JAKSA
JURNAL KAJIAN ILMU HUKUM DAN POLITIK

LPPM Universitas Sains dan Teknologi Komputer
Vol. 3 No. 4 Oktober 2025, Hal. 80-92
E-ISSN: 2988-5140; P-ISSN: 2988-7747
https: https://journal.stekom.ac.id/index.php/Jaksa/index

Politik Hukum Pidana dalam Penanggulangan Kejahatan Siber di Indonesia: Analisis Kriminologis terhadap Efektivitas Kebijakan Penal dan Non-Penal

Mohammad Alfan*[1]
[1]*UIN Sunan Kalijaga, Yogyakarta, Indonesia*
E-mail: alfanmoh@gmali.com

Article Info

Keywords:
Legal Politics
Cybercrime
Digital Criminology
Cyber Governance
Digital Justice

Abstract

This study analyzes the direction of Indonesia's criminal law politics in combating cybercrime through both penal and non-penal approaches within the framework of digital criminology. The research focuses on evaluating the effectiveness of legal policies, institutional dynamics, and the gap between legal norms and social behavior in digital spaces. A qualitative approach using the juridical-sociological method was employed, acknowledging that cybercrime cannot be understood solely through legal texts but must also be examined from social and behavioral perspectives in cyberspace. Data were collected through legal document analysis, interviews with policy actors, and reports from institutions such as BSSN, Kominfo, and the Cybercrime Directorate of the Indonesian National Police, and analyzed using the interactive model of Miles, Huberman, and Saldaña. The results reveal that Indonesia's cyber law politics remain reactive, emphasizing penal enforcement through criminal sanctions and legal prosecution. Conversely, non-penal strategies such as digital literacy and institutional collaboration have improved but have not significantly enhanced public cybersecurity awareness. The main contribution of this study lies in formulating an integrated cyber governance model based on the concept of cyber social control, which promotes synergy between legal instruments, education, and digital governance in building national cyber resilience and justice. This framework offers a more adaptive and inclusive direction for Indonesia's legal politics, oriented toward social defense and digital justice.

DOI: https://doi.org/10.51903/wx2hk609

Submitted: August 2025, Reviewed: September 2025, Accepted: October 2025

**Corresponding Author*

Abstrak

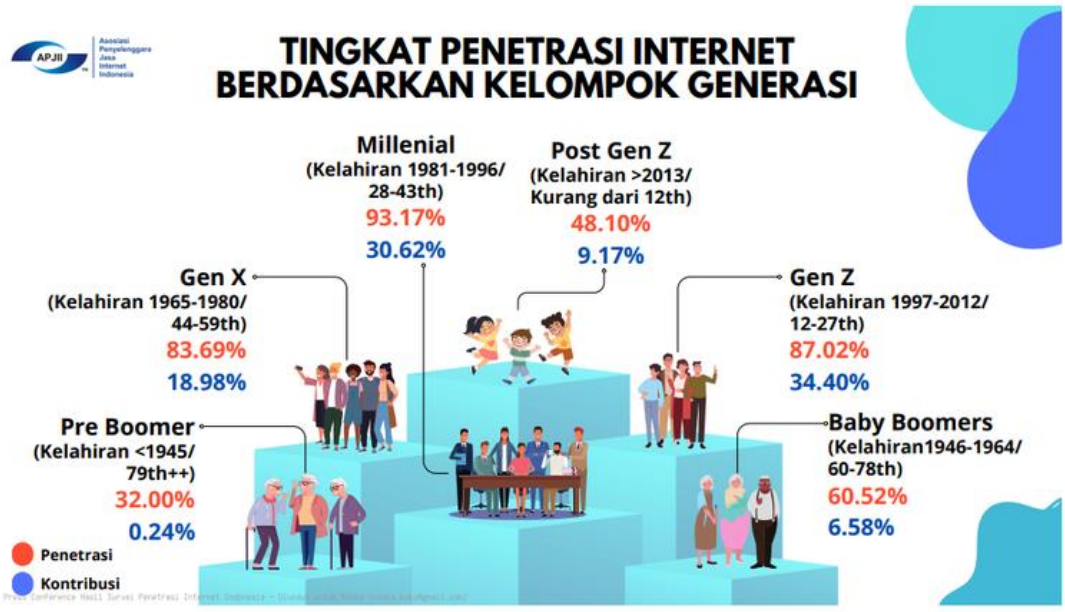
Penelitian ini bertujuan menganalisis arah politik hukum pidana Indonesia dalam penanggulangan kejahatan siber melalui pendekatan penal dan non-penal dengan perspektif kriminologi digital. Fokus kajian diarahkan pada efektivitas kebijakan hukum, dinamika kelembagaan, serta kesenjangan antara norma hukum dan perilaku sosial di ruang digital. Penelitian ini menggunakan pendekatan kualitatif dengan metode yuridis-sosiologis, karena fenomena kejahatan siber tidak dapat dipahami hanya melalui teks hukum, tetapi juga melalui interaksi sosial dan perilaku pelaku di dunia maya. Data diperoleh melalui telaah dokumen hukum, wawancara dengan aktor kebijakan, dan laporan lembaga seperti BSSN, Kominfo, serta Polri Siber, kemudian dianalisis menggunakan model analisis interaktif *Miles, Huberman*, dan *Saldaña*. Hasil penelitian menunjukkan bahwa politik hukum siber Indonesia masih bersifat reaktif, dengan dominasi pendekatan penal melalui penegakan hukum dan sanksi pidana. Di sisi lain, pendekatan non-penal seperti literasi digital dan kolaborasi kelembagaan mengalami kemajuan namun belum mampu meningkatkan kesadaran publik secara signifikan. Kontribusi penelitian ini terletak pada rumusan model integrated *cyber governance* berbasis *cyber social control*, yang menekankan pentingnya

sinergi antara hukum, edukasi, dan tata kelola digital dalam membangun keadilan dan ketahanan siber nasional. Model ini diharapkan menjadi arah baru politik hukum yang lebih adaptif, inklusif, dan berorientasi pada keadilan digital (*digital justice*).

Kata Kunci: *Politik Hukum, Kejahatan Siber, Kriminologi Digital, Cyber Governance, Digital Justice*

I. PENDAHULUAN

Perkembangan teknologi digital telah menghadirkan transformasi besar dalam kehidupan sosial, ekonomi, dan politik hukum di Indonesia (Oktareza et al., 2024). Menurut laporan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII, 2024), jumlah pengguna internet nasional telah mencapai lebih dari 221 juta jiwa terlihat dalam Gambar 1, bahwa gen Z menjadi kelompok usia yang paling banyak terkoneksi internet (Pebriyani, 2024), menjadikan Indonesia sebagai salah satu negara dengan populasi digital terbesar di Asia Tenggara (Ainy Asmaripa, 2023). Namun, di balik pertumbuhan ini, muncul eskalasi kejahatan siber *(cybercrime)* yang semakin kompleks, mencakup kejahatan finansial daring, peretasan data pribadi, penyebaran disinformasi, hingga manipulasi sistem digital lembaga pemerintahan (Siti, 2025). Laporan Badan Siber dan Sandi Negara (BSSN, 2023) mencatat lebih dari 403 insiden siber sepanjang tahun dengan tingkat penyelesaian hukum yang masih di bawah 10 persen (Febriari, 2024). Fenomena ini menunjukkan bahwa sistem hukum pidana nasional belum sepenuhnya adaptif terhadap dinamika dunia digital.



Gambar 1. Tingkat Penetrasi Internet Berdasarkan Generasi

Politik hukum pidana di Indonesia selama ini berfokus pada pendekatan penal, sebagaimana tampak dalam regulasi seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), Kitab Undang-Undang Hukum Pidana (KUHP), dan Rancangan Undang-Undang

Perlindungan Data Pribadi (RUU PDP) (Ramadan & Wahyudi, 2025). Namun, implementasi ketentuan tersebut sering menimbulkan perdebatan publik karena multitafsir, tumpang tindih antar-lembaga, dan kecenderungan overkriminalisasi terhadap warganet. Situasi ini mengindikasikan lemahnya arah politik hukum yang seharusnya menyeimbangkan antara kepastian hukum dan keadilan sosial digital (Erlyani et al., 2024). Pendekatan non-penal seperti literasi digital, edukasi hukum siber, dan penguatan etika digital belum diarusutamakan dalam kebijakan publik (Arafat & Tito, 2024). Akibatnya, efektivitas penanggulangan kejahatan siber tidak hanya bergantung pada perangkat hukum, tetapi juga pada kemampuan negara memahami faktor sosial dan perilaku kriminal dalam ruang digital (Aabid et al., 2025).

Kajian internasional menunjukkan bahwa tantangan serupa juga dihadapi oleh banyak negara. Regulasi hukum pidana sering kali tertinggal dari perkembangan teknologi dan pola kejahatan baru. Untuk memberikan pemetaan yang lebih komprehensif, Tabel 1 berikut merangkum penelitian-penelitian relevan secara global dan nasional yang mengkaji hubungan antara politik hukum pidana dan kriminologi digital.

Tabel 1. Penelitian Sebelumnya tentang Politik Hukum dan Kriminologi Siber

No	Peneliti & Tahun	Lokasi/Konteks	Fokus Kajian	Temuan Utama
1	(Nezam Eslami & Yavari, 2025)	Global	Politik hukum cybercrime	Kebijakan siber global terlalu berorientasi keamanan, belum memperhatikan hak digital warga.
2	(Nusa et al., 2025)	Inggris	Kriminologi digital	Hukum pidana tradisional gagal menangani kejahatan digital lintas yurisdiksi.
3	(Pascua Mateo, 2022)	AS & Eropa	Adaptive cyber law	Diperlukan politik hukum yang fleksibel terhadap inovasi teknologi.
4	(Pasculli, 2020)	Global	Digital criminology	Perilaku kejahatan digital perlu dijelaskan melalui pendekatan sosial-psikologis.
5	(Ashurov, 2023)	Negara berkembang	Penegakan hukum siber	Ketimpangan kapasitas negara berkembang menimbulkan *cyber impunity*.
6	(Cromvelle, 2025)	Asia Tenggara	Kebijakan AI & siber	ASEAN masih berbasis *soft law* tanpa kekuatan mengikat.
7	(Khan, 2024)	Singapura	Efektivitas kebijakan hukum siber	Kombinasi penal dan non-penal paling efektif menekan cybercrime.
8	(Masudianto & Barthos, 2025)	Indonesia	UU PDP & tanggung jawab hukum AI	Prinsip perlindungan data Eropa baru diadopsi sebagian di Indonesia.

Dari pemetaan penelitian tersebut terlihat adanya dua kecenderungan utama. Pertama, di tingkat global, problem utama adalah ketertinggalan hukum pidana dalam menghadapi perubahan digital yang cepat dan lintas batas. Kedua, di tingkat nasional, penelitian hukum siber masih terbatas pada analisis yuridis normatif tanpa mempertimbangkan dimensi perilaku kriminal dan konteks sosial digital. Dengan demikian, terdapat kesenjangan penelitian yang signifikan antara politik hukum pidana dan analisis kriminologis sebagai dasar evaluasi efektivitas kebijakan penal dan non-penal.

Penelitian ini hadir untuk menutup kesenjangan tersebut dengan pendekatan interdisipliner. Penelitian ini akan menelaah arah politik hukum pidana Indonesia dalam menanggulangi kejahatan siber. Kemudian, penelitian ini akan menganalisis efektivitas kebijakan penal (hukum pidana) dan non-penal (edukasi, teknologi, sosial) dengan menggunakan kerangka kriminologi digital. Dan, penelitian ini berupaya membangun model politik hukum responsif (Nonet & Selznick, 1978) yang mampu mengintegrasikan prinsip keadilan digital, keadilan sosial, dan perlindungan hak warga di ruang siber.

Dari sisi teoretis, penelitian ini berpijak pada tiga fondasi utama: teori politik hukum (Mahfud MD, 2009) yang menekankan peran kekuasaan negara dalam menentukan arah hukum pidana (Anggara et al., 2024); teori kriminologi digital yang menjelaskan perilaku kejahatan dalam konteks jaringan dan anonimitas (Malian, 2024); serta konsep hukum responsif yang mendorong penyesuaian hukum terhadap dinamika sosial. Integrasi ketiga perspektif ini diharapkan mampu menghasilkan analisis yang tidak hanya legalistik, tetapi juga sosiologis dan empiris (Rizki et al., 2022). Integrasi ketiga perspektif ini tidak hanya memberikan dasar legalistik, tetapi juga memperkuat analisis hubungan antara kebijakan hukum dan realitas sosial digital. Dalam konteks ini, teori kriminologi digital berperan penting menjelaskan lemahnya mekanisme pengawasan sosial di ruang maya atau cyber social control, sementara pendekatan situational crime prevention menekankan pentingnya upaya negara dalam mengurangi peluang kejahatan melalui edukasi, penguatan kapasitas teknis, dan pembentukan norma perilaku daring.

Secara akademik, kebaruan penelitian ini terletak pada integrasi pendekatan politik hukum dan kriminologi digital dalam menilai efektivitas kebijakan penal dan non-penal. Penelitian ini juga memperkenalkan konsep "keadilan digital" *(digital justice*) sebagai paradigma baru dalam perumusan politik hukum pidana yang adaptif terhadap transformasi teknologi. Secara praktis, hasil penelitian diharapkan menjadi dasar bagi pembuat kebijakan dalam merumuskan strategi penanggulangan kejahatan siber yang lebih komprehensif, adil, dan partisipatif, dengan mempertemukan instrumen hukum, pendidikan digital, dan tata kelola kolaboratif. Dengan demikian, penelitian ini memperkenalkan paradigma keadilan digital dalam politik hukum pidana Indonesia untuk menjembatani pendekatan hukum yang represif dan partisipatif dalam menghadapi kejahatan siber.

II. METODOLOGI PENELITIAN

A. Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan metode yuridis-sosiologis, karena isu kejahatan siber tidak dapat dipahami hanya melalui teks hukum, melainkan juga melalui realitas sosial dan perilaku pelaku di ruang digital. Pendekatan ini memungkinkan peneliti menelaah bagaimana hukum pidana, kebijakan publik, dan aspek sosial saling berinteraksi dalam proses penanggulangan kejahatan siber. Melalui metode ini, data yang dikumpulkan tidak hanya bersumber dari dokumen hukum tertulis, tetapi juga dari persepsi, pengalaman, dan praktik aktor hukum di lapangan.

Pendekatan yuridis-sosiologis menempatkan hukum sebagai gejala sosial yang hidup dalam masyarakat. Karena itu, penelitian ini tidak bertujuan hanya menafsirkan norma hukum, tetapi juga menilai efektivitas dan relevansinya dalam konteks sosial digital. Analisis dilakukan terhadap dinamika politik hukum pidana yang memengaruhi kebijakan siber nasional, serta bagaimana kebijakan tersebut berdampak terhadap perilaku masyarakat, aparat penegak hukum, dan pelaku kejahatan siber. Dengan demikian, pendekatan ini membantu menjembatani kesenjangan antara norma dan praktik hukum di lapangan.

B. Lokasi dan Fokus Penelitian

Penelitian ini difokuskan pada konteks hukum dan kebijakan siber di Indonesia, dengan studi kasus terhadap pelaksanaan UU ITE, KUHP, dan RUU Perlindungan Data Pribadi. Pemilihan Indonesia didasarkan pada kompleksitas peraturan hukum siber yang sering menimbulkan perdebatan publik dan persoalan implementasi, seperti kasus kriminalisasi ekspresi digital dan lemahnya perlindungan data pribadi. Analisis juga diarahkan untuk memahami relasi antar-lembaga, seperti BSSN, Polri Siber, dan Kementerian Kominfo, dalam merespons kejahatan digital.

Fokus penelitian tidak terbatas pada kebijakan penal (represif), melainkan juga mencakup kebijakan non-penal (preventif dan edukatif). Hal ini dilakukan agar hasil penelitian mampu memotret strategi penanggulangan kejahatan siber secara komprehensif, baik dari sisi hukum pidana maupun pendekatan sosial dan teknologi. Dengan cara ini, penelitian diharapkan menghasilkan evaluasi yang lebih utuh terhadap arah politik hukum pidana di era digital.

C. Jenis dan Sumber Data

Sumber data penelitian terdiri atas data primer dan data sekunder. Data primer diperoleh melalui wawancara mendalam dengan informan kunci, seperti pejabat BSSN, penyidik Direktorat Tindak Pidana Siber Polri, akademisi hukum pidana, pakar teknologi informasi, serta aktivis digital rights. Wawancara dilakukan secara semi-terstruktur agar memungkinkan eksplorasi terhadap pandangan subjektif informan mengenai efektivitas kebijakan hukum siber. Selain itu, peneliti juga melakukan observasi dokumenter terhadap pelaksanaan kebijakan dan kasus hukum yang relevan.

Data sekunder meliputi bahan hukum primer, seperti peraturan perundang-undangan (UU ITE, KUHP, RUU PDP), serta bahan hukum sekunder berupa jurnal ilmiah, laporan lembaga internasional (EU AI Act, ASEAN Secretariat, INTERPOL), dan publikasi nasional (BSSN, Kominfo, Mahkamah Agung). Penggunaan kombinasi data primer dan sekunder bertujuan memperkaya analisis, sekaligus memastikan triangulasi sumber sehingga hasil penelitian memiliki validitas tinggi.

D. Teknik Pengumpulan Data

Data dikumpulkan melalui wawancara mendalam, analisis dokumen, dan studi literatur. Wawancara dilakukan menggunakan pedoman umum dengan pertanyaan terbuka untuk menggali persepsi, strategi, dan tantangan dalam implementasi kebijakan hukum siber. Analisis dokumen meliputi telaah regulasi,

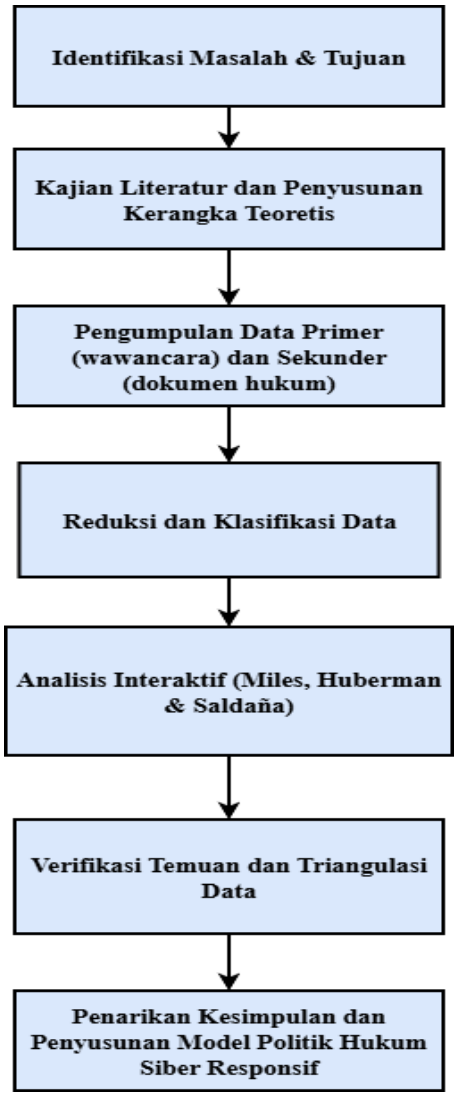
laporan tahunan lembaga, serta putusan pengadilan yang berkaitan dengan tindak pidana siber. Pendekatan ini memungkinkan peneliti memperoleh gambaran menyeluruh tentang arah politik hukum dan dinamika penegakan hukum digital di Indonesia.

Selain itu, studi literatur dilakukan terhadap berbagai penelitian terdahulu baik global maupun nasional untuk memperkuat kerangka analisis teoritis. Literatur yang dikaji meliputi teori politik hukum (Mahfud MD, 2009), hukum responsif (Nonet & Selznick, 1978), dan kriminologi digital (Wall, 2017; Yar, 2019). Dengan menggabungkan wawancara empiris dan kajian literatur teoritis, penelitian ini memperoleh kedalaman analisis sekaligus konteks akademik yang kuat.

E. Teknik Analisis Data

Analisis data dilakukan menggunakan model analisis interaktif Miles, Huberman, dan Saldaña (2018), yang meliputi tiga tahap utama: reduksi data, penyajian data, dan penarikan kesimpulan/verifikasi. Data yang diperoleh dari wawancara dan dokumen hukum diseleksi, dikategorikan, dan diinterpretasikan dalam konteks teori politik hukum dan kriminologi digital. Analisis ini bertujuan mengidentifikasi pola hubungan antara politik hukum pidana, efektivitas kebijakan, dan perilaku pelaku kejahatan siber.

Proses analisis dilakukan secara siklik, artinya setiap temuan awal diverifikasi ulang dengan sumber data lain untuk memastikan konsistensi, alur penelitian divisualisasikan pada Gambar 2. Pendekatan ini memungkinkan peneliti menemukan hubungan kausal antara kebijakan hukum dan perilaku sosial digital, serta merumuskan model politik hukum yang responsif. Dengan metode ini, hasil penelitian diharapkan dapat memberikan kontribusi empiris dan teoretis bagi pengembangan studi hukum pidana dan kriminologi di Indonesia.



Gambar 2. Diagram Alur Proses Penelitian Yuridis-Sosiologis

F. Validitas dan Keabsahan Data

Untuk menjamin keabsahan data, penelitian ini menerapkan teknik triangulasi sumber dan metode. Triangulasi sumber dilakukan dengan membandingkan hasil wawancara dari berbagai informan (pemerintah, akademisi, dan masyarakat sipil), sedangkan triangulasi metode dilakukan dengan mengombinasikan hasil wawancara, analisis dokumen, dan studi literatur. Pendekatan ini digunakan untuk memastikan bahwa hasil penelitian tidak bersifat bias dan tetap mencerminkan kondisi empiris yang objektif.

Selain triangulasi, peneliti juga menerapkan member check, yaitu mengonfirmasi hasil interpretasi kepada beberapa informan kunci untuk memastikan keakuratan data. Semua proses analisis dilakukan secara sistematis dengan menjaga integritas akademik dan prinsip etika penelitian. Dengan prosedur validasi ini, temuan penelitian diharapkan dapat dipercaya (trustworthy), dapat dipertanggungjawabkan secara ilmiah, dan bermanfaat bagi pengembangan politik hukum pidana yang adaptif terhadap era digital.

III. HASIL DAN PEMBAHASAN

Hasil

A. Dinamika Politik Hukum Pidana Siber di Indonesia

Politik hukum pidana Indonesia dalam penanggulangan kejahatan siber hingga 2024 masih bersifat reaktif dan belum sistemik, terlihat dari kebijakan yang muncul sebagai respons terhadap tekanan publik, bukan hasil desain regulatif yang terencana. Meskipun jumlah kasus menurun dari 4.210 kasus pada 2023 menjadi 3.331 kasus pada 2024, efektivitas penyelesaian meningkat hingga 2.073 kasus, menunjukkan kemajuan di tingkat penegakan hukum. Namun, tantangan utama tetap pada lemahnya sinkronisasi norma, pembuktian digital, dan kapasitas lembaga penegak hukum dalam adaptasi teknologi. Tren terbaru memperlihatkan lonjakan signifikan pada manipulasi data elektronik (+36,4%) dan judi online (+525%), serta peningkatan pemblokiran 11.160 situs ilegal, sebagaimana dirinci pada Tabel 2, yang menggambarkan ketimpangan antara peningkatan aktivitas kejahatan digital dan keterlambatan politik hukum dalam membentuk sistem regulatif yang adaptif dan berkeadilan.

Tabel 2. Data Kejahatan Siber di Indonesia Tahun 2023–2024

Kategori	2023	2024	Perubahan (%)	Sumber
Kasus kejahatan siber ditindak	4.210	3.331	-22,11%	Kompas (31 Des 2024)
Kasus diselesaikan (penyidikan–pengadilan)	1.463	2.073	+41,78%	Liputan6 (2024)
Manipulasi data (UU ITE)	10.200	13.922	+36,4%	Pusiknas Polri (2024)
Judi online (judol)	275	1.720	+525,45%	Antara News (2024)
Situs/konten ilegal diblokir	8.670	11.160	+28,75%	Tribrata News (2025)

B. Efektivitas Kebijakan Penal dalam Penanggulangan Kejahatan Siber

Kebijakan penal dalam penanggulangan kejahatan siber di Indonesia masih menghadapi kendala struktural dan implementatif, terutama pada aspek pembuktian digital, koordinasi antarinstansi, dan kapasitas aparat penegak hukum. Meskipun regulasi seperti UU No. 19 Tahun 2016 (ITE) dan UU No. 27 Tahun 2022 (PDP) telah memberikan dasar hukum, efektivitasnya belum optimal karena lemahnya perangkat teknis dan minimnya sumber daya manusia forensik digital. Berdasarkan data Bareskrim Polri dan BSSN, sepanjang 2024 terdapat 2.073 kasus kejahatan siber diselesaikan, dengan tingkat penyelesaian mencapai 62,2%, meningkat dari 34,7% pada 2023. Namun, hanya 41% laporan masyarakat yang dapat ditindaklanjuti akibat keterbatasan alat bukti dan validasi forensik. Selain itu, kerugian finansial akibat kejahatan siber di Indonesia mencapai Rp 14,5 triliun, menempatkan Indonesia di peringkat keempat tertinggi di Asia Tenggara. Hal ini memperlihatkan bahwa meskipun penegakan hukum penal meningkat, pendekatan penal saja belum cukup efektif tanpa sinergi dengan strategi non-penal dan preventif digital, sebagaimana tergambar dalam Tabel 3.

Tabel 3. Efektivitas Penegakan Hukum dan Dampak Ekonomi Kejahatan Siber di Indonesia (2023–2024)

Indikator	2023	2024	Perubahan (%)	Sumber
Kasus diselesaikan (Bareskrim)	1.463	2.073	+41,78%	Liputan6 (2024)

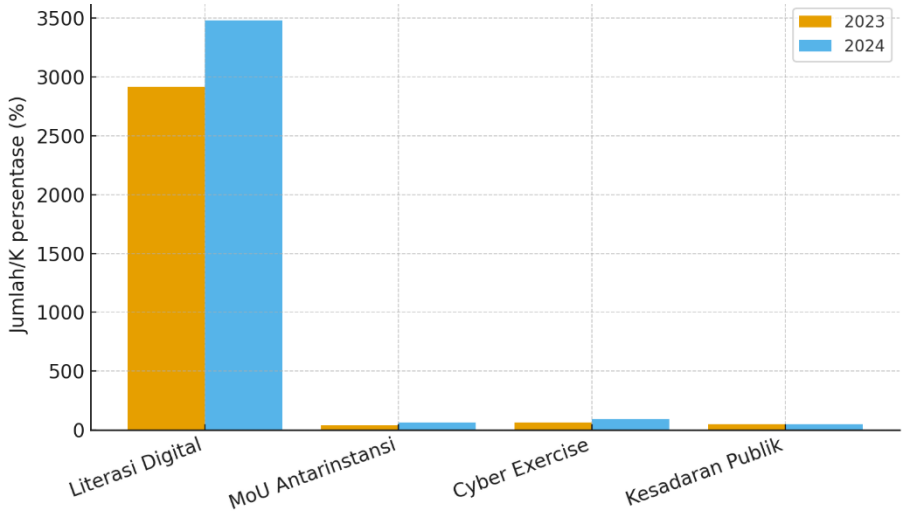
Tingkat penyelesaian laporan	34,7%	62,2%	+27,5%	Polri Cyber Crime Report (2024)
Laporan masyarakat diterima	5.980	8.422	+40,85%	BSSN (2024)
Laporan yang ditindaklanjuti	2.098	3.460	+64,9%	Detik News (2024)
Estimasi kerugian finansial (Rp)	10,3 triliun	14,5 triliun	+40,78%	Kominfo (2025)

C. Efektivitas Kebijakan Non-Penal dan Kolaborasi Institusional

Pendekatan non-penal dalam penanggulangan kejahatan siber menitikberatkan pada edukasi, pencegahan, dan kolaborasi kelembagaan antara BSSN, Kominfo, dan Polri. Pada 2024 tercatat peningkatan signifikan dalam literasi digital (3.480 kegiatan), MoU antarinstansi (65 kerja sama), serta partisipasi 96 lembaga dalam National Cyber Exercise terlihat Tabel 4. Tren peningkatan tersebut secara visual dapat dilihat pada Gambar 3 yang memperlihatkan kenaikan konsisten program non-penal sepanjang 2023–2024. Meski demikian, kesadaran publik terhadap keamanan digital justru menurun menjadi 48%, dan 62% pengguna internet belum pernah mengikuti pelatihan keamanan siber. Kepala BSSN (2024) menegaskan bahwa "sebagian besar insiden siber disebabkan oleh kelalaian manusia, bukan kelemahan sistem." Hal ini menandakan bahwa efektivitas kebijakan non-penal masih bergantung pada perubahan budaya digital masyarakat serta keberlanjutan kolaborasi lintas sektor.

Tabel 4. Kolaborasi dan Program Non-Penal Keamanan Siber di Indonesia (2023–2024)

Indikator	2023	2024	Perubahan (%)	Sumber
Kegiatan literasi digital (nasional)	2.915	3.480	+19,4%	Kominfo (2024)
MoU antarinstansi (pemerintah-swasta)	41	65	+58,5%	BSSN (2024)
Lembaga peserta *Cyber Exercise* nasional	67	96	+43,2%	CNN Indonesia (2024)
Survei kesadaran keamanan digital publik	52%	48%	-4%	Katadata Insight Center (2024)



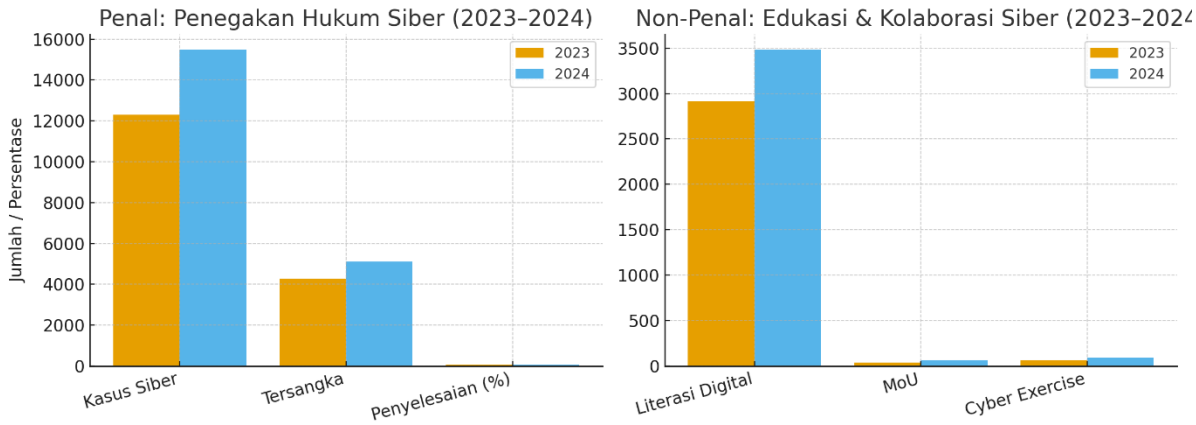
Gambar 3. Tren Peningkatan Program Non-Penal Keamanan Siber Indonesia (2023–2024)

Gambar 3 memperlihatkan adanya peningkatan pada indikator program non-penal seperti literasi digital, kerja sama antarinstansi, dan partisipasi Cyber Exercise. Namun, terjadi penurunan kesadaran publik terhadap keamanan digital. Pola ini menunjukkan bahwa kebijakan non-penal lebih berhasil

memperkuat kapasitas kelembagaan dibanding mengubah perilaku masyarakat daring. Secara kriminologis, hal ini sejalan dengan teori kontrol sosial yang menekankan bahwa perubahan perilaku membutuhkan internalisasi nilai, bukan sekadar perluasan program formal.

D. Analisis Komparatif Kebijakan Penal dan Non-Penal

Perbandingan antara kebijakan penal dan non-penal menunjukkan bahwa kedua pendekatan berkembang positif namun belum seimbang. Pendekatan penal menonjol dalam peningkatan jumlah kasus yang ditangani, tersangka, dan tingkat penyelesaian perkara, sedangkan pendekatan non-penal memperkuat literasi digital, kolaborasi kelembagaan, dan latihan keamanan siber. Meski demikian, efektivitas non-penal masih terbatas karena rendahnya kesadaran publik terhadap keamanan digital. Gambar 4 memperlihatkan bahwa kebijakan penal cenderung reaktif, sementara non-penal bersifat preventif namun membutuhkan waktu untuk menghasilkan dampak sosial. Oleh karena itu, integrasi keduanya melalui kebijakan cyber social control menjadi penting agar penegakan hukum dan pembentukan etika digital berjalan beriringan sebagai bagian dari strategi politik hukum siber nasional.



Gambar 4. Perbandingan Tren Penal dan Non-Penal dalam Penanggulangan Kejahatan Siber (2023–2024)

Pembahasan

Temuan penelitian ini memperlihatkan bahwa politik hukum siber di Indonesia masih berproses menuju keseimbangan antara penegakan hukum *(law enforcement)* dan pembentukan kesadaran hukum digital. Kinerja aparat dalam menangani kasus siber meningkat secara signifikan, namun belum dibarengi oleh kesiapan masyarakat terhadap ancaman kejahatan digital (Pertiwi et al., 2024). Pemerintah masih lebih menonjolkan strategi penal melalui revisi peraturan dan pembentukan unit khusus, seperti Direktorat Tindak Pidana Siber Bareskrim Polri, dibanding strategi edukatif dan preventif. Pola ini mencerminkan pendekatan hukum yang masih bersifat state-centered, dengan fokus pada pengendalian, bukan pemberdayaan. Dalam perspektif *responsive law* (Nonet & Selznick, 1978), kondisi tersebut menunjukkan bahwa hukum masih berfungsi sebagai alat kekuasaan, belum sepenuhnya menjadi mekanisme yang tanggap terhadap dinamika sosial dan kebutuhan masyarakat digital (Huda, 2023).

