewenangan penegakan. Prinsip tersebut relevan dalam cybercrime karena teknologi dapat mendorong perluasan pengawasan dan pengumpulan data. Kebijakan yang adaptif harus sekaligus efektif terhadap kejahatan dan terukur dalam membatasi intervensi negara.

Implikasi kebijakan yang dihasilkan penelitian ini adalah perlunya urutan reformasi yang jelas. Prioritas pertama adalah tata kelola bukti elektronik dan interoperabilitas antarinstansi, diikuti penguatan kapasitas forensik dan pencegahan berbasis desain. Kriminalisasi baru sebaiknya ditempatkan sebagai pilihan terakhir untuk kerugian yang benar-benar belum dapat dijangkau norma yang ada. Urutan ini membedakan kebutuhan penegakan yang mendesak dari dorongan memperluas delik secara reaktif.

Simpulan

Temuan inti penelitian menunjukkan bahwa cybercrime tidak dapat diperlakukan sebagai satu delik yang seragam. Pertanggungjawaban pidana harus ditentukan melalui hubungan antara posisi teknologi sebagai sasaran, sarana, atau lingkungan, unsur perbuatan, kesalahan pelaku, dan kualitas bukti digital. Analisis Putusan PN Surabaya Nomor 2574/Pid.Sus/2022/PN Sby dan Putusan PN Jakarta Selatan Nomor 616/Pid.Sus/2023/PN JKT.SEL menegaskan bahwa kecocokan antara unsur pasal, atribusi pelaku, dan bukti elektronik menjadi penentu utama penerapan hukum.

Masalah utama sistem penegakan terletak pada fragmentasi antarrezim hukum dan ketergantungan antarproses pembuktian. KUHP Nasional, UU ITE, UU Pelindungan Data Pribadi, dan KUHAP baru menyediakan dasar hukum yang lebih kuat, tetapi efektivitasnya masih dibatasi oleh perolehan data lintas platform, autentikasi dan integritas bukti, chain of custody, yurisdiksi lintas negara, ketimpangan kapasitas digital forensik, serta koordinasi kelembagaan. Reformasi bukti elektronik melalui Pasal 235 dan Pasal 242 KUHAP memperbaiki posisi formal, tetapi belum otomatis menyelesaikan persoalan implementasi.

Implikasi kebijakannya adalah mendahulukan harmonisasi penerapan norma, tata kelola bukti digital yang dapat diaudit, interoperabilitas antarinstansi, peningkatan kapasitas forensik, security by design, dan literasi digital. Pembentukan delik baru perlu dibatasi pada kerugian yang belum dapat dijangkau secara memadai oleh norma yang ada. Karena penelitian ini bersifat normatif dan menggunakan dua putusan secara purposif, penelitian selanjutnya perlu menguji pelaksanaan KUHAP

ISSN 2598-9928 (online), https://ijler.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Vol. 21 No. 4 (2026): November
DOI: 10.21070/ijler.v21i4.1655

2025 secara empiris, terutama konsistensi chain of custody, kecepatan akses data lintas yurisdiksi, dan pengalaman aparat serta korban.

Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada pihak-pihak yang telah mendukung proses penyusunan dan penyelesaian penelitian ini.

