JURNAL SINERGI PENGETAHUAN
Volume 7, No 2, April 2026
https://ejurnals.com/ojs/index.php/jsp

ANALISIS EFEKTIVITAS UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK DALAM MENEKAN ANGKA KEJAHATAN SIBER BERBASIS PENIPUAN DARING

Mario Randy Lengkong[1], Aprilia Pitoy[2], Imelda Melo[3], Gabriela Wowor[4], Jesheka Sumuan[5]

[1,2,3,4,5]Universitas Negeri Manado

mariolengkong@unima.ac.id[1], apriliapitoy25@gmail.com[2], imeldamelo963@gmail.com[3], gabrielawowor695@gmail.com[4], jeshekabenedicta@gmail.com[5]

ABSTRACT; *This research analyzes the effectiveness of the Electronic Information and Transactions Law in reducing cybercrime rates, specifically online fraud in Indonesia. Utilizing a normative juridical method with an empirical approach, this study evaluates fraud-related articles within this regulation against the cybercrime data from the last five years. Findings indicate that although the law provides a strong legal foundation, its effectiveness remains hindered by a lack of public digital literacy, cross-border jurisdictional constraints, and limited asset tracking infrastructure. Conclusively, this regulation requires specific revisions regarding digital financial crimes and the strengthening of strategic synergies between law enforcement authorities and technology platforms.*
Keywords: *Electronic Information Law, Cybercrime, Online Fraud, Law Enforcement, Digital Literacy.*

ABSTRAK; Penelitian ini menganalisis efektivitas Undang-Undang Informasi dan Transaksi Elektronik atau UU ITE dalam menekan angka kejahatan siber, khususnya penipuan daring yang semakin marak di Indonesia. Menggunakan metode yuridis normatif dengan pendekatan empiris, studi ini mengevaluasi implementasi pasal-pasal terkait penipuan dalam regulasi ini terhadap data kasus kejahatan siber lima tahun terakhir. Hasil penelitian menunjukkan bahwa meskipun UU ITE memberikan landasan hukum yang kuat, efektivitas penerapannya masih terhambat oleh kurangnya literasi digital masyarakat, kendala yurisdiksi lintas negara, dan keterbatasan infrastruktur pelacakan aset digital. Kesimpulannya, regulasi ini memerlukan revisi spesifik mengenai kejahatan finansial digital serta penguatan sinergi strategis antara aparat dan platform teknologi.
Kata Kunci: UU ITE, Kejahatan Siber, Penipuan Daring, Penegakan Hukum, Literasi Digital.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi pada era revolusi industri 4.0 dan transisi menuju society 5.0 telah mendisrupsi berbagai aspek kehidupan manusia, khususnya dalam bidang ekonomi dan transaksi komersial. Transformasi digital ini mendorong pergeseran masif dari aktivitas perdagangan konvensional menuju sistem perdagangan elektronik (e-commerce). Fenomena ini tidak hanya memperluas jangkauan pasar secara global tetapi juga menghadirkan ekosistem baru yang menjanjikan efisiensi dan kecepatan. Aji (2022) menegaskan bahwa peningkatan intensitas jual beli secara daring menuntut adanya kepastian hukum yang kuat, di mana integrasi antara Undang-Undang Perlindungan Konsumen dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) menjadi fondasi krusial untuk melindungi hak-hak konsumen di ruang siber. Tanpa adanya kerangka regulasi yang komprehensif, ekosistem ekonomi digital yang seharusnya membawa manfaat justru dapat menjadi ruang yang rentan terhadap berbagai eksploitasi yang merugikan masyarakat. Tata kelola informasi yang baik juga menjadi prasyarat penting dalam era keterbukaan ini. Sebagaimana disoroti oleh Winastwan (2022) dalam studi komparasinya mengenai undang-undang kearsipan dan keterbukaan informasi publik, manajemen informasi yang terstruktur, transparan, dan akuntabel merupakan pilar utama dalam membangun kepercayaan publik terhadap sistem digital dan tata kelola elektronik di Indonesia.

Namun, di balik kemudahan yang ditawarkan oleh digitalisasi, muncul ancaman serius berupa kejahatan siber (cybercrime) yang bertransformasi seiring dengan kemajuan teknologi itu sendiri. Kejahatan siber tidak lagi terbatas pada peretasan atau perusakan sistem, melainkan telah berevolusi menjadi kejahatan berbasis finansial yang terorganisir, dengan penipuan daring (online fraud) sebagai salah satu modus yang paling dominan dan meresahkan. Kejahatan penipuan daring mencakup berbagai skema, mulai dari penipuan transaksi e-commerce, investasi bodong, phising, hingga rekayasa sosial (social engineering). Kompleksitas kejahatan siber ini semakin diperparah ketika melibatkan transaksi lintas sektor. Pitaloka (2022) menyoroti adanya tantangan regulasi yang signifikan ketika kejahatan digital bersinggungan dengan sektor keuangan spesifik, seperti adanya pertentangan dan tumpang tindih kewenangan antara UU ITE dan Undang-Undang Transfer Dana dalam konteks perdagangan berjangka komoditi berbasis internet. Tumpang tindih

regulasi semacam ini menciptakan celah yurisdiksi yang sering kali dimanfaatkan oleh para pelaku kejahatan siber finansial untuk mengaburkan jejak aliran dana mereka dan menghindari jerat hukum, sehingga menyulitkan proses pelacakan aset dan pemulihan kerugian korban.

Untuk merespons ancaman tersebut, pemerintah Indonesia menetapkan UU ITE sebagai payung hukum utama (cyber law) dalam mengatur lalu lintas informasi digital dan menindak kejahatan siber. Aprilianti (2025) menjelaskan bahwa UU ITE secara konseptual dirancang untuk memberikan kepastian hukum, melindungi kepentingan umum, dan menjaga ketertiban dalam pemanfaatan teknologi informasi. Akan tetapi, efektivitas dan implementasi regulasi ini sebagai instrumen pencegahan dan penindakan kejahatan siber masih dihadapkan pada berbagai tantangan struktural dan substansial. Tantangan ini meliputi keterbatasan literasi digital masyarakat, infrastruktur penegakan hukum yang belum merata, serta asimetri kemampuan antara aparat penegak hukum dan para pelaku kejahatan siber yang terus berinovasi. Persepsi masyarakat terhadap efektivitas regulasi ini juga menjadi indikator penting. Penelitian yang dilakukan oleh Kurniawan et al. (2025) menunjukkan bahwa tinjauan hukum terhadap peran UU ITE berdasarkan persepsi akademisi dan mahasiswa masih menempatkan regulasi ini pada posisi yang ambivalen; di satu sisi diakui sebagai instrumen yang esensial, namun di sisi lain dianggap belum mampu secara optimal memberikan perlindungan nyata, khususnya bagi korban kejahatan penipuan siber yang terus meningkat secara kuantitatif maupun kualitatif.

Akar permasalahan dari belum optimalnya UU ITE dalam menekan angka penipuan daring sejatinya terletak pada kelemahan formulasi hukum dan ketidakjelasan norma dalam beberapa pasal krusial. Tan (2022) mengkritik keras eksistensi pasal-pasal dalam UU ITE yang sering dijuluki sebagai "pasal karet" karena rumusan deliknya yang tidak memenuhi asas kejelasan (lex certa) dan asas ketegasan (lex stricta). Ketidakjelasan frasa dalam regulasi ini membuka ruang bagi multitafsir di kalangan penegak hukum, yang pada gilirannya menciptakan disparitas putusan pengadilan dan ketidakpastian hukum bagi para pencari keadilan. Sejalan dengan hal tersebut, Suharto et al. (2022) dalam analisisnya terhadap kebijakan formulasi hukum pidana pada Pasal 27 Ayat (1) UU ITE menemukan bahwa struktur pemidanaan dan elemen delik yang dirumuskan belum sepenuhnya adaptif terhadap modus operandi kejahatan siber modern yang sangat dinamis. Formulasi hukum yang kaku

dan tertinggal dari perkembangan teknologi menyebabkan regulasi ini kehilangan daya prediktif dan preventifnya dalam mengantisipasi kejahatan digital yang menggunakan algoritma dan kecerdasan buatan.

Lebih spesifik lagi, celah semantik dalam UU ITE sering kali dieksploitasi oleh sindikat penipuan daring. Oktabiantoro dan Wulan (2024) membongkar ketidakjelasan makna leksikal dan gramatikal pada kata "mentransmisikan" yang termaktub dalam Pasal 28 Ayat 2 UU ITE (pasca revisi kedua). Ambiguasi terminologi hukum seperti ini menjadi kendala teknis yang serius di tahap penyidikan dan pembuktian di persidangan. Penegak hukum sering kali kesulitan membuktikan unsur mens rea (niat jahat) dan actus reus (tindakan jahat) dari pelaku penipuan jaringan perantara yang hanya berperan "meneruskan" informasi tanpa memproduksi konten penipuan tersebut secara langsung. Akibatnya, aktor intelektual atau dalang utama di balik sindikat penipuan daring berskala besar sering kali luput dari jangkauan hukum, sementara regulasi ini hanya mampu menjerat pelaku-pelaku tingkat bawah.

Di samping masalah formulasi hukum, implementasi UU ITE di lapangan justru mengalami disorientasi yang signifikan. Alih-alih difokuskan pada pemberantasan kejahatan siber berbasis ekonomi seperti penipuan daring yang menimbulkan kerugian material masif bagi masyarakat, penegakan hukum UU ITE justru lebih sering tersita pada kasus-kasus yang berkaitan dengan kebebasan berekspresi. Rauf et al. (2025) menyoroti polemik ekuivalensi antara kebebasan berekspresi dan perlindungan nama baik yang terus menjadi perdebatan sengit bahkan pasca perubahan UU ITE. Energi dan sumber daya penegak hukum banyak terkuras untuk menangani sengketa interpersonal di media sosial. Hal ini diperkuat oleh temuan Zhafira et al. (2023) yang melakukan tinjauan yuridis terhadap tindak pidana pencemaran nama baik dalam KUHP yang dikaitkan dengan Pasal 27 Ayat (3) UU ITE. Tingginya kriminalisasi terhadap kritik publik dan pelaporan pencemaran nama baik telah menciptakan efek ketakutan (chilling effect) di masyarakat, sekaligus mengalihkan fokus esensial dari urgensi pemberantasan sindikat penipuan daring. Dominasi kasus pencemaran nama baik ini menciptakan paradoks; di saat infrastruktur hukum sibuk mengurus sengketa verbal di ruang maya, para pelaku kejahatan finansial digital terus meraup keuntungan dari lemahnya pengawasan dan lambatnya respons penindakan.

Berdasarkan uraian problematika di atas, terlihat jelas adanya kesenjangan yang signifikan antara tujuan ideal pembentukan UU ITE dengan realitas empiris penegakan hukumnya di lapangan, khususnya dalam konteks kejahatan siber berbasis finansial. Di satu sisi, urgensi untuk menekan angka kejahatan penipuan daring semakin mendesak seiring dengan meningkatnya kerugian ekonomi masyarakat. Namun di sisi lain, instrumen hukum yang tersedia masih terkendala oleh tumpang tindih regulasi, ketidakjelasan formulasi delik, hingga disorientasi fokus penegakan hukum. Oleh karena itu, penelitian ini menjadi sangat krusial dan relevan untuk dilakukan. Penelitian ini bertujuan untuk menganalisis secara mendalam dan terstruktur mengenai efektivitas Undang-Undang Informasi dan Transaksi Elektronik, mengevaluasi implementasi pasal-pasal yang relevan secara faktual, serta memformulasikan solusi dan rekomendasi strategis (problem-solving) guna mereformasi pendekatan hukum dalam menekan angka kejahatan siber berbasis penipuan daring di Indonesia secara komprehensif.

Kompleksitas pemberantasan penipuan daring tidak dapat dipisahkan dari arsitektur ekosistem digital itu sendiri yang bersifat borderless (tanpa batas negara), anonim, dan asimetris. Ketika terjadi kejahatan siber berbasis finansial, aparat penegak hukum dihadapkan pada kendala teknis dan yurisdiksional yang rumit. Pelaku penipuan daring sering kali mengoperasikan server dari luar negeri, menggunakan jaringan proxy, atau memanfaatkan virtual private network (VPN) untuk menyamarkan jejak digital (digital footprint) mereka. Dalam konteks ini, kelemahan mendasar dari Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) mulai terlihat secara nyata pada aspek hukum acara dan pembuktian digital (digital forensics). Sebagaimana yang telah dielaborasi oleh Tan (2022) mengenai pelanggaran asas kejelasan rumusan dalam pasal-pasal UU ITE, ketidakpastian normatif ini menjalar pada kebingungan operasional di tingkat penyidikan. Aparat penegak hukum kerap kesulitan mengklasifikasikan barang bukti digital yang sifatnya sangat volatil dan mudah dimanipulasi, sehingga proses pembuktian rantai komando kejahatan (chain of custody) dalam sindikat penipuan daring sering kali terputus di tengah jalan. Hal ini mengakibatkan tingkat pengungkapan kasus (clearance rate) untuk penipuan finansial digital tetap rendah jika dibandingkan dengan volume aduan masyarakat yang terus melonjak.

Kerentanan ini semakin terekspos ketika kita menganalisis posisi konsumen dalam struktur transaksi elektronik. Konsumen sering kali menjadi mata rantai terlemah yang

dieksploitasi oleh pelaku kejahatan. Aji (2022) menekankan bahwa harmonisasi antara UU Perlindungan Konsumen dan UU ITE seharusnya mampu menciptakan perisai hukum yang solid. Namun, realitas praktik bisnis e-commerce sering kali melepaskan tanggung jawab platform (safe harbor policy) ketika terjadi penipuan yang dilakukan oleh pihak ketiga (merchant fiktif). Absennya kewajiban mutlak bagi penyelenggara sistem elektronik untuk memverifikasi identitas pengguna secara ketat (Know Your Customer/KYC) memberikan ruang bebas bagi para penipu untuk membuat ribuan akun palsu. Kegagalan sistemik ini mencerminkan bahwa UU ITE belum sepenuhnya mampu memaksa pelaku industri digital untuk membangun infrastruktur keamanan pencegahan penipuan yang proaktif. Hal ini didukung oleh persepsi kritis generasi muda, di mana Kurniawan et al. (2025) menemukan bahwa mahasiswa dan kaum terpelajar memandang UU ITE lebih sering hadir sebagai instrumen reaktif pasca-kejadian, alih-alih sebagai regulasi preventif yang mampu menekan niat atau kesempatan (mens rea dan actus reus) sebelum kejahatan siber tersebut terealisasi dan memakan korban.

Di ranah penegakan hukum pidana materil, persoalan menjadi semakin rumit akibat fragmentasi kewenangan antarlembaga. Pitaloka (2022) menggarisbawahi adanya benturan yurisdiksi antara UU ITE dan regulasi sektoral lainnya, seperti Undang-Undang Transfer Dana. Penipuan daring modern tidak lagi hanya mengandalkan transfer bank konvensional, melainkan telah memanfaatkan aset kripto, dompet digital (e-wallet), dan rekening penampung (money mules) yang berlapis-lapis. Ketika UU ITE hanya berfokus pada aspek "transmisi informasi elektronik", regulasi ini kehilangan cengkeramannya pada aspek "aliran dana ilegal" yang menjadi motivasi utama kejahatan tersebut. Akibatnya, terjadi kekosongan strategi pemiskinan koruptor digital (asset recovery). Praktik penegakan hukum saat ini masih berjalan secara sektoral; kepolisian mengusut tindak pidana sibernya, sementara pembekuan aliran dana memerlukan birokrasi panjang dengan Otoritas Jasa Keuangan (OJK) dan Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK). Disintegrasi ini membuat penanganan kasus menjadi lamban, memberikan waktu yang cukup bagi sindikat untuk mencairkan atau memindahkan dana hasil penipuan ke luar yurisdiksi hukum Indonesia.

Oleh karena itu, diperlukan sebuah reposisi strategis dalam menginterpretasikan dan menerapkan UU ITE. Merujuk pada kritik yang dilontarkan oleh Rauf et al. (2025) dan

Zhafira et al. (2023) terkait dominasi kasus pencemaran nama baik, negara harus berani melakukan moratorium atau penerapan keadilan restoratif (restorative justice) secara absolut untuk kasus-kasus sengketa verbal atau kebebasan berekspresi murni yang tidak berdampak pada kerugian ekonomi massal. Sumber daya aparat hukum yang berupa anggaran, waktu, dan keahlian penyidik siber—yang saat ini banyak tersedot untuk mengurus ketersinggungan personal di media sosial—harus direlokasi secara radikal untuk membentuk satuan tugas khusus (task force) anti-kejahatan finansial digital. Penegakan hukum harus diorientasikan pada "follow the money" (mengikuti aliran dana) alih-alih sekadar "follow the text" (mengikuti teks percakapan yang dianggap mencemarkan nama baik). Kebijakan dekriminalisasi de facto pada pasal-pasal defamasi akan memaksa institusi penegak hukum untuk memfokuskan energi mereka pada kejahatan penipuan daring yang secara nyata merusak fondasi ekonomi digital nasional dan memiskinkan masyarakat kelas menengah ke bawah.

Dari sudut pandang formulasi regulasi, tantangan ke depan menuntut adanya pembaruan tafsir hukum yang adaptif terhadap kecerdasan buatan (Artificial Intelligence) dan otomasi. Oktabiantoro dan Wulan (2024) yang mengkritisi ketidakjelasan makna "mentransmisikan" secara tidak langsung membuka kotak pandora mengenai subjek hukum dalam ruang siber. Sindikat penipuan saat ini tidak lagi mengetik pesan satu per satu, melainkan menggunakan bot, algoritma, dan perangkat lunak pengirim pesan massal (blast software) untuk menjerat korban secara eksponensial. Jika UU ITE (sebagaimana dianalisis oleh Suharto et al., 2022 terkait kebijakan formulasinya) masih berpegang pada paradigma kejahatan konvensional yang dilakukan secara manual oleh subjek manusia secara langsung, maka hukum akan selalu tertinggal. Diperlukan perluasan definisi delik yang mencakup pertanggungjawaban korporasi, penyedia infrastruktur, serta pencipta atau operator algoritma berbahaya (malicious code/bot). Hukum harus mampu menjerat pihak-pihak yang memfasilitasi terjadinya kejahatan, bukan hanya eksekutor akhir di lapangan.

Selain pembenahan di sektor hilir (penegakan hukum), solusi jangka panjang yang bersifat preventif dan integratif mutlak diperlukan di sektor hulu. Sesuai dengan urgensi yang disampaikan Aprilianti (2025) mengenai efektivitas dan implementasi hukum siber, pemerintah tidak bisa hanya mengandalkan pendekatan koersif. Literasi digital masyarakat harus direvolusi. Saat ini, edukasi masyarakat masih sebatas cara menggunakan teknologi

(digital skill), namun sangat minim dalam aspek keamanan digital (digital safety) dan kepekaan forensik dasar. Masyarakat harus dilatih untuk mengidentifikasi anomali komunikasi, memverifikasi tautan (link) mencurigakan, dan memahami rekam jejak digital. Bersamaan dengan itu, negara harus memaksa penyelenggara platform teknologi dan institusi perbankan untuk membangun sistem peringatan dini (early warning system) yang terintegrasi. Algoritma pendeteksi penipuan harus diwajibkan untuk disematkan pada setiap aplikasi perpesanan dan dompet digital yang beroperasi di Indonesia. Jika sebuah anomali transaksi atau transmisi informasi penipuan terdeteksi, sistem harus mampu melakukan pemblokiran sementara secara otomatis (auto-freeze mechanism) tanpa harus menunggu laporan polisi yang birokratis. Tata kelola informasi yang ditekankan oleh Winastwan (2022) dapat diaplikasikan dalam bentuk integrasi basis data nomor rekening, nomor telepon, dan identitas pelaku kejahatan siber yang dapat diakses secara real-time oleh seluruh penyedia layanan keuangan dan masyarakat umum, sehingga ruang gerak penipu dapat dipersempit secara komprehensif.

Secara keseluruhan, fenomena penipuan daring bukanlah sekadar residu dari kemajuan teknologi, melainkan sebuah ancaman terstruktur yang menguji ketahanan hukum dan kedaulatan digital negara. Kegagalan dalam meredam angka kejahatan siber berbasis finansial ini akan mendegradasi kepercayaan publik (public trust) terhadap ekosistem ekonomi digital, yang pada akhirnya dapat menghambat pertumbuhan ekonomi nasional. Oleh karena itu, penelitian ini tidak sekadar mendiagnosis kelemahan konseptual dan operasional dari Undang-Undang Informasi dan Transaksi Elektronik, tetapi lebih jauh lagi diarahkan untuk mengkonstruksi desain penyelesaian masalah (problem-solving) yang taktis dan strategis. Diperlukan sinkronisasi regulasi lintas sektor, reorientasi penegakan hukum dari delik aduan personal menuju delik ekonomi siber, serta penciptaan ekosistem keamanan digital yang mengikat tanggung jawab platform penyedia layanan. Melalui analisis kritis dan komprehensif terhadap berbagai literatur, putusan hukum, serta realitas empiris di lapangan, diharapkan penelitian ini mampu merumuskan cetak biru reformasi hukum siber yang tidak hanya menjamin kepastian keadilan, tetapi juga mampu memproteksi ruang finansial digital masyarakat Indonesia dari ancaman kejahatan tanpa wajah di era society 5.0.

TINJAUAN PUSTAKA

Kajian terhadap tata kelola informasi dan arsitektur hukum siber di Indonesia tidak dapat dilepaskan dari peran sentral Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) sebagai instrumen regulasi utama. Secara konseptual, kehadiran regulasi ini diniatkan untuk merespons transisi peradaban menuju era digital yang menuntut kepastian hukum atas setiap pertukaran data dan nilai ekonomi di ruang maya. Aprilianti (2025) dalam kajiannya menegaskan bahwa efektivitas dan implementasi UU ITE sebagai hukum siber di Indonesia sejatinya dirancang untuk memberikan pelindungan komprehensif, namun pada praktiknya masih terbelit oleh berbagai tantangan struktural yang membutuhkan solusi konkret. Pelindungan ini sangat krusial, terutama pada sektor perdagangan elektronik (e-commerce) yang melibatkan interaksi langsung antara pelaku usaha dan konsumen. Dalam konteks ini, Aji (2022) menyoroti pentingnya sinkronisasi pengaturan jual beli secara daring yang harus menyandingkan UU ITE dengan Undang-Undang Perlindungan Konsumen. Harmonisasi kedua regulasi ini menjadi fondasi penyelesaian masalah (problem-solving) yang elementer guna memastikan bahwa sistem elektronik tidak hanya memfasilitasi transaksi, tetapi juga menjamin hak ganti rugi serta keamanan data konsumen dari potensi kejahatan penipuan digital. Lebih jauh, pengelolaan data dan informasi digital yang menopang seluruh aktivitas ini juga membutuhkan tata kelola yang transparan dan akuntabel, di mana prinsip-prinsip keterbukaan informasi yang dianalisis oleh Winastwan (2022) dalam studi komparasinya turut memegang peranan penting dalam membangun ekosistem digital yang terpercaya dan terawasi oleh publik.

Meskipun kerangka dasar hukum siber telah terbentuk, literatur akademik secara konsisten mengidentifikasi kelemahan substansial pada tingkat perumusan norma atau formulasi delik dalam UU ITE yang justru menghambat efektivitas penegakan hukum. Kelemahan ini berakar pada pelanggaran asas legalitas, khususnya asas kejelasan rumusan (lex certa). Analisis komprehensif yang dilakukan oleh Tan (2022) secara spesifik membongkar eksistensi "pasal karet" di dalam UU ITE. Ketidakjelasan batasan terminologi hukum dalam regulasi ini menciptakan ruang multitafsir yang sangat lebar, sehingga penegak hukum memiliki diskresi yang berlebihan dalam menafsirkan sebuah perbuatan. Akibatnya, alih-alih memberikan kepastian hukum bagi korban kejahatan siber yang sebenarnya, regulasi ini sering kali memunculkan disparitas penindakan. Problematika formulasi ini juga

dielaborasi lebih tajam oleh Suharto, Parulian, dan Achmad (2022) melalui tinjauan mereka terhadap kebijakan formulasi hukum pidana pada Pasal 27 Ayat (1) UU ITE. Mereka menemukan bahwa pendekatan pemidanaan yang dirumuskan masih bersifat konvensional dan belum sepenuhnya memadai untuk menjerat kompleksitas kejahatan siber modern. Ketertinggalan formulasi hukum ini mengakibatkan instrumen pidana gagal berfungsi sebagai alat pencegahan (deterrent effect) yang efektif terhadap laju evolusi kejahatan digital.

Kecacatan linguistik hukum dalam UU ITE tidak hanya berhenti pada tataran teori, melainkan berdampak langsung pada kegagalan teknis dalam mengusut tuntas sindikat kejahatan siber, termasuk penipuan daring. Oktabiantoro dan Wulan (2024) menyoroti ketidakjelasan makna leksikal pada frasa "mentransmisikan" yang diatur dalam Pasal 28 Ayat 2 UU ITE pasca revisi kedua. Dalam anatomi kejahatan penipuan daring, pelaku jarang beroperasi secara tunggal; mereka menggunakan jaringan afiliator, bot, dan operator lapis bawah untuk menyebarkan tautan jebakan (phising) atau tawaran investasi fiktif. Ambiguasi makna "mentransmisikan" menyulitkan aparat hukum untuk membedakan antara pelaku utama yang memiliki niat jahat (mens rea) dengan pihak perantara yang sering kali tidak menyadari bahwa mereka sedang mendistribusikan muatan penipuan. Kesenjangan makna ini adalah celah operasional yang terus dieksploitasi oleh sindikat kejahatan siber berskala besar untuk melindungi aktor intelektual (mastermind) mereka dari jerat pemidanaan, sementara hukum hanya mampu menindak pelaku operasional di tingkat bawah.

Selain kendala formulasi delik, kebuntuan pemberantasan penipuan daring juga diperparah oleh benturan yurisdiksi lintas sektoral ketika kejahatan siber bertransformasi menjadi kejahatan finansial yang kompleks. Pitaloka (2022) secara kritis membedah pertentangan antara UU ITE dengan Undang-Undang Transfer Dana, khususnya dalam konteks perdagangan berjangka komoditi berbasis internet. Kejahatan penipuan daring saat ini sangat bergantung pada kecepatan pemindahan aset digital dan pencucian uang melalui berbagai instrumen keuangan elektronik. Ketika UU ITE hanya memiliki kapasitas untuk menindak aspek transmisi data ilegalnya, instrumen ini kehilangan taji untuk memblokir, menyita, dan mengembalikan aset korban secara cepat karena terhalang oleh birokrasi regulasi perbankan dan transfer dana. Pertentangan norma ini mengindikasikan bahwa sistem hukum Indonesia belum memiliki pendekatan holistik (integrated criminal justice system)

dalam menangani kejahatan ekonomi digital. Solusi atas permasalahan ini menuntut adanya restrukturisasi kewenangan yang memungkinkan aparat penegak hukum siber untuk melakukan intervensi langsung terhadap lalu lintas keuangan elektronik tanpa harus terjebak dalam yurisdiksi hukum sektoral yang kaku.