Kebijakan non-penal di sisi lain menekankan literasi digital, pelatihan keamanan siber, dan kerja sama kelembagaan. Namun, efektivitasnya terbatas karena implementasi masih bersifat simbolik dan belum menjangkau lapisan masyarakat yang paling rentan (Najwa et al., 2024). Rendahnya tingkat kesadaran keamanan digital (48%) menunjukkan bahwa intervensi preventif belum mampu membentuk budaya hukum yang kuat (Putri et al., 2025). Dalam konteks kriminologi, kondisi ini menggambarkan lemahnya situational crime prevention, di mana perubahan perilaku individu belum sejalan dengan kompleksitas ancaman siber (Atara et al., 2025). Untuk itu, penerapan prinsip digital justice menjadi penting sebagai penghubung antara efektivitas hukum dan perilaku sosial; hukum harus tidak hanya menghukum pelanggar, tetapi juga memulihkan keadilan dan kepercayaan publik di ruang digital.

Dari perspektif politik hukum, diperlukan pergeseran dari paradigma reaktif menuju *integrated cyber governance,* yaitu tata kelola keamanan siber yang menggabungkan aspek hukum positif, edukasi sosial, dan kolaborasi publik-swasta (Ansori et al., 2025). Pendekatan ini menempatkan kebijakan penal dan non-penal bukan sebagai dikotomi, melainkan sebagai satu kesatuan strategi sosial. Refleksi kritis perlu diarahkan pada risiko over-penalization dalam UU ITE yang berpotensi menimbulkan efek jera berlebihan dan mengancam kebebasan berekspresi di ruang digital. Dengan demikian, politik hukum siber Indonesia dapat berkembang menjadi sistem yang tidak hanya menindak pelanggaran, tetapi juga membangun ketahanan sosial digital sebagai basis keadilan dan kedaulatan nasional.

IV. KESIMPULAN

Politik hukum siber di Indonesia menunjukkan arah yang progresif namun masih menghadapi dilema antara penegakan hukum yang represif dan pembangunan kesadaran digital yang partisipatif. Hasil penelitian memperlihatkan bahwa peningkatan penanganan kasus siber dan kolaborasi kelembagaan telah berjalan paralel, tetapi kesenjangan kesadaran publik masih menjadi titik lemah utama. Hal ini menegaskan bahwa keberhasilan kebijakan keamanan siber tidak hanya ditentukan oleh instrumen hukum, tetapi juga oleh kemampuan negara membentuk budaya hukum digital yang berkelanjutan dan inklusif.

Oleh karena itu, ke depan diperlukan desain politik hukum yang bersifat integratif melalui penguatan *cyber social control* berbasis kolaborasi antara pemerintah, masyarakat, dan sektor swasta. Model ini akan mempertemukan dimensi penal dan non-penal dalam satu kerangka tata kelola siber nasional yang adaptif, adil, dan berorientasi pada keadilan sosial. Integrasi tersebut tidak hanya memperkuat ketahanan digital nasional, tetapi juga menjadi fondasi bagi pembangunan hukum yang responsif terhadap transformasi teknologi dan dinamika kejahatan global. Penerapan model *cyber social control* dapat menjadi basis politik hukum pidana yang kolaboratif, adil, dan berorientasi pada keadilan digital di Indonesia, sehingga arah kebijakan siber ke depan lebih menekankan keseimbangan antara keamanan, kebebasan, dan tanggung jawab digital.

REFERENSI

Aabid, M., Dzaky, T., & Fikma Edrisy, I. (2025). Strategi Pencegahan Kejahatan Siber di Indonesia: Sinergi antara UU ITE dan Kebijakan Keamanan Digital. *PESHUM: Jurnal Pendidikan, Sosial dan Humaniora*, *4*(2), 12. Diambil dari https://ulilalbabinstitute.id/index.php/PESHUM/article/view/8311/6317

Ainy Asmaripa, Z. (2023). Akses Digital dan Status Kesehatan Masyarakat di Asia Tenggara: Studi Deskriptif di Indonesia, Malaysia, Dan Thailand. *J-REMI : Jurnal Rekam Medik dan Informasi Kesehatan*, *5*(1), 44–53. https://doi.org/10.25047/j-remi.v5i1.4261

Anggara, R. B., Apriyanti, R., & Syahuri, T. (2024). Politik Hukum Di Mata Para Tokoh. *Lex Sharia Pcta Sun Servanda: Jurnal Hukum Islam dan Kebijakan*, *1*(3), 1–13.

Ansori, A., Ali, K., Susilo, T., Hadisuseno, B., & Amperawan, C. (2025). Cyber Leadership in the Digital Age: Building a Resilient Indonesian Defense in Cyberspace. *Indonesian Journal of Interdisciplinary Research in Science and Technology*, *3*(9), 915–932.

Arafat, M., & Tito, A. W. E. (2024). Kebijakan Kriminal dalam Penanganan Siber di Era Digital : Studi Kasus di Indonesia Criminal Policy in handing Cyber in the Digital Era. *Equality: Journal of Law and Justice*, *1*(2), 221–241. https://doi.org/10.5281/Zenodo.4766614

Ashurov, A. (2023). Collaboration Challenges in Cross-Border Cybercrime Investigations. *J. Natl. Security Law Policy*, *15*(2), 245–278.

Atara, I., Syallomeita, S., & Haksoro, R. A. B. (2025). Analisis Kriminologi Terhadap Pencurian Data Pribadi di Era Digital: Studi Kasus Kebocoran Data Pengguna Aplikasi Mypertamina Tahun 2023. *Jurnal Ilmiah Penelitian Mahasiswa*, *3*(2), 129–140. Diambil dari https://doi.org/10.61722/jipm.v3i2.787

Cromvelle, S. D. (2025). Algorithmic Discrimination and Equal Protection Law: Legal Remedies for AI Bias In Automated Decision-Making. *International Journal of Law, Policy and Scientific Research*, *1*(1), 1–12.