References

1. P. J. I. Indonesia, "Tiga dekade APJII dorong konektivitas inklusif hingga wilayah 3T," 2026. [Online]. Available: https://apjii.or.id/berita/d/tiga-dekade-apjii-dorong-konektivitas-inklusif-hingga-wilayah-3t
2. K. K. dan D. R. Indonesia, "Angka kerugian scam di Indonesia capai Rp7,5 triliun, Wamen Nezar dorong pelindungan konsumen digital," 2026. [Online]. Available: https://www.komdigi.go.id/berita/siaran-pers/detail/angka-kerugian-scam-di-indonesia-capai-rp75-triliun-wamen-nezar-dorong-pelindungan-konsumen-digital
3. Erikha and A. Saptomo, "Dilemma of legal policy to address cybercrime in the digital era," Asian J. Soc. Humanit., vol. 3, no. 3, 2024, doi: 10.59888/ajosh.v3i3.452.
4. B. Fransiska and F. B. L. Tobing, "Securing Indonesia cyber space: Strategies for cyber security in the digital era," J. Stud. Sos. dan Polit., vol. 7, no. 1, pp. 50–62, 2023, doi: 10.19109/jssp.v7i1.15925.
5. Z. Kasim, "Kebijakan hukum pidana untuk penanggulangan cyber crime di Indonesia," Indragiri Law Rev., vol. 2, no. 1, pp. 18–24, 2024, doi: 10.32520/ilr.v2i1.22.
6. S. Suseno, A. M. Ramli, R. F. Mayana, T. Safiranita, and B. A. N. Tiarma, "Cybercrime in the new criminal code in Indonesia," Cogent Soc. Sci., vol. 11, no. 1, Art. no. 2439543, 2025, doi: 10.1080/23311886.2024.2439543.
7. D. G. G. Santosa and K. M. I. Kamali, "Acquisition and presentation of digital evidence in criminal trial in Indonesia," J. Huk. dan Peradil., vol. 11, no. 2, pp. 195–218, 2022, doi: 10.25216/jhp.11.2.2022.195-218.
8. Hardinanto, B. N. Arief, and J. Setiyono, "The significance of computer forensics in electronic documents as evidence in criminal law," J. Cakrawala Huk., vol. 14, no. 2, pp. 155–166, 2023, doi: 10.26905/idjch.v14i2.10820.
9. M. Lasaka, "Ius constituendum of electronic evidence arrangement in criminal procedure law," J. Leg., vol. 16, no. 2, pp. 154–166, 2023, doi: 10.33756/jelta.v16i2.20306.
10. H. Samudra, S. Basu, and C. Sáenz Pérez, "Digital challenge, analogue mind-set: Assessing Indonesia's electronic criminal evidence framework," J. Indones. Leg. Stud., vol. 11, no. 1, pp. 257–298, 2026, doi: 10.15294/jils.v11i1.35378.
11. S. M. T. Situmeang, D. Pudjiastuti, and Sutarjo, "Adequacy of Indonesian cybercriminal law against generative AI-based social engineering attacks," Res Nullius Law J., vol. 6, no. 1, pp. 82–97, 2024, doi: 10.34010/rnlj.v6i1.19927.
12. S. A. Kusnadi and D. W. S. Putri, "Perlindungan hak privasi dalam penyalahgunaan teknologi deepfake di Indonesia," J. Rechts Vinding Media Pembin. Huk. Nas., vol. 14, no. 2, pp. 195–210, 2025, doi: 10.33331/rechtsvinding.v14i2.2135.
13. S. Butt, "Indonesia's new Criminal Code: Indigenising and democratising Indonesian criminal law?," Griffith Law Rev., vol. 32, no. 2, pp. 190–214, 2023, doi: 10.1080/10383441.2023.2243772.
14. K. Phillips, J. C. Davidson, R. R. Farr, C. Burkhardt, S. Caneppele, and M. P. Aiken, "Conceptualizing cybercrime: Definitions, typologies and taxonomies," Forensic Sci., vol. 2, no. 2, pp. 379–398, 2022, doi: 10.3390/forensicsci2020028.
15. J. Lusthaus, "Reconsidering crime and technology: What is this thing we call cybercrime?," Annu. Rev. Law Soc. Sci., vol. 20, pp. 369–385, 2024, doi: 10.1146/annurev-lawsocsci-041822-044042.
16. L. Vlasenko, N. Lutska, N. Zaiets, and V. Lysenko, "Ontological analysis of the digital crime conceptual model," 2023, doi: 10.1109/CSIT61576.2023.10324030.
17. D. A. R. Pakpahan and A. Widyawati, "Reformulation of cybercrime regulations in the misuse of artificial intelligence in Indonesia," Law Res. Rev. Q., vol. 12, no. 1, pp. 139–163, 2026, doi: 10.15294/lrrq.v12i1.42659.
18. Yusliwidaka, M. A. R. Abqa, and K. A. Wardana, "A discourse of personal data protection: How Indonesia responsible under domestic and international law?," Pandecta Res. Law J., vol. 19, no. 2, 2024, doi: 10.15294/pandecta.v19i2.13279.
19. M. A. Chairani, K. Yitawati, and A. P. Pradhana, "Urgensi pengaturan hukum bagi penyalahgunaan aplikasi deepfake," J. Rechtens, vol. 13, no. 1, 2024, doi: 10.56013/rechtens.v13i1.2668.
20. S. Nurkholisah, D. Rismana, A. E. Nugroho, A. Munjiyah, and Q. Ayunisa, "Deepfake sebagai bentuk kejahatan siber baru: Tantangan kriminalisasi dalam hukum pidana Indonesia," J. USM Law Rev., vol. 8, no. 3, pp. 2421–2445, 2025, doi: 10.26623/julr.v8i3.13060.
21. Hermanto, A. I. Nur, and I. Zulfa, "Dinamika pengaturan hukum siber Indonesia: Refleksi Putusan Mahkamah Konstitusi dalam ius constituendum," J. Rechts Vinding Media Pembin. Huk. Nas., vol. 14, no. 2, pp. 315–335, 2025, doi: 10.33331/rechtsvinding.v14i2.2045.
22. M. A. R. Indonesia, Putusan Pengadilan Negeri Surabaya Nomor 2574/Pid.Sus/2022/PN Sby. 2023. [Online]. Available: https://putusan3.mahkamahagung.go.id/direktori/putusan/zaedb1cfc3b3d5a693ca313730393031.html
23. M. A. R. Indonesia, Putusan Pengadilan Negeri Jakarta Selatan Nomor 616/Pid.Sus/2023/PN JKT.SEL. 2024. [Online]. Available: https://putusan3.mahkamahagung.go.id/pengadilan/profil/pengadilan/pn-jakarta-selatan/page/198.html
24. R. S. Billah and H. Saragih, "Tantangan penegakan hukum kejahatan siber bagi hakim dari aspek hukum pembuktian di Indonesia," Arus J. Sos. dan Hum., vol. 5, no. 2, 2025, doi: 10.57250/ajsh.v5i2.1543.