Ironisnya, di tengah keterbatasan instrumen hukum untuk menangani kejahatan finansial yang masif, implementasi penegakan UU ITE di lapangan justru mengalami disorientasi fokus yang tajam. Energi sistem peradilan pidana lebih banyak terkuras untuk menangani sengketa interpersonal yang berkaitan dengan ketersinggungan dan reputasi. Rauf, Ahamd, dan Moha (2025) menganalisis secara mendalam ekuivalensi antara kebebasan berekspresi dan perlindungan nama baik pasca perubahan UU ITE. Mereka menemukan bahwa pasal-pasal defamasi masih menjadi instrumen utama yang paling sering dilaporkan, menciptakan tumpang tindih antara kritik publik dan tindak pidana murni. Hal ini sejalan dengan temuan Zhafira, Ismansyah, dan Yoserwan (2023) yang melakukan tinjauan yuridis terhadap tindak pidana pencemaran nama baik dalam KUHP yang dikorelasikan dengan Pasal 27 Ayat (3) UU ITE. Over-kriminalisasi pada aspek pencemaran nama baik tidak hanya menciptakan efek ketakutan (chilling effect) pada tatanan demokrasi, tetapi secara strategis merugikan agenda pemberantasan kejahatan siber. Sumber daya penyidik, laboratorium forensik digital, dan kapasitas pengadilan tersita untuk menyelesaikan konflik verbal di media sosial, sehingga penanganan kasus-kasus penipuan daring yang terorganisir dan menimbulkan kerugian material miliaran rupiah menjadi terbengkalai dan berjalan sangat lambat.

Kegagalan sistemik ini pada akhirnya berimplikasi langsung pada tingkat kepercayaan publik terhadap supremasi hukum di ruang digital. Tinjauan hukum yang dilakukan oleh Kurniawan et al. (2025) mengonfirmasi hal ini melalui pengukuran persepsi mahasiswa terhadap peran UU ITE. Publik, khususnya kalangan terpelajar, memandang bahwa UU ITE gagal menjalankan fungsi esensialnya sebagai instrumen perlindungan pelopor bagi masyarakat rentan di dunia maya. Persepsi negatif ini merupakan indikator empiris bahwa pendekatan hukum positif (legal-positivistik) yang dianut selama ini tidak lagi relevan tanpa diimbangi oleh reformasi institusional. Berdasarkan sintesis dari berbagai literatur di atas, terlihat jelas sebuah kesenjangan fundamental: hukum siber Indonesia saat ini terlalu sibuk mengelola etika berkomunikasi (defamasi) dan terjebak dalam ambiguitas leksikal,

sementara kejahatan riil berupa penipuan finansial digital dibiarkan berkembang melalui celah yurisdiksi sektoral. Oleh karena itu, kerangka penyelesaian masalah yang harus dikonstruksi ke depan tidak lagi sekadar menuntut revisi redaksional pasal per pasal, melainkan sebuah rekayasa hukum (social engineering by law) yang mengintegrasikan kewenangan pelacakan aliran dana digital, penegasan pertanggungjawaban penyedia platform elektronik, serta reorientasi absolut penegakan hukum dari delik aduan personal menuju pemberantasan kejahatan ekonomi siber transnasional

METODE PENELITIAN

Penelitian ini menggunakan desain penelitian hukum campuran (mixed-method legal research) yang mengintegrasikan metode yuridis normatif dengan pendekatan yuridis empiris (sosio-legal). Pemilihan metodologi ini didasarkan pada urgensi pemecahan masalah (problem-solving) terkait disrupsi kejahatan siber finansial yang tidak cukup hanya dianalisis melalui kacamata teks undang-undang semata, melainkan menuntut evaluasi faktual atas bekerjanya hukum tersebut di tengah masyarakat. Pendekatan yuridis normatif difokuskan untuk membedah struktur, hierarki, dan sinkronisasi norma hukum positif yang mengatur ruang siber di Indonesia. Dalam pelaksanaannya, penelitian ini menerapkan pendekatan perundang-undangan (statute approach) untuk memetakan arsitektur regulasi yang saling bersinggungan. Sebagaimana metode yang diaplikasikan oleh Aji (2022), pendekatan ini digunakan secara taktis untuk menganalisis relasi dan harmonisasi antara Undang-Undang Perlindungan Konsumen dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) guna membangun konstruksi perlindungan hukum yang presisi bagi korban penipuan transaksi elektronik. Lebih jauh, pendekatan sistematis (systematic approach) dikerahkan untuk mengidentifikasi dan mengurai antinomi atau pertentangan hukum antar-regulasi sektoral. Merujuk pada kerangka analisis Pitaloka (2022), metode ini diadopsi untuk membedah tumpang tindih yurisdiksi antara UU ITE dengan Undang-Undang Transfer Dana, sebuah langkah esensial untuk memformulasikan strategi pelacakan aliran dana dan pemulihan aset (asset recovery) dalam tindak pidana penipuan berbasis internet. Sinkronisasi vertikal dan horizontal ini juga diperluas dengan meninjau korelasi UU ITE terhadap rezim pidana umum, menggunakan landasan tinjauan yuridis seperti yang dicontohkan oleh Zhafira, Ismansyah, dan Yoserwan (2023) dalam mengaitkan ketentuan pidana khusus siber dengan Kitab Undang-Undang Hukum Pidana (KUHP).

Untuk menelisik lebih dalam akar kelemahan regulasi yang selama ini menghambat pemberantasan penipuan daring, penelitian normatif ini juga mengoperasionalkan pendekatan konseptual (conceptual approach) dan pendekatan analitis (analytical approach) dalam membedah formulasi delik. Penelitian ini secara kritis mengevaluasi kebijakan formulasi hukum pidana yang termaktub dalam UU ITE dengan mereplikasi instrumen analisis kebijakan hukum (penal policy) yang digagas oleh Suharto, Parulian, dan Achmad (2022). Tujuannya adalah untuk mendiagnosis apakah struktur pemidanaan saat ini masih adaptif dan relevan dengan modus operandi kejahatan digital modern yang terotomasi. Selain itu, untuk mengurai problematika ketidakpastian hukum, penelitian ini menggunakan penafsiran gramatikal (grammatical interpretation) dan penafsiran otentik untuk membedah makna teks dalam regulasi. Pendekatan ini secara langsung diilhami oleh kajian Tan (2022) yang menganalisis rasio logis dari pasal-pasal yang kerap dilabeli "pasal karet" terhadap pemenuhan asas kejelasan rumusan (lex certa) dan ketegasan (lex stricta). Secara lebih spesifik, analisis linguistik hukum juga diterapkan untuk mendekonstruksi makna frasa-frasa krusial, meminjam presisi metode bedah leksikal yang dilakukan oleh Oktabiantoro dan Wulan (2024) terhadap ketidakjelasan makna kata “mentransmisikan” pasca revisi regulasi. Dengan metode bedah bahasa hukum ini, ambiguitas pasal yang selama ini menjadi celah bagi lolosnya aktor intelektual (mastermind) sindikat penipuan daring dapat diidentifikasi dan dirumuskan ulang secara taktis agar tidak menimbulkan bias di tahap peradilan.

Sebagai pelengkap analisis tekstual, penelitian ini mengadopsi pendekatan historis (historical approach) dan pendekatan perbandingan (comparative approach). Pendekatan historis digunakan untuk melacak rasio legis dan dinamika perubahan paradigma legislator dari waktu ke waktu. Hal ini diimplementasikan dengan menelaah risalah persidangan dan naskah akademik rentetan revisi UU ITE, sejalan dengan metode analisis pasca-perubahan regulasi yang diterapkan oleh Rauf, Ahamd, dan Moha (2025) ketika mengevaluasi pergeseran fokus hukum antara ekuivalensi kebebasan berekspresi dan pencemaran nama baik. Pemahaman terhadap sejarah dan disorientasi perundang-undangan ini sangat krusial untuk memastikan bahwa tawaran solusi ke depan dapat secara radikal merelokasi fokus hukum kembali pada pemberantasan kejahatan ekonomi siber. Sementara itu, pendekatan komparatif diaplikasikan untuk mencari patokan praktik tata kelola sistem terbaik. Sebagaimana desain studi komparasi silang regulasi yang digunakan oleh Winastwan (2022)

dalam membandingkan rezim kearsipan dan keterbukaan informasi, metode perbandingan dalam penelitian ini diarahkan untuk menganalisis efektivitas mekanisme tata kelola basis data elektronik lintas lembaga guna menciptakan sistem peringatan dini (early warning system) yang terintegrasi, yang dapat mendeteksi indikasi penipuan daring sebelum menimbulkan kerugian material masif.

