



RELEVANSI FAKTOR PENEGAKAN HUKUM MENURUT SOERJONO SOEKANTO DALAM MENGHADAPI FENOMENA CYBER CRIME

Rima Fadhilatunnisa¹⁾, Ahmad Rama²⁾, Antonia Alda Resalda³⁾, Muhammad Sulthon Robani Thai'ib⁴⁾, Rima Yuni Saputri⁵⁾, Dian Permata Sari⁶⁾

¹⁾Pendidikan Pancasila dan Kewarganegaraan, Fakultas Keguruan dan Ilmu Pendidikan, Universitas Lampung, Bandar Lampung, Indonesia
Email: rimafadhila656@gmail.com

²⁾Pendidikan Pancasila dan Kewarganegaraan, Fakultas Keguruan dan Ilmu Pendidikan, Universitas Lampung, Bandar Lampung, Indonesia
Email: ahmadramaips@gmail.com

³⁾Pendidikan Pancasila dan Kewarganegaraan, Fakultas Keguruan dan Ilmu Pendidikan, Universitas Lampung, Bandar Lampung, Indonesia
Email: antonialda77@gmail.com

⁴⁾Pendidikan Pancasila dan Kewarganegaraan, Fakultas Keguruan dan Ilmu Pendidikan, Universitas Lampung, Bandar Lampung, Indonesia
Email: intersulton@gmail.com

⁵⁾Pendidikan Pancasila dan Kewarganegaraan, Fakultas Keguruan dan Ilmu Pendidikan, Universitas Lampung, Bandar Lampung, Indonesia
Email: rima.yuni@fkip.unila.ac.id

⁶⁾Pendidikan Pancasila dan Kewarganegaraan, Fakultas Keguruan dan Ilmu Pendidikan, Universitas Lampung, Bandar Lampung, Indonesia
Email: dianpermatasari@fkip.unila.ac.id

Abstract.

The main challenge is the legal character, which often struggles to keep up with technological developments, and the failure in handling cyber crime is caused by a lack of balance among the five law enforcement factors of Soerjono Soekanto. This study aims to systematically describe the law enforcement factors according to Soerjono Soekanto. The research method used is a qualitative approach with a type of normative juridical research. This study shows that the development of information technology has brought significant changes in crime patterns, with cyber crime experiencing rapid growth in Indonesia. Therefore, education and the instilling of digital ethical values are needed to build intrinsic collective awareness, so that society is not only the object of protection but also an active subject in creating a safe and orderly digital space.

Keywords: Law enforcement, normative juridical, digital ethics.

Abstrak.

Tantangan utama karakter hukum yang seringkali tertatih mengikuti perkembangan teknologi, dan kegagalan dalam menangani *cyber crime* disebabkan oleh kurangnya keseimbangan di antara lima faktor penegakan hukum Soerjono Soekanto, Penelitian ini bertujuan untuk menggambarkan secara sistematis faktor-faktor penegakan hukum menurut Soerjono Soekanto, Metode penelitian yang digunakan adalah pendekatan kualitatif dengan jenis penelitian yuridis normatif, penelitian ini menunjukkan bahwa perkembangan teknologi informasi telah membawa perubahan signifikan dalam pola kejahatan, dengan *cyber crime* mengalami peningkatan pesat di Indonesia, Oleh karena itu perlu adanya pendidikan dan penanaman nilai etika digital untuk membangun kesadaran kolektif yang intrinsik, sehingga masyarakat tidak hanya menjadi objek perlindungan tetapi juga subjek aktif dalam menciptakan ruang digital yang aman dan tertib.

Kata kunci: Penegakan Hukum, yuridis normatif, etika digital.



LATAR BELAKANG

Dinamika evolusi Kejahatan di Ruang digital Transformasi digital yang masif telah mengubah cara orang berinteraksi dan sekaligus menghadirkan tantangan baru, yaitu cyber crime yang bersifat internasional, tanpa identitas, dan teknis. Fenomena ini bukan sekadar gangguan sistem, melainkan menjadi ancaman serius terhadap privasi, ekonomi, dan stabilitas negara. Akan tetapi, penanganan kejahatan siber sering terhambat oleh cara penegakan hukum tradisional yang lambat dalam merespon cepatnya perkembangan teknologi. dalam Jurnal Hukum Lex Generalis mengungkapkan bahwa meningkatnya kejahatan siber di Indonesia membutuhkan evaluasi yang mendalam terhadap efektivitas peraturan yang ada, mengingat modus operandi pelaku sering kali lebih maju daripada kemampuan deteksi hukum normatif (Putri et al., 2024).

Fondasi Teori Soerjono Soekanto sebagai Alat Analisis Ketika menghadapi masalah yang kompleks ini, pemikiran klasik Soerjono Soekanto mengenai faktor-faktor yang mempengaruhi penegakan hukum tetap menjadi alat analisis yang sangat relevan. Soekanto mengidentifikasi lima pilar utama: aspek hukum (peraturan), aparat penegak hukum, sarana atau fasilitas, masyarakat, dan budaya. Kelima aspek ini merupakan bagian yang saling terkait dan menentukan keberhasilan penegakan hukum di lapangan. dalam Jurnal Kertha Semaya menekankan bahwa kegagalan dalam menangani kejahatan siber di Indonesia biasanya disebabkan oleh lebih dari satu faktor, tapi juga karena kurangnya keseimbangan di antara lima faktor penegakan hukum tersebut yang belum berjalan secara harmoni (Yustitiana, 2021).

Pentingnya Aspek Hukum dan Kesiapan Aparat Penegak Hukum Secara khusus, aspek hukum (isi undang-undang) dan aparat penegak hukum menjadi garis depan dalam menghadapi serangan siber. Meskipun Indonesia telah memiliki UU ITE dan UU Perlindungan Data Pribadi (PDP), tantangan muncul pada aspek penerapan dan tafsiran pasal-pasal yang dianggap fleksibel. Di sisi lain, keahlian aparat penegak hukum dalam teknik forensik digital menjadi syarat penting yang tidak dapat dinegosiasikan dalam Jurnal Ilmiah Penegakan Hukum mencatat bahwa tanpa adanya integrasi antara regulasi yang menyeluruh dan peningkatan kemampuan teknis aparat, penegakan hukum dalam dunia siber hanya akan menjadi tindakan reaktif yang tidak menasar sumber masalah (R., 2025).

Peran Sarana, Masyarakat, dan Budaya Hukum dalam Ekosistem Siber Akhirnya, keberhasilan penegakan hukum sangat tergantung pada tersedianya sarana teknologi yang mendukung serta respons sosiologis dari masyarakat. Faktor fasilitas, seperti hardware dan software untuk melacak jejak digital, sering menjadi titik lemah karena mahalnya investasi teknologi. Selain itu, masyarakat dan budaya hukum termasuk tingkat literasi digital dan kesadaran hukum warga menentukan sejauh mana regulasi akan diikuti atau justru dicari celahnya. dalam Jurnal Keadilan Masyarakat menyimpulkan bahwa penguatan budaya hukum digital merupakan landasan penting; sebab sekuat apa pun teknologi dan regulasi yang ada, penegakan hukum akan lemah jika masyarakatnya masih memiliki tingkat kepatuhan dan

kesadaran risiko digital yang rendah (Herfindo, 2025).