Vol. 21 No. 4 (2026): November
DOI: 10.21070/ijler.v21i4.1655

25. Monique, Y. Yuliati, and F. Sulistio, "Exploring the role of digital forensics in identifying cyber crime in Indonesia's criminal procedure law," Pena Justisia Media Komun. dan Kaji. Huk., vol. 23, no. 2, 2024, doi: 10.31941/pj.v23i2.4068.
26. N. Aisyah et al., "Analisa perkembangan digital forensik dalam penyidikan cybercrime di Indonesia secara systematic review," J. Esensi Infokom J. Esensi Sist. Inf. dan Sist. Komput., vol. 6, no. 1, pp. 22–27, 2022, doi: 10.55886/infokom.v6i1.452.
27. R. R. Ananta, D. B. Wicaksono, Indrawati, Istikhomah, and Z. Amalina, "Potensi konflik kewenangan pada perlindungan dari ancaman siber di Indonesia," J. Rechts Vinding Media Pembin. Huk. Nas., vol. 14, no. 2, pp. 233–252, 2025, doi: 10.33331/rechtsvinding.v14i2.2199.
28. R. Stoykova, "The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations," Comput. Law Secur. Rev., vol. 49, Art. no. 105801, 2023, doi: 10.1016/j.clsr.2023.105801.
29. J. D. B. S. Nono, S. K. Janggur, and R. S. Thene, "Legal consciousness in the digital era: Challenges of disinformation and cybercrime," J. Ilm. Huk. dan Hak Asasi Mns., vol. 6, no. 1, pp. 61–71, 2026, doi: 10.35912/jihham.v6i1.6611.
30. A. Fikri and T. Amelia, "Indonesia's legal policy on protecting personal data from artificial intelligence abuse," SHS Web Conf., vol. 204, Art. no. 07002, 2024, doi: 10.1051/shsconf/202420407002.

ISSN 2598-9928 (online), https://ijler.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo