ASAS LEGALITAS DAN TREN PENINGKATAN KEJAHATAN SIBER DI INDONESIA: KAJIAN HUKUM EMPIRIS BERBASIS STATISTIK DESKRIPTIF

Candra niko[1], Hery Chariansyah[2]
[12]Program Magister Hukum, Universitas Krisnadwipayana, Jakarta, Indonesia
Alamat e-mail: Candranikotogatorop@gmail.com

ABSTRACT

The rapid development of information technology constantly introduces new cybercrime modi operandi, challenging the boundaries and implementation of the legality principle in Indonesian criminal law. This study aims to map the characteristics of rising cybercrime trends and critically analyze the limitations of the legality principle in addressing these developments. The research employs an empirical legal method with a sociological jurisprudence approach. Descriptive statistical analysis is applied to the statistical recapitulation of public reports throughout 2025, accessed via the Cyber Crime Investigation Portal of the Indonesian National Police (Polri) on June 20, 2026. The findings indicate a significant upward trend in cybercrime reports, with online fraud emerging as the most reported category (39.9%), followed by cyber-extortion/threats (23.7%), and online defamation (18.1%). The legal implications of these data trends show that rigid adherence to the principles of lex scripta, lex certa, and lex stricta within the formal legality framework potentially risks creating a legal vacuum or statutory limitations when facing fast-paced technological shifts. This study suggests a necessary reorientation of the legislative formulations toward a more adaptive approach while firmly upholding the fundamental principle of legal certainty.

Keywords: *Legality Principle; Cybercrime; Descriptive Statistics; Empirical Legal Method; IT Law.*

ABSTRAK

Perkembangan teknologi informasi secara konstan memunculkan modus operandi kejahatan siber baru yang memberikan tantangan bagi keterbatasan implementasi asas legalitas hukum pidana di Indonesia. Penelitian ini bertujuan untuk memetakan karakteristik tren peningkatan kejahatan siber dan menganalisis keterbatasan implementasi asas legalitas dalam menghadapi perkembangan tersebut. Metode penelitian yang digunakan adalah yuridis empiris dengan pendekatan sosiologi hukum. Analisis statistik deskriptif diterapkan pada rekapitulasi statistik laporan masyarakat sepanjang tahun 2025 yang diakses melalui Portal Patroli Siber Kepolisian Republik Indonesia (Polri) pada tanggal 20 Juni 2026. Hasil penelitian berbasis statistik deskriptif menunjukkan adanya tren peningkatan volume laporan kejahatan siber, dengan penipuan online sebagai kategori yang paling banyak dilaporkan (39,9%), diikuti oleh ancaman kekerasan (23,7%), dan pencemaran nama baik (18,1%). Implikasi hukum dari temuan data menunjukkan bahwa pembatasan pada prinsip lex scripta, lex certa, dan lex stricta dalam asas legalitas formal berpotensi menimbulkan kekosongan hukum atau keterbatasan pengaturan hukum terhadap dinamika teknologi mutakhir. Studi ini merekomendasikan perlunya pembaharuan hukum pidana materiil nasional yang adaptif terhadap teknologi informasi dengan tetap mempertahankan prinsip kepastian hukum.

Kata Kunci: *Asas Legalitas; Kejahatan Siber; Statistik Deskriptif; Yuridis Empiris; UU ITE.*

A. Pendahuluan

Transformasi digital telah mengubah pola interaksi masyarakat sekaligus meningkatkan risiko terjadinya kejahatan siber (*cybercrime*) baik pada skala global maupun nasional (BSSN, 2024). Gejala kriminalitas di ruang siber ini merefleksikan pergeseran lokus kejahatan konvensional menuju medium digital yang bersifat lintas batas. Sebagai salah satu negara dengan jumlah pengguna internet terbesar di Asia Tenggara, Indonesia menghadapi tantangan nyata berupa kerentanan infrastruktur digital yang memicu maraknya tindak pidana komputer. Ruang siber yang berkembang dinamis, asimetris, dan tanpa batas geografis memfasilitasi perkembangan delik-delik baru yang melampaui batas yurisdiksi hukum negara.

Berdasarkan data publik resmi dari Portal Patroli Siber Kepolisian Republik Indonesia (Polri), grafik laporan masyarakat menunjukkan tren kenaikan volume perkara yang signifikan dalam beberapa periode terakhir (Patroli Siber Polri, 2024). Data statistik deskriptif dari portal tersebut menempatkan penipuan online sebagai kategori yang paling banyak dilaporkan oleh masyarakat, diikuti oleh perkara pengancaman secara digital serta penyebaran konten ilegal. Kuantitas tindak pidana siber di Indonesia bertransformasi menjadi permasalahan sistemik yang menyasar hak kebendaan, reputasi sosial, serta privasi warga negara secara masif. Karakteristik kuantitatif ini menunjukkan bahwa ruang digital di Indonesia memerlukan perhatian khusus dari aspek penegakan hukum pidana guna mengimbangi intensitas kriminalitas yang terjadi.

Di sisi lain, arsitektur penegakan hukum pidana materil di Indonesia secara dogmatis bersandar pada Asas Legalitas yang dikodifikasikan dalam Pasal 1 ayat (1) Kitab Undang-Undang Hukum Pidana (KUHP) Lama serta UU No. 1 Tahun 2023 (KUHP Baru). Asas ini menekankan pilar hukum tertulis (*lex scripta*), rumusan delik yang jelas (*lex certa*), dan penafsiran yang ketat (*lex stricta*) (Andi Hamzah, 2022; Moeljatno, 2015). Doktrin *nullum delictum nulla poena sine praevia lege poenali* ini berfungsi menjaga agar penegakan hukum tetap berjalan dalam koridor kepastian hukum (*rechtszekerheid*) sekaligus melindungi hak asasi individu dari tindakan sewenang-wenang (Pujiyono & Azhar, 2022). Konsekuensi logis dari doktrin formal ini adalah larangan penggunaan analogi dalam mengadili suatu perbuatan pidana yang belum diatur oleh undang-undang (Pahlevi, 2022). Prinsip ini menuntut bahwa ketertiban hukum tidak boleh ditegakkan dengan melanggar batasan teks undang-undang tertulis, sekalipun perbuatan tersebut merugikan masyarakat.

Permasalahan yuridis muncul ketika rigiditas prinsip *lex scripta* dan *lex certa* berhadapan langsung dengan karakteristik kejahatan siber yang bersifat cair, tidak berwujud (*immaterial*), dan berubah secara cepat (Brenner, 2007). Penegak hukum dihadapkan pada situasi kekosongan hukum atau keterbatasan aturan hukum ketika terdapat perbuatan kejahatan siber jenis baru yang merugikan kepentingan hukum masyarakat, namun teks undang-undang belum memberikan rumusan delik yang eksplisit untuk menjeratnya (Sjawie, 2023). Hal ini melahirkan kesenjangan antara kebutuhan

sosiologis akan keadilan substansial dengan tuntutan doktrinal akan kepastian hukum formal.

Beberapa penelitian terdahulu telah mengkaji dinamika penegakan hukum kejahatan siber ini. Studi oleh Pujiyono dan Azhar (2022) menitikberatkan analisisnya pada aspek normatif rekonstruksi teoritis reorientasi asas legalitas materiil untuk mengatasi ketertinggalan legislasi. Sementara itu, riset sosiologis oleh Santoso (2023) mengamati efektivitas penegakan hukum dari dimensi kapasitas personel serta hambatan penyidik kepolisian di lapangan. Meskipun demikian, terdapat kesenjangan penelitian (*research gap*) dari literatur terdahulu yang cenderung berorientasi normatif-doktrinal murni sehingga belum memanfaatkan data kuantitatif dari portal resmi penegak hukum sebagai instrumen evaluasi implementasi pilar-pilar asas legalitas secara nyata.

Berbeda dengan penelitian terdahulu yang murni menggunakan pendekatan doktrinal kaku atau struktural kepolisian, penelitian ini mengintegrasikan analisis hukum dengan statistik deskriptif berdasarkan data riil Portal Patroli Siber Polri. Kontribusi utama penelitian ini terletak pada pemanfaatan rekapitulasi data empiris makro nasional sebagai alat uji kritis terhadap kapasitas aplikatif pilar *lex scripta*, *lex certa*, dan *lex stricta*. Melalui integrasi interdisipliner ini, penelitian tidak hanya menguraikan kelemahan teks undang-undang, melainkan membuktikan secara empiris titik sumbat penegakan hukum akibat benturan dogma, sekaligus menawarkan pembaruan kebijakan kriminal yang adaptif. Penelitian ini bertujuan untuk memetakan tren kejahatan siber di Indonesia menggunakan statistik deskriptif, serta menganalisis secara kritis keterbatasan implementasi asas legalitas dalam menghadapi perkembangan modus operandi baru kejahatan siber di ruang digital.

B. Metode Penelitian

Penelitian ini menerapkan metode penelitian hukum empiris (yuridis empiris) yang mengkaji bekerjanya hukum di dalam realitas sosial masyarakat (Soekanto, 2019). Pendekatan penelitian yang digunakan adalah pendekatan sosiologi hukum (*sociological jurisprudence*) guna mengamati relevansi norma hukum positif tertulis terhadap penanganan fenomena kejahatan di lapangan (Setiadi, 2021). Fokus utama pendekatan ini diarahkan untuk mengidentifikasi ada atau tidaknya kesenjangan (*gap*) antara hukum dalam teks (*law in books*) dengan hukum dalam tindakan (*law in action*) di tengah maraknya kriminalitas ruang siber.

Sumber data dalam penelitian ini secara khusus menggunakan bahan hukum sekunder dan data empiris sekunder. Bahan hukum sekunder bersumber dari peraturan perundang-undangan pidana, seperti KUHP, UU ITE, serta literatur hukum terkait asas legalitas. Data empiris sekunder berupa data kuantitatif laporan aduan masyarakat diperoleh melalui rekapitulasi data publik pada Portal Resmi Statistik Laporan Masyarakat Patroli Siber Kepolisian Republik Indonesia (Polri) (Patroli Siber Polri, 2024). Penggunaan data empiris sekunder ini memberikan jaminan akurasi karena bersumber langsung dari pencatatan satu pintu yang dikelola dan divalidasi oleh Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri.

Teknik pengambilan sampel yang diterapkan dalam penelitian ini adalah teknik sampling total (*total sampling*) atau metode sensus (Sugiyono, 2020). Berdasarkan metode ini, peneliti menjadikan seluruh data populasi laporan kejahatan siber nasional yang tercatat sepanjang tahun kalender 2025 sebagai objek analisis, tanpa melakukan pengurangan sampel atau generalisasi parsial. Teknik pengumpulan data dilakukan melalui kombinasi antara studi dokumentasi dan studi kepustakaan. Studi dokumentasi dilakukan dengan cara mengamati dan mengunduh dasbor rekapitulasi statistik resmi laporan masyarakat tahun 2025 pada Portal Patroli Siber Polri yang diakses pada tanggal 20 Juni 2026. Sementara itu, studi kepustakaan dijalankan dengan menelaah buku teks, artikel jurnal terakreditasi, dan naskah regulasi yang berkaitan dengan dogmatika hukum pidana.

Teknik analisis data dalam penelitian ini sepenuhnya bersandarkan pada analisis statistik deskriptif menggunakan perangkat lunak Microsoft Excel (Sugiyono, 2020). Data laporan kejahatan siber diolah ke dalam bentuk distribusi frekuensi dan persentase proporsi kumulatif guna menyajikan visualisasi data yang objektif dan sistematis. Selanjutnya, tahapan analisis hukum sekunder dijalankan menggunakan metode penalaran hukum (*legal reasoning*) secara kualitatif (Marzuki, 2022). Hasil pengolahan angka statistik deskriptif tersebut digunakan sebagai basis pembuktian empiris untuk mengevaluasi bekerjanya pilar *lex scripta*, *lex certa*, dan *lex stricta* dalam memayungi fenomena kriminalitas siber kontemporer.

C. Hasil Penelitian dan Pembahasan

A. Karakteristik Tren Kejahatan Siber di Indonesia Berdasarkan Data Patroli Siber Polri

Analisis terhadap data sekunder resmi yang bersumber dari Portal Laporan Masyarakat Patroli Siber Kepolisian Republik Indonesia (Polri) menunjukkan pemusatan persebaran perkara yang signifikan. Guna memahami dinamika kriminalitas di ruang digital secara komprehensif, pengolahan statistik deskriptif dilakukan terhadap akumulasi laporan masyarakat untuk menyajikan visualisasi sebaran frekuensi, proporsi, serta interpretasi distribusi data yang otentik.

Tabel 1. Distribusi Kategori Kejahatan Siber Tahun 2025

No	Kategori Kejahatan Siber	Jumlah Laporan Polisi (Absolut)	Proporsi Data (%)	Tahun Data	Keterangan Sumber
1	Penipuan Online	14.496	39,9%	2025	Laporan Terverifikasi
2	Ancaman Kekerasan	8.614	23,7%	2025	Laporan Terverifikasi
3	Pencemaran Nama Baik	6.556	18,1%	2025	Laporan Terverifikasi
4	Ancaman Pencemaran	3.675	10,1%	2025	Laporan Terverifikasi

5	Kategori Lainnya	2.880	8,2%	2025	Laporan Kombinasi
	Total Seluruh Kasus	**36.221**	**100%**		**Akumulasi Riil Nasional**

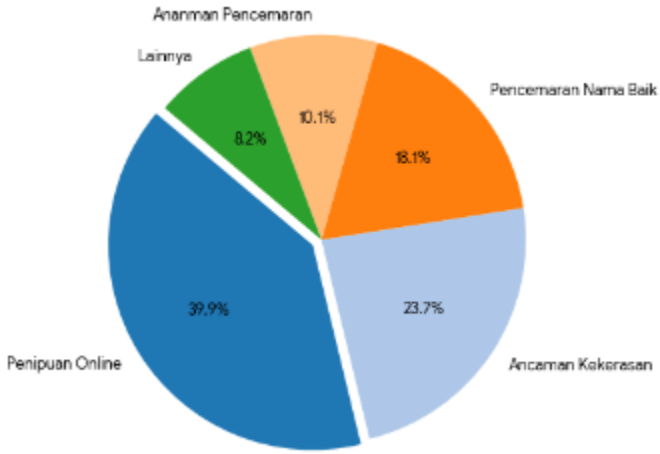
Sumber: Data Sekunder Diolah dari Portal Resmi Statistik Laporan Masyarakat Patroli Siber Polri (Diakses pada 20 Juni 2026) [14]

Interpretasi Distribusi Data dan Proporsi Tiap Kategori

Berdasarkan visualisasi kuantitatif pada Tabel 1, distribusi perkara menempatkan klaster penipuan online sebagai kategori yang paling banyak dilaporkan oleh masyarakat Indonesia. Kategori ini mencakup proporsi data sebesar 39,9% dari total keseluruhan aduan, atau setara dengan 14.496 laporan polisi aktif. Tingginya proporsi ini mengindikasikan adanya kecenderungan dominasi tipe kejahatan siber yang menyasar sektor finansial dan hak milik pribadi. Klaster terbesar kedua ditempati oleh ancaman kekerasan atau pemerasan daring dengan angka 23,7% (8.614 laporan). Sektor aduan kemudian diikuti oleh pencemaran nama baik sebesar 18,1% (6.556 laporan), serta ancaman pencemaran atau perundungan siber sebesar 10,1% (3.675 laporan).

Apabila distribusi data ini dikelompokkan lebih lanjut, terlihat bahwa akumulasi dari kategori penipuan daring dan pemerasan daring mencakup lebih dari 60% total laporan perkara. Hal ini menggambarkan bahwa ruang siber di Indonesia didominasi oleh kejahatan ekonomi yang difasilitasi oleh komputer (*computer-enabled crime*). Modus operandi yang mengemuka di lapangan didominasi oleh pemanfaatan manipulasi psikologis atau rekayasa sosial (*social engineering*) guna mengeksploitasi kelengahan pengguna teknologi informasi. Karakteristik ini lebih dominan dibandingkan serangan teknis yang murni menyasar sistem komputer (*computer-dependent crime*).

Berikut adalah grafik proporsi persentase karakteristik kejahatan siber di Indonesia berdasarkan data rekapitulasi statistik tahun 2025:



Gambar 1. Proporsi Laporan Kasus Kejahatan Siber Tahun 2025
Sumber: Portal Patroli Siber Polri (2026) [14]

Kecenderungan Dominasi dan Implikasi Statistik

Secara statistik, kecenderungan dominasi ini membawa implikasi bahwa risiko viktimisasi kejahatan siber di Indonesia berkolerasi dengan aktivitas transaksi ekonomi digital sehari-hari. Tingginya angka penipuan dan pemerasan daring juga mencerminkan adanya ketimpangan literasi keamanan digital publik. Masyarakat sangat adaptif terhadap penggunaan platform teknologi finansial, perdagangan elektronik (*e-commerce*), dan dompet digital. Namun, adaptasi tersebut tidak dibarengi dengan proteksi data pribadi yang memadai. Akibatnya, data

kredensial publik menjadi komoditas eksploitatif bagi pelaku kriminal digital.

Implikasi statistik ini sekaligus menjadi indikator empiris bagi institusi penegak hukum bahwa beban penanganan perkara (*workload*) kepolisian saat ini terkonsentrasi pada delik-delik kerugian materiil. Tingginya jumlah laporan menunjukkan perlunya instrumen hukum pidana yang lebih adaptif terhadap perkembangan kejahatan siber. Ketersediaan aturan hukum yang jelas dan tidak multitafsir menjadi prasyarat utama. Kepastian regulasi diperlukan agar angka laporan masyarakat yang tinggi ini dapat ditindaklanjuti secara optimal pada tahap penyidikan hingga penuntutan di pengadilan. Jika sistem hukum formil tidak mampu mentransformasikan laporan kuantitatif ini menjadi berkas dakwaan yang solid akibat hambatan dogmatis, maka kepercayaan publik terhadap ekosistem digital dapat mengalami degradasi.

B. Implikasi Temuan Data terhadap Keterbatasan Doktrinal Asas Legalitas

Tingginya kuantitas laporan masyarakat di lapangan memicu permasalahan yuridis dalam tataran penegakan hukum pidana materil saat dihadapkan pada batas-batasan dogmatis asas legalitas. Guna membedah polemik ini secara komprehensif, analisis hukum dibagi ke dalam tiga dimensi utama yang melekat pada Pasal 1 ayat (1) KUHP, yaitu prinsip *lex scripta*, *lex certa*, dan *lex stricta*. Ketiga prinsip ini diuji relevansinya untuk melihat sinkronisasi antara norma tertulis kaku dengan realitas kejahatan siber yang bergerak cepat.

B.1 Prinsip Lex Scripta (Hukum Tertulis)

Prinsip *lex scripta* mewajibkan bahwa pemidanaan atas suatu perbuatan pidana harus didasarkan pada ketentuan hukum tertulis yang telah dikodifikasikan sebelum perbuatan tersebut terjadi (Andi Hamzah, 2022). Karakteristik hukum tertulis ini dirancang untuk menciptakan stabilitas hukum. Hukum pidana tidak memperkenankan adanya hukum kebiasaan atau norma tidak tertulis untuk dijadikan dasar menjatuhkan sanksi pidana.

Data kuantitatif pada Tabel 1 membuktikan bahwa klaster penipuan online mendominasi angka laporan nasional dengan proporsi 39,9% (14.496 laporan). Angka ini mengonfirmasi secara gambaran empiris keterbatasan pengaturan hukum tertulis. Sifat kejahatan siber yang asimetris membuat variasi modus operandi berkembang lebih cepat dibandingkan dengan ritme legislasi tertulis. Fenomena penipuan online ini dalam praktiknya berpotensi berkembang melalui penggunaan teknologi baru seperti pemalsuan suara (*voice cloning*) hingga manipulasi video rekayasa (*deepfake*). Ketika penegak hukum menerima laporan perkara dengan indikasi manipulasi canggih tersebut, teks tertulis dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) hasil perubahan kedua (UU No. 1 Tahun 2024) belum memuat klausul spesifik yang mendefinisikan delik otonom pemidanaan rekayasa kecerdasan buatan secara eksplisit.

Temuan ini memperkuat hasil penelitian hukum oleh Pujiyono dan Azhar (2022) yang menyatakan bahwa hukum tertulis nasional selalu mengalami ketertinggalan dalam merespons

kecepatan pembaruan teknologi informasi. Hal ini berbanding lurus dengan pandangan mengenai percepatan akselerasi digital (*technological acceleration*) yang kerap berada di luar jangkauan adaptasi hukum (Goodin, 2020). Keterikatan mutlak pada hukum tertulis membuat negara tidak dapat memberikan perlindungan hukum yang instan kepada korban kejahatan siber. Pembuatan undang-undang membutuhkan waktu rancangan legislasi yang lama, sementara variasi modus operandi digital berkembang sangat dinamis di internet. Akibatnya, pilar *lex scripta* berpotensi menimbulkan kesulitan penegakan hukum karena perbuatannya belum tertulis di dalam lembaran negara secara formal.

B.2 Prinsip Lex Certa (Rumusan Jelas)

Prinsip *lex certa* menuntut agar pembuat undang-undang merumuskan elemen-elemen perbuatan pidana secara jelas, spesifik, dan tidak multitafsir (Moeljatno, 2015). Kejelasan rumusan norma ini bertujuan agar masyarakat memahami batasan perilaku yang dilarang. Kejelasan ini sekaligus mencegah penyalahgunaan wewenang oleh aparat dalam menginterpretasikan hukum pidana. Syarat keterbukaan informasi hukum ini mengharuskan rumusan delik memiliki batasan yang tegas. Dalam konteks kejahatan siber, penerapan *lex certa* kerap kali terbentur pada penggunaan istilah teknis teknologi yang ambigu atau terlalu umum dalam pasal undang-undang (Setiadi, 2021).

Hubungan empiris pilar *lex certa* dengan data statistik terlihat nyata pada tingginya angka aduan pencemaran nama baik sebesar 18,1% (6.556 laporan) dan ancaman pencemaran sebesar 10,1% (3.675 laporan). Penumpukan kuantitas perkara pada dua sektor ini berakar dari kurangnya kepastian rumusan norma dalam pasal-pasal UU ITE yang menggunakan frasa elastis seperti "bermuatan penghinaan" atau "melanggar kesusilaan" (Wahyudi, 2023). Ketidakjelasan rumusan norma ini memicu tumpang tindih interpretasi di lapangan antara hak kebebasan berpendapat dengan perbuatan kriminal kejahatan siber.

Ketika rumusan delik tidak memiliki kepastian makna, efektivitas penegakan hukum terhadap angka kejahatan siber yang tinggi menjadi tidak terukur. Hasil analisis ini sejalan dengan argumen Situmeang (2021) yang menegaskan bahwa kekaburan norma dalam delik siber formal justru menurunkan kepastian hukum (*rechtszekerheid*). Sifat kejahatan siber yang cair membuat elemen perbuatan fisik (*actus reus*) dalam hukum konvensional menjadi kabur saat diaplikasikan di ruang digital, yang pada akhirnya memicu evolusi transisional atas sifat kejahatan itu sendiri (Wall, 2021). Rumusan delik yang kurang spesifik memaksa aparat untuk memilah-milah unsur perbuatan secara parsial. Hal ini membuktikan bahwa pemenuhan prinsip *lex certa* dalam regulasi siber nasional masih menghadapi kendala substansial. Hukum pidana nasional sering kali menggunakan terminologi hukum konvensional lama untuk mengadili realitas digital yang baru.