KAJIAN TEORITIS

1. Hukum dan Dinamika Legislasi Digital

Dalam perspektif Soekanto, faktor hukum bukan sekadar keberadaan teks undang-undang, melainkan sejauh mana kepastian hukum tersebut mampu memayungi realitas sosial. Dalam menghadapi *cyber crime*, tantangan utama terletak pada karakter hukum yang seringkali tertatih mengikuti derap langkah teknologi (*lagging behind the technology*). Meskipun Indonesia memiliki UU ITE, relevansinya sering diuji oleh munculnya modus operandi baru seperti kejahatan berbasis *Artificial Intelligence* (AI) atau *deepfake*. Kedalaman faktor ini menuntut adanya harmonisasi hukum yang tidak hanya bersifat nasional tetapi juga internasional, mengingat sifat *cyber crime* yang lintas batas (*transnational*). Jika rumusan pasal dalam undang-undang terlalu kaku atau justru terlalu multitafsir (pasal karet), maka asas legalitas akan sulit ditegakkan, yang pada akhirnya mengakibatkan kegagalan hukum dalam memberikan perlindungan bagi korban di ruang digital (Rangkuty et al., 2025).

2. Profesionalisme di Era Bit dan Byte

Penegak hukum merupakan ujung tombak yang menentukan apakah hukum hanya menjadi "macan kertas" atau kekuatan nyata. Soerjono Soekanto menekankan bahwa mentalitas dan peran penegak hukum sangat vital. Dalam konteks siber, intelektualitas penegak hukum tidak lagi cukup hanya dengan pemahaman pasal, melainkan harus mencakup literasi digital tingkat lanjut. Seorang penyidik harus memahami mekanisme forensik digital, cara kerja enkripsi, hingga pelacakan transaksi kripto. Kendala yang sering muncul adalah adanya diskoneksi antara kompleksitas kasus siber dengan kapasitas teknis aparat yang belum merata. Tanpa adanya pembaruan pengetahuan yang berkelanjutan (*up-skilling*), penegak hukum akan kesulitan dalam melakukan pembuktian di persidangan, di mana bukti digital bersifat sangat rapuh (*volatile*) dan mudah dimanipulasi (Khabiru, 2026).

3. Infrastruktur Forensik sebagai

Soekanto menegaskan bahwa mustahil hukum ditegakkan secara efektif tanpa fasilitas pendukung yang memadai. Dalam *cyber crime*, sarana bukan lagi sekadar gedung kantor atau kendaraan operasional, melainkan laboratorium digital forensik, perangkat lunak pelacak IP, hingga sistem keamanan siber yang mumpuni. Ketiadaan fasilitas ini akan menghambat



kecepatan respons terhadap kejahatan siber yang terjadi dalam hitungan detik. Investasi pada teknologi pendukung seringkali menjadi titik lemah karena membutuhkan anggaran yang besar dan pemeliharaan yang intensif. Tanpa sarana yang modern, proses penegakan hukum akan kehilangan momentumnya, terutama dalam upaya pemulihan data atau pelacakan pelaku yang bersembunyi di balik jaringan anonimitas seperti *Dark Web* (Waluyo, 2022).

4. Partisipasi dan Literasi Hukum Digital

Efektivitas hukum sangat bergantung pada bagaimana masyarakat memandang dan merespons hukum tersebut. Soerjono Soekanto melihat masyarakat sebagai lingkungan di mana hukum itu berlaku. Dalam fenomena *cyber crime*, sering terjadi fenomena "under-reporting", di mana korban enggan melaporkan kejahatan karena merasa malu (dalam kasus pemerasan seksual/sexortion) atau menganggap kerugian materiil tidak sebanding dengan rumitnya birokrasi pelaporan. Selain itu, rendahnya literasi digital membuat masyarakat menjadi target yang empuk bagi skema *phishing* atau penipuan sosial (*social engineering*). Penegakan hukum akan menjadi sangat berat jika masyarakat tidak memiliki kesadaran kolektif untuk menjaga keamanan data pribadi dan tidak memiliki kepercayaan terhadap sistem peradilan digital (Maskun, S.H., 2022).

5. Pergeseran Nilai di Ruang Maya

Faktor kebudayaan dalam teori Soekanto mencakup nilai-nilai yang mendasari hukum yang berlaku. Kejahatan siber sering kali berakar dari benturan budaya antara dunia nyata dan dunia maya, di mana batas-batas privasi dan etika komunikasi menjadi kabur. Budaya "instan" dan keinginan untuk eksis di media sosial seringkali meniadakan rasa waspada terhadap ancaman siber. Selain itu, adanya persepsi bahwa dunia maya adalah ruang bebas tanpa aturan (anarkisme digital) menciptakan budaya di mana pelanggaran hukum dianggap sebagai hal biasa. Relevansi faktor ini terletak pada upaya membangun kebudayaan hukum baru, yaitu budaya sadar risiko siber yang harus diintegrasikan ke dalam nilai-nilai sosial masyarakat modern agar penegakan hukum tidak hanya bersifat represif (penindakan), tetapi juga preventif (pencegahan) melalui nilai-nilai etika digital (Maskun, S.H., 2022).

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan jenis penelitian yuridis normatif yang difokuskan pada analisis mendalam terhadap konsep serta teori penegakan hukum sebagaimana dikemukakan oleh Soerjono Soekanto, khususnya mengenai relevansi lima faktor penegakan hukum dalam menghadapi fenomena *cyber crime* di era digital. Dengan sifat deskriptif-analitis, penelitian ini bertujuan untuk menggambarkan secara sistematis faktor-faktor penegakan hukum tersebut yang meliputi faktor hukum, penegak hukum, sarana atau fasilitas, masyarakat, serta kebudayaan untuk kemudian dianalisis keterkaitannya dengan dinamika kejahatan siber yang semakin kompleks. Guna mencapai tujuan tersebut, penelitian ini mengandalkan data sekunder

yang mencakup bahan hukum primer berupa peraturan perundang-undangan seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), bahan hukum sekunder yang bersumber dari buku, jurnal ilmiah, dan opini para ahli, serta bahan hukum tersier seperti kamus hukum dan ensiklopedia sebagai pendukung pemahaman konsep (Rangkuty et al., 2025).

Seluruh data dikumpulkan melalui teknik studi kepustakaan (*library research*) dengan mengkaji berbagai literatur yang relevan, yang kemudian diolah menggunakan teknik analisis kualitatif melalui proses interpretasi dan sinkronisasi antara teori klasik Soerjono Soekanto dengan realitas aktual penanganan kejahatan di ruang siber. Dalam pelaksanaannya, penelitian ini mengombinasikan pendekatan konseptual (*conceptual approach*) untuk membedah teori penegakan hukum secara fundamental dan pendekatan perundang-undangan (*statute approach*) untuk meninjau regulasi yang berlaku di Indonesia. Melalui integrasi metode-metode tersebut, penelitian ini diharapkan mampu menyajikan gambaran yang utuh dan komprehensif mengenai sejauh mana teori lima faktor penegakan hukum tetap relevan dan efektif dalam menjawab tantangan serta hambatan penegakan hukum terhadap kejahatan siber di tengah pesatnya perkembangan teknologi informasi saat ini (Rangkuty et al., 2025).

HASIL DAN PEMBAHASAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam berbagai aspek kehidupan masyarakat, termasuk dalam pola kejahatan. Cyber crime menjadi salah satu bentuk kejahatan yang mengalami peningkatan cukup pesat di Indonesia. Hal ini ditandai dengan semakin beragamnya modus operandi yang digunakan oleh pelaku, seperti phishing, penipuan berbasis digital, peretasan sistem, pencurian identitas, hingga penyebaran malware. Fenomena ini tidak hanya merugikan individu, tetapi juga berdampak pada stabilitas ekonomi dan keamanan nasional. Dalam perspektif teori penegakan hukum menurut Soerjono Soekanto, terdapat lima faktor utama yang memengaruhi efektivitas penegakan hukum, yaitu faktor hukum, penegak hukum, sarana atau fasilitas, masyarakat, dan kebudayaan. Kelima faktor ini memiliki relevansi yang sangat kuat dalam menganalisis fenomena cyber crime di era digital (Soekanto, 2011).

Dalam konteks cyber crime, Indonesia telah memiliki regulasi seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang menjadi landasan hukum dalam penindakan kejahatan siber. Namun demikian, dinamika perkembangan teknologi yang sangat cepat sering kali tidak diimbangi dengan pembaruan regulasi yang memadai. Banyak modus kejahatan baru yang belum secara spesifik diatur dalam



peraturan perundang-undangan, sehingga menimbulkan kekosongan hukum atau multitafsir dalam penerapannya. Oleh karena itu, diperlukan pembaruan hukum yang lebih adaptif dan responsif terhadap perkembangan teknologi digital (Haoxing & System, n.d.).

Aparat penegak hukum seperti polisi, jaksa, dan hakim memiliki peran penting dalam menangani kasus cyber crime. Akan tetapi, penanganan kejahatan siber memerlukan keahlian khusus di bidang teknologi informasi, seperti kemampuan digital forensik dan analisis data. Dalam praktiknya, masih ditemukan keterbatasan kompetensi teknis serta kurangnya pelatihan khusus bagi aparat penegak hukum, sehingga penanganan kasus menjadi kurang optimal. Selain itu, koordinasi antar lembaga juga menjadi tantangan tersendiri dalam menangani kejahatan yang bersifat lintas wilayah bahkan lintas negara (Khabiru, 2026).

Penegakan hukum terhadap cyber crime membutuhkan dukungan teknologi yang memadai, seperti perangkat digital forensik, sistem pelacakan data, serta infrastruktur keamanan siber. Namun, tidak semua wilayah di Indonesia memiliki fasilitas tersebut secara merata. Keterbatasan anggaran dan infrastruktur menjadi hambatan dalam meningkatkan efektivitas penegakan hukum terhadap kejahatan siber. Hal ini menunjukkan bahwa modernisasi sarana dan prasarana menjadi kebutuhan mendasak dalam menghadapi tantangan cyber crime (Khabiru, 2026).

Tingkat kesadaran dan literasi digital masyarakat sangat memengaruhi keberhasilan penegakan hukum. Rendahnya pemahaman masyarakat mengenai keamanan digital sering kali menyebabkan mereka menjadi korban kejahatan siber. Selain itu, masih banyak masyarakat yang enggan melaporkan kasus yang dialaminya karena kurangnya kepercayaan terhadap aparat atau ketidaktahuan mengenai prosedur pelaporan (Aabid et al., 2025).

Perubahan budaya masyarakat yang semakin bergantung pada teknologi digital belum sepenuhnya diimbangi dengan kesadaran hukum yang memadai. Kebiasaan membagikan informasi pribadi secara bebas di media sosial, misalnya, menjadi salah satu faktor yang mempermudah pelaku dalam melakukan kejahatan siber. Selain itu, budaya hukum yang masih lemah juga terlihat dari kurangnya kepatuhan terhadap aturan yang berlaku di ruang digital. Hal ini menunjukkan bahwa pembentukan budaya hukum yang kuat menjadi aspek penting dalam mendukung penegakan hukum. Oleh karena itu, faktor penegakan hukum menurut Soerjono Soekanto masih sangat relevan dalam memahami dan menganalisis fenomena cyber crime di era digital (Aabid et al., 2025).

Upaya penanggulangan cyber crime harus dilakukan secara komprehensif, tidak hanya melalui pembaruan regulasi, tetapi juga peningkatan kualitas sumber daya manusia aparat penegak hukum, penyediaan sarana dan prasarana yang memadai, peningkatan literasi digital masyarakat, serta penguatan budaya hukum di tengah masyarakat. Pendekatan yang holistik ini diharapkan mampu menciptakan sistem penegakan hukum yang lebih efektif dan adaptif dalam menghadapi tantangan kejahatan siber di masa depan. Adapun faktor penegakan hukum menurut Soerjono Soekanto sebagai berikut:

1. Faktor hukum (substansi) dalam menghadapi cyber crime

Lonjakan kejahatan berbasis digital memperlihatkan bahwa perangkat hukum tidak bisa lagi berjalan dengan pola yang konvensional. Dalam kerangka Soerjono Soekanto, kualitas hukum menjadi penentu utama efektif atau tidaknya penegakan hukum di masyarakat. Kehadiran Undang-Undang ITE memang menjadi langkah awal, namun dalam praktiknya masih menyisakan persoalan seperti multitafsir dan keterlambatan dalam menjawab perkembangan teknologi digital (Waluyo, 2022).

Perubahan lanskap teknologi seperti *artificial intelligence* dan *deepfake* menghadirkan bentuk kejahatan yang semakin sulit diprediksi. Situasi ini menunjukkan bahwa hukum tidak cukup hanya ada, tetapi harus terus berkembang agar mampu mengimbangi dinamika kejahatan siber yang semakin kompleks. Ketajaman substansi hukum juga tercermin dari sejauh mana norma yang ada mampu menghindari ambiguitas dalam penerapannya. Dalam praktik penegakan hukum *cyber crime*, ketidakjelasan rumusan pasal dapat memicu perbedaan interpretasi di antara aparat penegak hukum, yang pada akhirnya berdampak pada inkonsistensi putusan. Situasi ini menegaskan bahwa pembaruan hukum tidak cukup hanya bersifat kuantitatif, tetapi juga harus memperhatikan kualitas rumusan norma agar lebih tegas dan tidak menimbulkan multitafsir (Maskun, S.H., 2022).

Karakter lintas batas yang melekat pada kejahatan siber turut memperluas kompleksitas penanganannya. Perbedaan yurisdiksi antarnegara sering kali menghambat proses penindakan terhadap pelaku, terutama ketika pelaku berada di wilayah hukum yang berbeda. Kondisi ini mengisyaratkan pentingnya harmonisasi regulasi serta penguatan kerja sama internasional guna menciptakan sistem penegakan hukum yang lebih efektif dalam menghadapi *cyber crime*. Urgensi perlindungan data pribadi semakin mengemuka seiring meningkatnya kasus kebocoran informasi digital di tengah masyarakat. Keberadaan regulasi yang belum sepenuhnya mampu menjamin keamanan data menunjukkan bahwa substansi hukum masih perlu diperkuat, khususnya dalam memberikan perlindungan terhadap hak-hak digital. Dengan demikian, pengembangan hukum siber tidak hanya berorientasi pada penindakan, tetapi juga pada perlindungan preventif bagi masyarakat (Waluyo, 2022).

Kondisi tersebut menunjukkan bahwa substansi hukum dalam penanganan *cyber crime* belum sepenuhnya mampu mengimbangi kompleksitas perkembangan teknologi digital. Ketertinggalan ini tidak hanya berdampak pada lemahnya efektivitas penegakan hukum, tetapi juga berpotensi mengurangi tingkat kepercayaan masyarakat terhadap sistem



hukum itu sendiri. Oleh karena itu, pembaruan hukum perlu diarahkan tidak hanya pada penyesuaian terhadap perkembangan teknologi, tetapi juga pada penguatan kualitas norma agar mampu memberikan kepastian, keadilan, dan perlindungan hukum secara optimal (Waluyo, 2022).

2. Faktor Penegak Hukum

Titik krusial dari penegakan hukum terletak pada kemampuan aparat dalam menerjemahkan aturan ke dalam tindakan nyata. Dalam kasus *cyber crime*, tuntutan terhadap aparat tidak hanya berhenti pada pemahaman hukum, tetapi juga pada penguasaan teknologi digital dan teknik *digital forensics*. Kompleksitas kejahatan siber membuat proses penanganannya jauh lebih rumit dibandingkan kejahatan konvensional (Adinda Lola Sariyani, 2024).