Erlyani, R., Prihantono, P., & Syahuri, T. (2024). Dinamika Politik Hukum Dalam Konteks Perubahan Sosial. *Lex Sharia Pacta Sunt Servanda: Jurnal Hukum Islam dan Kebijakan*, *1*(3), 14–24.

Febriari, S. (2024). Sepanjang 2023, Ada 403 Juta Serangan Siber ke Indonesia. *metronews.com*. Diambil dari https://www.metrotvnews.com/play/b1oC9wGX-sepanjang-2023-ada-403-juta-serangan-siber-ke-indonesia#:~:text=Badan Siber dan Sandi Negara,penurunan kepercayaan terhadap suatu organisasi.&text=Di era digitalisasi saat ini,signifikan dalam kehidupan sehari–har

Huda, N. (2023). *Politik Hukum dan Pembangunan Sistem Hukum Nasional*. (O. V. Rahmadianti, A. Fa'iq, & Tarmizi, Ed.). Sinar Grafika Offset.

Khan, A. A. (2024). Reconceptualizing Policing for Cybercrime: Perspectives from Singapore†. *Laws*, *13*(4), 1–19. https://doi.org/10.3390/laws13040044

Malian, D. (2024). Penanganan Dan Tantangan Cybercrime Di Era Digital Perspektif Kriminologi. *Innovative : Journal of Social Science Research*, *4*(6), 7048–7056.

Masudianto, D. N., & Barthos, M. (2025). Optimization of Personal Data Rights Protection in the Artificial Intelligence Era Under Indonesia's Cybersecurity Law. *Interdisciplinary Journal and*

Hummanity (INJURITY), *4*(7), 452–462. https://doi.org/10.58631/injurity.v4i7.1451

Najwa, Y., Amanda, P. D., Fatmawati, F., Al-Kalam, S., & Wahyudi, S. N. (2024). Analisis Efektivitas Program Perlindungan Sosial dalam Meningkatkan Kesejahteraan Kelompok Rentan di Indonesia. *Al-I'timad: Jurnal Dakwah dan Pengembangan Masyarakat Islam*, *2*(1), 1–20. https://doi.org/10.35878/alitimad.v2i1.1131

Nezam Eslami, I., & Yavari, E. (2025). Analysis of Criminal Laws Related to Cybercrimes Against National Security (Such as Cyber Espionage) and Examination of the Challenges of Identifying and Punishing These Crimes. *Legal Studies in the Digital Age*, *4*(3), 1–13. https://doi.org/10.61838/kman.lsda.190

Nusa, Q. I., Sugiri, B., Yuliati, & Sulistio, F. (2025). Law Enforcement of Cybercrime Tracking Digital Footprints of Cross-Border Hackers. *International Journal of Islamic Education, Multiculturalism (IJIERM)*, *7*(2), 776–802.

Oktareza, D., Noor, A., Saputra, E., & Yulianingrum, A. V. (2024). CENDEKIA: Jurnal Hukum, Sosial & Humaniora Transformasi Digital 4.0: Inovasi yang Menggerakkan Perubahan Global. *CENDEKIA: Jurnal Hukum, Sosial & Humaniora*, *2*(3), 661–672. Diambil dari https://doi.org/10.5281/zenodo.12742216

Pascua Mateo, F. (2022). European Parliament and Representation of the Union's Citizens: What can be Expected from Electoral Law from a Democratic Standpoint? *European Law Journal*, *28*(1–3), 63–88. https://doi.org/10.1111/eulj.12456

Pasculli, L. (2020). The Global Causes of Cybercrime and State Responsibilities: Towards an Integrated Interdisciplinary Theory. *Journal of Ethics and Legal Technologies (JELT)*, *2*(1), 48–74.

Pebriyani, H. (2024). Hasil Survei APJII: Pengguna Internet di Indonesia Tembus 221 Juta, Mendominasi Gen Z. *komite.id*. Diambil dari https://www.komite.id/2024/02/06/hasil-survei-apjii-pengguna-internet-di-indonesia-tembus-221-juta-mendominasi-gen-z/

Pertiwi, N. A. S., Umardiyah, F., Mansyur, M. N., Munir, M., Sapiâ€™i, I., Sholichah, A., & Fudlah, T. N. (2024). Sosialisasi Kesadaran Keamanan Digital di Era Revolusi Industri 4.0. *Jumat Informatika: Jurnal Pengabdian Masyarakat*, *5*(1), 49–55. https://doi.org/10.32764/abdimasif.v5i1.4525

Putri, A., Sari, N., Fajrina, P., & Aisyah, S. (2025). Keamanan Online dalam Media Sosial : Pentingnya Perlindungan Data Pribadi di Era Digital (Studi Kasus Desa Jurnal Pengabdian Nasional (JPN) Indonesia. *Jurnal Pengabdian Nasional (JPN) Indonesia*, *6*(1), 38–52.

Ramadan, M. I., & Wahyudi, E. (2025). Comparative Study : The Urgency Of Reformulating Deepfake Criminal Sanctions In The Criminal Code And The ITE Law S. *Jurnal Hukum Sehasem*, *11*(2), 353–362.

Rizki, D., Sari, E., & Yusrizal, Y. (2022). Penerapan Hukum Responsif Dalam Pembentukan Undang-Undang Di Indonesia. *Suloh:Jurnal Fakultas Hukum Universitas Malikussaleh*, *10*(1), 31. https://doi.org/10.29103/sjp.v10i1.7934

Siti Maesaroh, R. (2025). Tantangan Keamanan Siber dan Implikasinya terhadap Hukum Kenegaraan: Tinjauan atas Peran Negara dalam Menjamin Ketahanan Digital. *Staatsrecht: Jurnal Hukum Kenegaraan dan Politik Islam*, *4*(2), 255–274. https://doi.org/10.14421/3n8bxw79