Beranjak pada aspek operasional, penelitian ini menerapkan pendekatan yuridis empiris untuk mengukur tingkat efektivitas (effectiveness measure) perlindungan hukum secara faktual. Pendekatan ini berangkat dari landasan pemikiran bahwa kebenaran sebuah regulasi tidak hanya diuji di atas kertas, tetapi pada kapabilitasnya dalam merekayasa perilaku masyarakat (social engineering) dan menekan angka kejahatan secara kuantitatif. Untuk mengevaluasi hal ini, kerangka asesmen efektivitas dan implementasi hukum siber yang diuraikan oleh Aprilianti (2025) digunakan sebagai metrik penilaian utama. Pengukuran efektivitas ini menyoroti kesiapan struktur penegak hukum, substansi regulasi dalam menghadapi kejahatan transnasional, serta budaya hukum masyarakat. Dalam menggali data riil terkait budaya hukum dan tingkat literasi digital, penelitian ini menggunakan teknik pengumpulan data primer berupa kuesioner dan observasi partisipatoris. Penggunaan data persepsi lapangan ini sangat relevan dan divalidasi oleh kerangka metodologis yang diusung oleh Kurniawan et al. (2025), di mana tinjauan hukum berdasarkan pandangan spesifik dari masyarakat terpelajar (seperti mahasiswa) dijadikan instrumen kalibrasi yang sahih untuk menilai sejauh mana UU ITE benar-benar hadir sebagai perisai perlindungan, dan bukan sekadar instrumen penindakan reaktif.

Integrasi data dalam penelitian ini dikelola melalui teknik triangulasi (data triangulation) yang ketat antara studi dokumen tertulis, statistik kasus kejahatan siber dari kepolisian, dan wawancara mendalam (in-depth interview) dengan praktisi hukum, penyidik forensik digital, serta perwakilan sektor perbankan. Seluruh himpunan data kemudian dianalisis menggunakan metode kualitatif deskriptif dengan logika penalaran deduktif-induktif yang difokuskan sepenuhnya pada penciptaan solusi praktis (problem-solving oriented analysis). Secara deduktif, penelitian ini menguji presisi norma UU ITE terhadap kasus-kasus penipuan daring kontemporer. Secara induktif, penelitian ini mengonstruksi temuan empiris di lapangan menjadi sebuah sintesis kebijakan baru. Tahap akhir dari alur metodologi ini tidak berhenti pada konklusi deskriptif, melainkan bermuara pada perumusan

rancangan intervensi yang konkret; mulai dari draf usulan revisi pasal spesifik untuk membasmi celah yurisdiksi, desain standard operating procedure (SOP) pelacakan aset digital lintas instansi, hingga perancangan model pertanggungjawaban mutlak (strict liability) bagi platform penyedia sistem elektronik. Melalui kerangka metodologi yang komprehensif ini, penelitian diproyeksikan mampu menghasilkan intervensi hukum dan teknologi yang dapat langsung diadopsi secara nyata untuk mereduksi eskalasi penipuan daring di Indonesia.

HASIL DAN PEMBAHASAN

Implementasi Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) sebagai instrumen utama hukum siber di Indonesia menunjukkan disparitas yang tajam antara tujuan regulasi dan realitas empiris, khususnya dalam menekan eskalasi kejahatan siber berbasis penipuan daring. Secara arsitektural, regulasi ini dikonstruksi untuk menjamin kepastian hukum dan melindungi masyarakat di ruang digital, namun efektivitasnya berulang kali diuji oleh dinamika kejahatan yang terotomasi dan lintas batas (Aprilianti, 2025). Ketidakmampuan regulasi ini dalam menghadirkan perlindungan preventif tercermin kuat dari skeptisisme publik. Evaluasi yang mengukur persepsi kelompok terpelajar membuktikan bahwa UU ITE cenderung dipersepsikan gagal menjalankan peran perlindungan substansialnya, dan lebih sering hadir sebagai instrumen reaktif pasca-kejadian yang tidak berpihak pada pemulihan kerugian korban penipuan (Kurniawan et al., 2025). Oleh karena itu, pendekatan pemecahan masalah (problem-solving) yang harus segera diterapkan oleh pemerintah adalah mengubah paradigma penegakan hukum dari yang bersifat kuratif-reaktif menjadi preventif-sistemik. Hal ini menuntut adanya restrukturisasi tugas pokok aparat penegak hukum siber agar tidak hanya berfokus pada penangkapan pelaku setelah laporan dibuat, tetapi juga mewajibkan patroli siber yang terintegrasi dengan algoritma pendeteksi anomali transaksi pada platform digital, sehingga upaya pencegahan (deterrent effect) dapat berjalan optimal sebelum kejahatan terealisasi.

Akar fundamental dari inefisiensi UU ITE dalam menjerat sindikat penipuan daring terletak pada kecacatan perumusan norma hukum pidana (penal policy) di dalamnya. Kebijakan formulasi pidana dalam UU ITE terbukti masih sangat konvensional dan gagal mengantisipasi lompatan teknologi yang digunakan oleh pelaku kejahatan kerah putih digital (Suharto et al., 2022). Kelemahan ini diperparah oleh pelanggaran asas kejelasan rumusan

(lex certa), yang melahirkan pasal-pasal karet dengan multitafsir tinggi di kalangan penegak hukum (Tan, 2022). Disparitas interpretasi ini memberikan celah bagi penjahat siber untuk memanipulasi konstruksi hukum, sehingga mereka dapat berkelit dari jerat pidana. Sebagai solusi taktis yang dapat langsung diterapkan, Dewan Perwakilan Rakyat (DPR) bersama instansi terkait harus segera melakukan amendemen spesifik yang meredefinisi elemen delik kejahatan siber finansial secara rigid. Frasa-frasa teknis terkait kejahatan siber tidak boleh lagi menggunakan terminologi makro yang ambigu. Harus ada pembakuan definisi yang mengikat secara nasional mengenai instrumen kejahatan siber seperti *phising*, rekayasa sosial (*social engineering*), dan manipulasi algoritma, sehingga penyidik memiliki pedoman baku yang tidak dapat dibantah dalam proses penyidikan hukum acara pidana.

Lebih rinci pada tataran leksikal, ambiguitas operasional juga terjadi pada frasa "mentransmisikan" sebagaimana diatur dalam Pasal 28 Ayat 2 UU ITE. Dalam anatomi kejahatan penipuan daring kontemporer, sindikat kejahatan memecah peran operasionalnya menjadi produsen konten, distributor (afiliator/bot), dan penadah dana. Ketidakjelasan makna "mentransmisikan" mengakibatkan penegak hukum sering kali hanya mampu menangkap operator tingkat bawah atau perantara yang mendistribusikan tautan penipuan, sementara aktor intelektual (*mastermind*) tetap tidak tersentuh (Oktabiantoro & Wulan, 2024). Langkah penyelesaian konkret untuk mengatasi kebuntuan ini adalah Mahkamah Agung harus menerbitkan Peraturan Mahkamah Agung (PERMA) atau Surat Edaran Mahkamah Agung (SEMA) yang memberikan perluasan tafsir resmi atas pasal tersebut. Tafsir ini harus mencakup doktrin pertanggungjawaban komando (*command responsibility*) dalam kejahatan siber terorganisir. Dengan demikian, pihak yang mendanai, memfasilitasi server, atau menyusun skema penipuan dapat dijerat secara kumulatif meskipun mereka tidak secara fisik menekan tombol transmisi data jebakan tersebut kepada korban.

Di sisi lain, kelemahan struktural UU ITE diperburuk oleh disorientasi penegakan hukum yang akut. Alih-alih mengalokasikan sumber daya investigasi siber untuk mengejar sindikat penipuan daring yang menyedot triliunan rupiah uang rakyat, aparat justru terjebak dalam pusaran penanganan kasus-kasus defamasi. Polemik mengenai ekuivalensi antara kebebasan berekspresi dan perlindungan nama baik terus menyita kapasitas sistem peradilan pidana (Rauf et al., 2025). Over-kriminalisasi pada delik pencemaran nama baik yang dikaitkan dengan ketentuan KUHP menciptakan beban perkara yang tidak proporsional dan

mengerdilkan urgensi pemberantasan kejahatan ekonomi digital (Zhafira et al., 2023). Solusi radikal yang dapat diimplementasikan segera oleh Kepolisian Negara Republik Indonesia adalah memberlakukan diskresi ketat berupa penerapan keadilan restoratif (*restorative justice*) secara absolut bagi seluruh kasus penghinaan atau pencemaran nama baik berbasis siber yang murni merupakan sengketa personal. Melalui pemangkasan birokrasi kasus defamasi ini, seluruh sumber daya penyidik forensik digital, anggaran investigasi, dan kapasitas laboratorium siber dapat direalokasikan 100% untuk membentuk Satuan Tugas Khusus Anti-Penipuan Finansial Daring yang bekerja secara progresif memburu sindikat kejahatan siber ekonomi.

Persoalan semakin kompleks ketika kejahatan siber bersinggungan langsung dengan sistem keuangan digital, memunculkan benturan yurisdiksi antara UU ITE dan regulasi sektoral lainnya. Penipuan daring selalu bermuara pada pemindahan aset, namun instrumen pelacakan UU ITE sering kali bertentangan atau tumpang tindih dengan yurisdiksi Undang-Undang Transfer Dana, yang menyulitkan upaya pemblokiran aliran uang hasil kejahatan secara cepat (Pitaloka, 2022). Sindikat memanfaatkan birokrasi lintas sektoral ini untuk memindahkan aset kripto atau mencairkan dana sebelum polisi mendapatkan izin penyitaan. Pemecahan masalah yang strategis untuk kondisi ini adalah pembentukan mekanisme *Auto-Freeze* (pemblokiran otomatis) yang terlegitimasi hukum. Pemerintah harus menerbitkan Peraturan Pemerintah (PP) yang memandatkan integrasi *Application Programming Interface* (API) antara Kepolisian, Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK), Bank Indonesia, dan seluruh penyelenggara dompet digital. Jika sebuah rekening atau nomor telepon terdeteksi menerima dana dari banyak korban dalam waktu singkat dan dilaporkan melalui portal nasional, sistem harus secara otomatis membekukan akun tersebut dalam hitungan detik tanpa harus menunggu surat perintah pengadilan, guna menyelamatkan aset korban (*asset recovery*).

Perlindungan terhadap korban juga mengharuskan adanya pelibatan tanggung jawab mutlak dari penyelenggara sistem elektronik (platform e-commerce dan penyedia layanan digital). Selama ini, perlindungan konsumen dalam jual beli daring belum sepenuhnya sinkron dengan penegakan UU ITE, sehingga platform sering kali berlindung di balik kebijakan pelepasan tanggung jawab (*safe harbor policy*) ketika terjadi penipuan di ekosistem mereka (Aji, 2022). Praktik lepas tangan ini tidak boleh dilanjutkan. Kementerian

Komunikasi dan Digital harus menerapkan regulasi kewajiban *Strict Liability* (tanggung jawab mutlak) bagi platform digital. Jika terbukti bahwa sebuah platform memiliki sistem *Know Your Customer* (KYC) yang lemah sehingga memungkinkan penipu membuat akun fiktif berulang kali, maka platform tersebut wajib menanggung beban ganti rugi secara proporsional kepada korban. Sanksi administratif berupa pencabutan izin operasi sementara harus diberlakukan bagi platform yang menolak memperketat verifikasi identitas penggunanya berbasis data biometrik kependudukan.

Sebagai langkah penyempurnaan, tata kelola informasi harus dioptimalkan untuk memutus rantai penyebaran kejahatan siber. Praktik manajemen keterbukaan informasi dan integrasi kearsipan data publik yang baik dapat menjadi alat deteksi dini yang mematikan bagi pelaku kejahatan (Winastwan, 2022). Solusi jangka panjang yang harus dikerjakan adalah membangun *National Cyber-Fraud Database Center* (Pusat Data Penipuan Siber Nasional) yang bersifat *open-source* bagi para pengembang teknologi keamanan. Basis data ini akan mengarsipkan seluruh nomor telepon, rekening bank, tautan URL, dan alamat IP yang pernah dilaporkan terlibat penipuan. Penyelenggara jasa telekomunikasi dan penyedia layanan internet (ISP) diwajibkan oleh hukum untuk mengintegrasikan basis data ini ke dalam infrastruktur mereka, sehingga setiap SMS phising, panggilan penipuan, atau akses ke situs bodong dapat diblokir secara proaktif di tingkat operator sebelum pesan tersebut mencapai layar ponsel masyarakat. Dengan mengintegrasikan reformasi regulasi, realokasi fokus penegakan hukum, tanggung jawab mutlak platform digital, dan inovasi tata kelola data terpusat, kelemahan fundamental implementasi UU ITE dapat diatasi secara komprehensif untuk menekan angka kejahatan penipuan daring di Indonesia.

Eskalasi ancaman penipuan daring tidak hanya menguji keandalan teks hukum nasional, tetapi juga menyingkap kerentanan yurisdiksi dalam menghadapi kejahatan transnasional yang tidak mengenal batas negara (borderless). Aprilianti (2025) secara komprehensif menguraikan bahwa tantangan terbesar implementasi Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) sebagai hukum siber di Indonesia adalah asimetri antara yurisdiksi aparat penegak hukum yang dibatasi oleh wilayah kedaulatan, dengan infrastruktur kejahatan siber yang sering kali mengoperasikan peladen (server) dan pusat komando dari luar negeri. Ketika sindikat penipuan berbasis di yurisdiksi asing, proses penyidikan hukum acara pidana Indonesia kerap menemui jalan buntu. Sebagai solusi taktis

yang dapat segera dieksekusi oleh pemerintah, Kementerian Luar Negeri bersama Kementerian Komunikasi dan Digital harus menginisiasi pembentukan Perjanjian Bantuan Hukum Timbal Balik (Mutual Legal Assistance Treaty/MLAT) yang dikhususkan secara eksklusif untuk tindak pidana siber finansial di kawasan ASEAN. Traktat ini harus memuat klausul *fast-track extradition* dan pembagian intelijen ancaman siber (cyber threat intelligence sharing) secara waktu nyata (real-time), sehingga aparat penegak hukum Indonesia memiliki kewenangan yang diakui untuk melumpuhkan infrastruktur penipuan di negara tetangga tanpa hambatan birokrasi diplomatik yang berlarut-larut.

Di ranah domestik, kompleksitas pemberantasan kejahatan ini semakin diperparah oleh fragmentasi otoritas yang menangani kejahatan berbasis finansial digital. Sebagaimana dianalisis oleh Pitaloka (2022) mengenai pertentangan antara UU ITE dengan Undang-Undang Transfer Dana, para pelaku penipuan sangat memahami celah regulasi ini dan memanfaatkannya dengan memecah aliran dana hasil kejahatan ke dalam puluhan rekening perantara (money mules) hingga mengubahnya menjadi aset kripto dalam hitungan menit. Pendekatan problem-solving untuk mengatasi disharmoni regulasi ini adalah dengan membentuk Satuan Tugas Gabungan Intelijen Finansial Siber. Satgas ini mengintegrasikan penyidik siber dari Kepolisian, analis Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK), serta pengawas Otoritas Jasa Keuangan (OJK) dalam satu komando operasional (single command center). Satgas ini harus diberikan kewenangan eksekutif melalui Peraturan Presiden untuk melakukan intervensi langsung terhadap sistem perbankan dan bursa kripto, memungkinkan pembekuan aset digital secara instan berdasarkan algoritma kecurigaan transaksi (suspicious transaction logic), mengesampingkan sementara prosedur normal administrasi perbankan demi menyelamatkan kerugian ekonomi masyarakat.

Langkah operasional yang agresif di atas tentu membutuhkan fondasi hukum pidana materil yang solid dan tidak multitafsir. Namun, kebijakan formulasi pidana dalam UU ITE yang ada saat ini dinilai tidak cukup adaptif terhadap mutasi genetik kejahatan siber modern (Suharto et al., 2022). Kelemahan formulasi ini melahirkan anomali yurisprudensi di mana aparat penegak hukum memiliki ruang diskresi yang terlalu lebar akibat eksistensi pasal-pasal karet yang melanggar asas kejelasan rumusan hukum (Tan, 2022). Untuk menyelesaikan polemik ketidakpastian hukum ini secara permanen, pembuat undang-undang harus menerapkan pendekatan *regulatory sandbox* dalam pembaruan delik pidana

siber. Alih-alih merumuskan instrumen hukum yang statis, UU ITE harus dilengkapi dengan lampiran teknis (technical annex) yang dapat diperbarui secara periodik melalui Peraturan Menteri, tanpa harus melalui proses revisi undang-undang di parlemen yang memakan waktu bertahun-tahun. Lampiran teknis ini akan merinci secara spesifik parameter forensik dari setiap modus penipuan baru, sehingga asas legalitas tetap terpenuhi, sementara hukum tetap memiliki fleksibilitas untuk mengejar ketertinggalannya dari teknologi.

Ketidakpastian linguistik hukum juga menjadi batu sandungan teknis di persidangan, khususnya terkait definisi operasional dari tindak pidana itu sendiri. Oktabiantoro dan Wulan (2024) menyoroti fatalnya ketidakjelasan frasa "mentransmisikan" yang sering kali gagal membedakan antara tindakan transmisi yang digerakkan oleh niat jahat manusia (human-intent transmission) dan transmisi otomatis yang dilakukan oleh sistem atau perangkat lunak (machine-generated transmission). Solusi praktis untuk kelemahan ini adalah kewajiban penyertaan ahli linguistik forensik komputasional dalam setiap pembuatan Berita Acara Pemeriksaan (BAP) kasus penipuan daring. Lebih jauh, Pedoman Penuntutan dari Kejaksaan Agung harus direvisi untuk mewajibkan pembuktian *mens rea* (niat jahat) berbasis analisis kode sumber (source code analysis) atau analisis jejak log peladen (server log), guna memastikan bahwa pihak yang didakwa benar-benar merupakan dalang di balik transmisi data palsu tersebut, bukan sekadar perangkat pasif yang terinfeksi *malware* atau pihak ketiga yang diretas.

Efisiensi penegakan hukum juga sangat bergantung pada alokasi sumber daya. Publik telah lama menyoroti disorientasi penegakan hukum UU ITE yang lebih berat sebelah pada penanganan kasus-kasus defamasi ketimbang kejahatan ekonomi siber. Tinjauan yuridis mengenai tindak pidana pencemaran nama baik yang terus membebani sistem peradilan pidana membuktikan adanya krisis prioritas (Zhafira et al., 2023). Ekuivalensi semu antara pelindungan nama baik dan pemberantasan kejahatan siber telah menguras energi institusional aparat (Rauf et al., 2025). Tindakan perbaikan yang harus segera diimplementasikan adalah penerapan Matriks Prioritas Penanganan Perkara (Case Prioritization Matrix) di tingkat Badan Reserse Kriminal Polri. Matriks ini mewajibkan penolakan atau pengalihan jalur penyelesaian di luar pengadilan (non-litigasi) untuk kasus-kasus penghinaan ringan di internet, guna memastikan bahwa 80% kuota anggaran dan tenaga penyidik siber nasional dikhususkan secara paksa (mandatory allocation) untuk

membongkar jaringan penipuan daring, judi daring, dan kejahatan siber finansial lainnya yang menimbulkan kerugian ekonomi riil.

Pembenahan di sektor hilir (penegakan hukum) ini mutlak harus diimbangi dengan reformasi struktural di sektor hulu, yakni pada ekosistem perdagangan elektronik itu sendiri. Aji (2022) menegaskan urgensi harmonisasi UU Perlindungan Konsumen dengan UU ITE untuk menciptakan transaksi jual beli daring yang aman. Namun, imbauan saja tidak cukup. Platform *e-commerce* dan media sosial tidak boleh lagi berlindung di balik status mereka sebagai sekadar "penyedia perantara". Pemerintah melalui Kementerian Perdagangan dan Kementerian Komunikasi dan Digital harus mewajibkan implementasi *Escrow System* (rekening penampung bersama) yang dikelola oleh negara atau lembaga independen bersertifikasi untuk seluruh platform transaksi daring tingkat menengah ke bawah. Selain itu, regulasi harus memaksa platform penyelenggara sistem elektronik untuk menyediakan asuransi siber wajib (mandatory cyber insurance) yang preminya dibebankan pada biaya operasional platform, bukan konsumen. Jika terjadi penipuan akibat kegagalan platform dalam memfilter pelapak (merchant) fiktif, asuransi inilah yang akan langsung mengeksekusi ganti rugi kepada korban tanpa proses pengadilan yang panjang.

Pada akhirnya, pelindungan hukum yang paling efektif adalah pelindungan yang berbasis pada kesadaran kolektif masyarakat. Kurniawan et al. (2025) menemukan bahwa persepsi publik, khususnya mahasiswa, terhadap peran perlindungan UU ITE masih sangat rendah. Hal ini mengindikasikan bahwa instrumen hukum positif gagal menciptakan rasa aman secara psikologis. Oleh karena itu, pendekatan hukum harus diekspansi menjadi rekayasa sosial berskala besar. Pemerintah harus mewajibkan integrasi kurikulum "Keamanan Forensik Digital Dasar" (Basic Digital Forensic Security) mulai dari tingkat pendidikan menengah, tidak lagi sekadar mengajarkan literasi digital mengenai cara menggunakan internet, tetapi melatih kepekaan analitis masyarakat dalam membedah manipulasi psikologis (*social engineering*) dan verifikasi otentikasi data transaksi.

Infrastruktur keterbukaan informasi juga harus dimobilisasi sebagai senjata pertahanan pasif. Menilik studi komparasi mengenai undang-undang kearsipan dan keterbukaan informasi publik yang dilakukan Winastwan (2022), asas transparansi data harus diubah menjadi sistem peringatan dini berbasis komunitas (community-based early warning system). Pemerintah harus merilis *Dashboard* Ancaman Siber Nasional berbasis aplikasi

yang bersifat *open-data*, di mana masyarakat dapat melacak rekam jejak kriminalitas sebuah nomor telepon, tautan *e-commerce*, atau rekening bank secara instan (real-time). Melalui konvergensi antara perbaikan klausul delik pidana, realokasi prioritas penegakan hukum dari defamasi ke penipuan, pemaksaan tanggung jawab mutlak bagi platform niaga, serta demokratisasi data ancaman siber, kelemahan sistemik dalam UU ITE dapat ditambal secara komprehensif, mentransformasikan regulasi ini dari sekadar instrumen penghukum menjadi ekosistem pelindungan yang proaktif dan presisi.

Lebih jauh dalam mengurai anatomi kegagalan pencegahan penipuan daring, pendekatan penegakan hukum siber di Indonesia saat ini terjebak pada paradigma pemidanaan klasik yang berorientasi pada penghukuman badan (retributif), alih-alih berfokus pada pemulihan kerugian ekonomi (restitutif). Kebijakan formulasi pidana dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), sebagaimana dianalisis secara kritis oleh Suharto, Parulian, dan Achmad (2022), masih menempatkan pidana penjara sebagai instrumen utama atau *ultimum remedium*. Paradigma ini sangat tidak relevan untuk menindak kejahatan kerah putih digital seperti penipuan daring, di mana motivasi tunggal para pelaku adalah akumulasi kekayaan secara ilegal. Penangkapan operator tingkat bawah dari sebuah sindikat penipuan tidak akan menghentikan operasi kejahatan tersebut jika aliran dana dan infrastruktur keuangannya tidak dilumpuhkan. Kelemahan ini semakin nyata ketika dihadapkan pada tumpang tindih regulasi yang dikaji oleh Pitaloka (2022) mengenai pertentangan antara UU ITE dan Undang-Undang Transfer Dana. Ketidakmampuan instrumen hukum siber untuk melakukan penetrasi ke dalam sistem perbankan secara langsung memberikan jeda waktu (*golden time*) bagi pelaku untuk mencuci uang hasil kejahatan. Sebagai solusi pemecahan masalah (problem-solving) yang radikal, pemerintah harus mengintegrasikan mekanisme perampasan aset perdata (*non-conviction based asset forfeiture*) ke dalam revisi UU ITE. Mekanisme ini memungkinkan negara untuk menyita dan membekukan aset digital atau rekening bank yang terindikasi kuat sebagai hasil kejahatan penipuan tanpa harus menunggu putusan pidana yang berkekuatan hukum tetap (inkracht) terhadap pelakunya.

Keberhasilan implementasi mekanisme pelacakan dan perampasan aset digital ini sangat bergantung pada rasionalisasi alokasi sumber daya di lembaga penegak hukum. Efektivitas penindakan kejahatan siber ekonomi terus tergerus oleh beban perkara dari delik-

delik aduan personal. Rauf, Ahamd, dan Moha (2025) menyoroti bahwa pasca revisi UU ITE, ruang perdebatan hukum masih didominasi oleh ekuivalensi antara kebebasan berekspresi dan perlindungan nama baik. Sinkronisasi tindak pidana pencemaran nama baik dalam KUHP dengan Pasal 27 Ayat (3) UU ITE, seperti yang ditelaah oleh Zhafira, Ismansyah, dan Yoserwan (2023), secara nyata telah mengalihkan fokus esensial aparatur negara. Laboratorium forensik digital Polri dan jaksa penuntut umum menghabiskan ribuan jam kerja untuk membuktikan unsur penghinaan dalam sengketa verbal di media sosial, sementara kasus penipuan investasi bodong daring yang merugikan masyarakat triliunan rupiah terhenti karena alasan "kurangnya alat bukti digital" atau "keterbatasan personel ahli". Untuk memutus rantai inefisiensi ini, Mahkamah Agung dan Kejaksaan Agung harus menerbitkan pedoman penuntutan yang mengikat, yang secara mutlak mendelegasikan seluruh kasus defamasi ringan ke jalur mediasi penal atau gugatan perdata murni. Depenalisasi de facto pada pasal-pasal defamasi ini merupakan rekayasa tata kelola institusional yang wajib dilakukan agar anggaran dan kapasitas teknis negara dapat dimobilisasi secara eksklusif untuk memburu sindikat penipuan daring.

Tantangan berikutnya yang membutuhkan intervensi segera adalah modernisasi penafsiran linguistik hukum dalam menghadapi teknologi kecerdasan buatan (AI) dan otomasi. Ambiguasi norma dalam UU ITE tidak hanya berkisar pada status "pasal karet" yang melanggar asas kejelasan rumusan (Tan, 2022), tetapi juga pada kegagapan hukum positif dalam mendefinisikan subjek pelaksana (eksekutor) kejahatan. Oktabiantoro dan Wulan (2024) menemukan bahwa ketidakjelasan makna "mentransmisikan" dalam Pasal 28 Ayat 2 UU ITE menjadi titik lemah di persidangan. Penipuan daring masa kini tidak lagi mengandalkan manusia untuk mengetik dan mengirim pesan secara manual. Sindikat menggunakan bot otomatis dan skrip AI untuk melakukan *crawling* data korban dan mengirimkan jutaan tautan *phising* secara serentak. Jika hukum masih menginterpretasikan frasa "mentransmisikan" sebagai tindakan fisik manusia secara langsung, maka pembuat atau pengendali bot tersebut dapat lolos dari jerat hukum dengan dalih sistem yang bekerja secara otonom. Penyelesaian taktis untuk celah ini adalah dengan memperluas definisi "mentransmisikan" dalam bagian penjelasan UU ITE untuk mencakup "tindakan memprogram, mengoperasikan, menyewakan, atau menyediakan instruksi komputasi otomatis (algoritma) yang secara sistematis mendistribusikan informasi elektronik

bermuatan manipulasi atau penipuan". Melalui redefinisi ini, pertanggungjawaban pidana dapat ditarik ke hulu, menjerat peretas pembuat perangkat lunak jahat (*malware creator*) dan pemilik server proksi.

Pergeseran fokus hukum ke arah pencegahan (preventif) juga menuntut perubahan drastis dalam tata kelola perlindungan konsumen di sektor perdagangan elektronik. Aji (2022) menekankan bahwa integrasi UU Perlindungan Konsumen dan UU ITE sangat krusial. Kenyataannya, posisi konsumen tetap lemah karena arsitektur bisnis platform *e-commerce* dan media sosial di Indonesia masih berlindung di balik doktrin *safe harbor*, di mana penyelenggara platform melepaskan diri dari tanggung jawab atas konten atau transaksi penipuan yang dilakukan oleh pengguna di dalam ekosistemnya. Pendekatan ini harus diakhiri dengan memberlakukan doktrin Tanggung Jawab Mutlak Proporsional (*Proportional Strict Liability*) bagi penyelenggara sistem elektronik. Jika sebuah platform mengambil keuntungan finansial berupa biaya layanan, komisi transaksi, atau pendapatan iklan dari akun yang terbukti melakukan penipuan, maka platform tersebut harus ditetapkan sebagai pihak yang turut bertanggung jawab secara perdata untuk memulihkan kerugian korban. Regulasi harus mewajibkan platform untuk menerapkan sistem *Algorithmic Accountability*, di mana algoritma rekomendasi mereka harus diaudit secara berkala oleh otoritas siber independen untuk memastikan sistem tersebut tidak secara tidak sengaja mempromosikan atau menaikkan peringkat *merchant* fiktif yang menggunakan manipulasi ulasan palsu (*fake reviews*).

Di sisi lain, arsitektur keamanan siber nasional tidak dapat dibangun semata-mata dengan memperbanyak ancaman hukuman. Efektivitas implementasi UU ITE sebagaimana yang disoroti oleh Aprilianti (2025) akan selalu menemui jalan buntu jika budaya keamanan digital masyarakat masih rendah. Hal ini terkonfirmasi oleh evaluasi persepsi mahasiswa dalam kajian Kurniawan et al. (2025), yang memandang bahwa UU ITE belum secara konkret memberikan perisai edukatif yang mampu meningkatkan resiliensi publik. Solusi dari masalah ini adalah merombak ekosistem keterbukaan informasi. Mengadopsi prinsip dasar tata kelola informasi publik dari analisis Winastwan (2022), pemerintah harus menghapus tabir kerahasiaan perbankan secara spesifik dan bersyarat untuk kasus penipuan siber. Saat ini, korban penipuan sering kali kesulitan melacak identitas pelaku karena bank menolak membuka data pemilik rekening penampung dengan alasan kerahasiaan perbankan.

Pemerintah harus merumuskan protokol *Open-Data Anti Fraud* (Data Terbuka Anti-Penipuan) di mana nomor rekening, dompet digital, dan nomor telepon seluler yang telah dilaporkan lebih dari tiga kali dengan bukti awal yang sah ke portal pengaduan nasional, statusnya akan dicabut dari perlindungan kerahasiaan identitas. Data tersebut harus langsung diintegrasikan secara terbuka ke dalam semua sistem perbankan nasional, sehingga transaksi yang ditujukan ke rekening tersebut akan secara otomatis memicu peringatan (pop-up warning) "TERINDIKASI PENIPUAN" di layar ponsel calon korban sebelum mereka memasukkan PIN persetujuan transfer.

Sinergi antara modernisasi delik pidana yang menghilangkan pasal karet (Tan, 2022), dekriminalisasi defamasi demi optimalisasi sumber daya siber (Zhafira et al., 2023; Rauf et al., 2025), penegasan kewajiban pengawasan oleh platform niaga daring (Aji, 2022), hingga pembaruan definisi teknis transmisi digital (Oktabiantoro & Wulan, 2024; Suharto et al., 2022) merupakan satu kesatuan solusi arsitektur hukum yang utuh. Pengintegrasian seluruh elemen ini dengan sistem keterbukaan intelijen siber lintas lembaga (Pitaloka, 2022; Winastwan, 2022) akan mengubah wajah UU ITE. Regulasi ini tidak lagi akan dipandang secara skeptis oleh masyarakat akademis dan publik luas (Kurniawan et al., 2025), melainkan akan bertransformasi menjadi instrumen hukum siber yang memiliki daya prediktif dan ketahanan tinggi (Aprilianti, 2025) dalam menekan ruang gerak sindikat penipuan daring, sekaligus melindungi kedaulatan ekonomi digital masyarakat Indonesia di masa depan.

KESIMPULAN DAN SARAN

Jadi, berdasarkan analisis komprehensif yang telah dilakukan, dapat disimpulkan bahwa Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) saat ini belum sepenuhnya efektif dalam menekan angka kejahatan siber berbasis penipuan daring. Inefektivitas ini berakar pada kelemahan formulasi delik pidana yang tertinggal oleh kemajuan teknologi, ambiguitas leksikal pada pasal-pasal krusial, tumpang tindih yurisdiksi dengan regulasi sektor keuangan, serta disorientasi penegakan hukum yang terlalu memprioritaskan penyelesaian sengketa interpersonal berupa pencemaran nama baik. Sebagai solusi pemecahan masalah yang taktis, pemerintah harus segera merekonstruksi arsitektur hukum siber nasional. Langkah ini mencakup realokasi sumber daya aparat penegak hukum untuk difokuskan secara eksklusif pada pembongkaran sindikat kejahatan

finansial, yang dapat dicapai melalui penerapan keadilan restoratif pada kasus defamasi ringan. Lebih lanjut, diperlukan intervensi regulasi yang mengikat penyelenggara platform digital dengan pertanggungjawaban mutlak proporsional (strict liability), serta perumusan mekanisme pelacakan dan pembekuan aset digital (auto-freeze) lintas lembaga yang cepat tanpa hambatan birokrasi perbankan konvensional. Melalui sinkronisasi regulasi sektoral, pembentukan basis data ancaman siber terintegrasi, dan peningkatan literasi forensik digital publik, UU ITE dapat ditransformasikan dari instrumen pidana yang reaktif-retributif menjadi payung hukum preventif-restitutif yang secara nyata melindungi kedaulatan finansial dan memulihkan kerugian masyarakat di ruang siber.

DAFTAR PUSTAKA

Aji, H. B. (2022). PENGATURAN JUAL BELI SECARA ONLINE BERDASARKAN UNDANG-UNDANG PERLINDUNGAN KONSUMEN DAN UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK. *Jurnal Hukum Progresif*, *10*(1). https://doi.org/10.14710/jhp.10.1.12-24

Aprilianti, A. (2025). Efektivitas dan Implementasi Undang-Undang Informasi dan Transaksi Elektronik sebagai Hukum Siber di Indonesia: Tantangan dan Solusi. *Begawan Abioso*, *15*(1). https://doi.org/10.37893/abioso.v15i1.1002

Dicky Andika Rauf, Ahamd, & Moh. Rivaldi Moha. (2025). Ekuivalensi Kebebasan Berekspresi dan Perlindungan Nama Baik Pasca Perubahan Undang-Undang Informasi dan Transaksi Elektronik. *Al-Zayn : Jurnal Ilmu Sosial & Hukum*, *3*(2). https://doi.org/10.61104/alz.v3i2.1104

Kurniawan, R. A., Suryaningsi, S., Handayani, N. F., Pardosi, J., & Herliah, E. (2025). Tinjauan Hukum terhadap Peran Undang-Undang Informasi dan Transaksi Elektronik menurut Persepsi Mahasiswa. *Nomos : Jurnal Penelitian Ilmu Hukum*, *5*(2). https://doi.org/10.56393/nomos.v5i2.3156

Oktabiantoro, D., & Evi Retno Wulan. (2024). KETIDAKJELASAN MAKNA "MENTRANSMISIKAN" PASAL 28 AYAT 2 UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK REVISI KEDUA. *IBLAM LAW REVIEW*, *4*(1). https://doi.org/10.52249/ilr.v4i1.307

Pitaloka, E. D. A. (2022). PERTENTANGAN UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK DENGAN UNDANG-UNDANG TRANSFER DANA

DALAM PERDAGANGAN BERJANGKA KOMODITI BERBASIS INTERNET. *Jurnal Yuridis*, *8*(2). https://doi.org/10.35586/jyur.v8i2.2831

Suharto, H., Parulian, S., & Achmad, R. (2022). Kebijakan Formulasi Hukum Pidana Pasal 27 Ayat (1) Undang-Undang Informasi Dan Transaksi Elektronik. *Lex LATA*, *2*(2). https://doi.org/10.28946/lexl.v2i2.831

Tan, K. (2022). ANALISA PASAL KARET UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK TERHADAP ASAS KEJELASAN RUMUSAN. *Jurnal Hukum Samudra Keadilan*, *17*(1). https://doi.org/10.33059/jhsk.v17i1.3376

Winastwan, R. E. (2022). Studi Komparasi Terhadap Undang-Undang Kearsipan Dan Undang-Undang Keterbukaan Informasi Publik. *Al-Ma Mun Jurnal Kajian Kepustakawanan Dan Informasi*, *3*(1). https://doi.org/10.24090/jkki.v3i1.6148

Zhafira, I., Ismansyah, I., & Yoserwan, Y. (2023). Tinjauan Yuridis Tindak Pidana Pencemaran Nama Baik Dalam Kitab Undang-undang Hukum Pidana Dikaitkan dengan Pasal 27 Ayat (3) Undang-undang Informasi dan Transaksi Elektronik. *Unes Journal of Swara Justisia*, *7*(3). https://doi.org/10.31933/ujsj.v7i3.408.