B.3 Prinsip Lex Stricta (Penafsiran Ketat)

Prinsip *lex stricta* menegaskan bahwa ketentuan hukum pidana harus ditafsirkan secara ketat dan secara tegas melarang penggunaan analogi (*analogieverbod*) dalam mengadili

suatu perbuatan yang belum diatur oleh undang-undang (Pahlevi, 2022). Larangan analogi ini merupakan pembatas yang menjaga agar penegak hukum tidak memperluas ruang lingkup hukum pidana secara subjektif demi memenuhi asas kepastian hukum. Tanpa adanya *lex stricta*, fungsi yudisial hakim akan bergeser menjadi fungsi legislatif, karena hakim dapat mempidanakan seseorang hanya berdasarkan kemiripan sifat perbuatan dengan delik yang sudah ada.

Dalam praktik peradilan, penggunaan penafsiran oleh hakim tetap dimungkinkan sepanjang tidak berkembang menjadi analogi yang bertentangan dengan prinsip *lex stricta* (Andi Hamzah, 2022). Hakim dalam batas tertentu masih dapat menerapkan metode penafsiran gramatikal (berdasarkan arti kata), penafsiran sistematis (menghubungkan dengan pasal lain), maupun penafsiran teleologis atau sosiologis (berdasarkan tujuan hukum dan kebutuhan masyarakat) (Prastyo, 2023). Namun, perkembangan modus operandi berbasis kecerdasan buatan tetap menimbulkan tantangan nyata dalam penerapan ketentuan pidana yang berlaku saat ini. Batas demarkasi antara perluasan penafsiran teleologis dengan penciptaan analogi baru menjadi sangat bias ketika berhadapan dengan objek hukum immaterial digital.

Permasalahan yuridis terjadi karena tipisnya batasan antara perluasan penafsiran teleologis dan penggunaan analogi dalam kasus digital. Penggunaan penafsiran oleh hakim tetap dimungkinkan sepanjang tidak berkembang menjadi analogi yang bertentangan dengan prinsip *lex stricta*. Namun, perkembangan modus operandi berbasis kecerdasan buatan tetap menimbulkan tantangan dalam penerapan ketentuan pidana yang berlaku. Hal ini berakibat pada ketidakseimbangan yurisprudensi: jika hakim menolak memproses laporan karena tidak adanya pasal tertulis yang presisi, angka penyelesaian perkara dari total 36.221 aduan siber akan terus merosot. Kondisi tersebut mengorbankan asas keadilan demi mematuhi kepastian formal asas legalitas. Berbeda dengan penelitian Santoso (2023) yang cenderung berfokus pada kapasitas sarana kepolisian, data komparatif makro ini mengonfirmasi keterbatasan penegakan hukum siber bersumber dari risiko perluasan interpretasi kaku yang diatur oleh pilar *lex stricta*.

D. Kesimpulan

Berdasarkan hasil analisis data dan pembahasan yang telah diuraikan, penelitian ini menarik dua kesimpulan pokok sebagai berikut:

1. Karakteristik kejahatan siber di Indonesia berdasarkan data resmi Portal Patroli Siber Polri secara empiris menunjukkan pola pemusatan yang didominasi oleh klaster kejahatan finansial berbasis rekayasa sosial, khususnya penipuan online dan pemerasan daring. Temuan ini mengonfirmasi adanya pergeseran sosiologis dalam pola kriminalitas kontemporer, di mana pelaku cenderung memanfaatkan kerentanan literasi digital masyarakat daripada melakukan peretasan sistem yang bersifat teknis murni.
2. Asas legalitas tetap kokoh sebagai fondasi negara hukum demi menjamin hak kepastian individu dari kesewenang-wenangan aparat, namun penerapannya mengalami hambatan operasional yang

signifikan di era digital. Prinsip *lex scripta* dan *lex certa* yang rigid memicu keterbatasan pengaturan hukum akibat lambatnya proses kodifikasi legislatif nasional dalam mengimbangi kecepatan pergeseran teknologi komputer. Sementara itu, pilar *lex stricta* membatasi keleluasaan interpretasi hakim saat menghadapi sengketa pembuktian modus kejahatan jenis baru, sehingga rentan memicu celah impunitas hukum di pengadilan.

DAFTAR PUSTAKA

Andi Hamzah. (2022). *Asas-Asas Hukum Pidana Indonesia*. Yarsif Watampone.

Anggara, A., & Wahyudi, R. (2023). Problematika Penghinaan Ringan Ruang Siber dan Karakteristik Lex Certa. *Jurnal Konstitusi*, *20*(2), 289-304. doi.org [20]

Brenner, S. W. (2007). Law in an Era of "Smart" Cybercrime. *International Journal of Cyber Criminology*, *1*(1), 27-43.

BSSN. (2024). *Laporan Tahunan Lanskap Keamanan Siber Indonesia 2023*. Badan Siber dan Sandi Negara.

Goodin, R. E. (2020). Technological Acceleration and the Lagging Law. *Journal of Political Philosophy*, *28*(3), 241-255. doi.org [6]

INTERPOL. (2023). *Global Crime Trend Report 2023*. Interpol General Secretariat.

Khair, M., & Prastyo, A. (2023). Konstruksi Teleologis dalam Penafsiran Hukum Pidana Siber. *Jurnal Hukum Dan Peradilan*, *12*(2), 201-218. doi.org [6]

Marzuki, P. M. (2022). *Penelitian Hukum: Edisi Revisi*. Prenadamedia Group.

Maskun. (2021). *Kejahatan Siber: Komparasi Regulasi Domestik dan Internasional*. Prenadamedia Group.

Moeljatno. (2015). *Asas-Asas Hukum Pidana*. Rineka Cipta.

Nawi, S., & Pahlevi, F. S. (2022). Kebijakan Penegakan Hukum Tindak Pidana Siber di Indonesia. *Jurnal Jati Hukum*, *14*(1), 34-49. [8]

Patroli Siber Polri. (2024). *Statistik Laporan Masyarakat*. Portal Resmi Patroli Siber Kepolisian Republik Indonesia. patrolisiber.id [14]

Prabowo, H., & Rifai, A. (2022). Penafsiran Hukum Pidana Berdasarkan Asas Larangan Analogi pada Kasus Kejahatan Teknologi Baru. *Jurnal De Jure*, *22*(3), 341-356. doi.org

Pujiyono, P., & Azhar, M. (2022). Reorientasi Asas Legalitas Materiil dalam Pembaharuan Hukum Pidana Nasional. *Jurnal Hukum Lex Generalis*, *3*(2), 112-129. doi.org [11]

Santoso, B. (2023). Hambatan Sosiologis Penyidikan Tindak Pidana Siber Terkait Keterbatasan Regulasi. *Jurnal Masalah-Masalah Hukum*, *52*(1), 44-56. doi.org [13]

Setiadi, E. (2021). Batas Ideal Penafsiran Hukum oleh Hakim Menghadapi Cybercrime. *Jurnal Yudisial*, *14*(2), 175-190. doi.org [14]

Situmeang, S. (2021). Dampak Dualisme Regulasi UU ITE terhadap Kepastian Hukum Pidana Indonesia. *Jurnal Ilmiah Kebijakan Hukum*, *15*(3), 401-416. doi.org [15]

Soekanto, S. (2019). *Pengantar Penelitian Hukum*. UI Press.

Sugiyono. (2020). *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*. Alfabeta.

Wall, D. S. (2021). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press.