Kondisi di lapangan menunjukkan bahwa kapasitas tersebut belum sepenuhnya terpenuhi. Keterbatasan sumber daya manusia berdampak pada rendahnya efektivitas penanganan perkara *cyber crime*, khususnya dalam proses identifikasi dan pembuktian berbasis digital. Hal ini mempertegas pentingnya peningkatan kualitas aparat sebagai bagian dari strategi penegakan hukum (Adinda Lola Sariyani, 2024).

Kapabilitas aparat penegak hukum dalam merespons kejahatan siber tidak lagi dapat dipahami dalam kerangka konvensional, melainkan harus ditempatkan dalam konteks transformasi digital yang berlangsung secara cepat dan kompleks. Dinamika ini menuntut adanya kemampuan adaptif yang tidak hanya bersifat teknis, tetapi juga analitis dalam membaca pola kejahatan yang terus berkembang. Tanpa kemampuan tersebut, penegakan hukum berpotensi mengalami ketertinggalan struktural terhadap inovasi modus kejahatan yang semakin canggih (Setiawan, 2021).

Kebutuhan akan spesialisasi menjadi konsekuensi logis dari kompleksitas *cyber crime* yang berbasis teknologi tinggi. Penanganan kejahatan siber tidak cukup mengandalkan pendekatan umum, melainkan memerlukan keahlian khusus seperti analisis forensik digital, pelacakan jejak elektronik, serta pemahaman mendalam terhadap sistem jaringan dan keamanan data. Hal ini menunjukkan bahwa penguatan kapasitas aparat harus diarahkan pada pembentukan sumber daya manusia yang profesional dan memiliki kompetensi multidisipliner (Maskun, S.H., 2022).

Pengembangan kualitas aparat penegak hukum juga perlu didukung oleh sistem kelembagaan yang mampu mendorong pembelajaran berkelanjutan. Integrasi antara pelatihan teknis, kolaborasi dengan pakar teknologi, serta pemanfaatan inovasi digital menjadi langkah strategis dalam meningkatkan efektivitas penegakan hukum. Dengan demikian, peran aparat tidak hanya terbatas sebagai pelaksana hukum, tetapi juga sebagai aktor yang mampu beradaptasi dan berinovasi dalam menghadapi tantangan *cyber crime* (Adinda Lola Sariyani, 2024).

Kondisi tersebut menunjukkan bahwa peran aparat penegak hukum dalam menghadapi *cyber crime* tidak lagi bersifat konvensional, melainkan menuntut transformasi yang berkelanjutan seiring dengan perkembangan teknologi digital. Ketidaksiapan dalam mengimbangi kompleksitas tersebut berpotensi menurunkan efektivitas penegakan hukum, bahkan

membuka celah bagi pelaku kejahatan siber untuk terus berinovasi. Oleh karena itu, penguatan kapasitas aparat tidak hanya menjadi kebutuhan teknis, tetapi juga merupakan bagian dari strategi sistemik dalam menciptakan penegakan hukum yang responsif dan adaptif (Maskun, S.H., 2022).

3. Faktor Sarana dan Fasilitas

Kinerja penegakan hukum tidak dapat dilepaskan dari dukungan teknologi yang memadai. Penanganan *cyber crime* membutuhkan perangkat seperti laboratorium forensik digital, sistem pelacakan data, serta teknologi keamanan jaringan untuk mengungkap bukti-bukti yang bersifat digital. Tanpa dukungan tersebut, proses pembuktian akan mengalami kesulitan yang signifikan (Maskun, S.H., 2022).

Di sisi lain, cepatnya perkembangan teknologi menuntut pembaruan fasilitas secara terus-menerus. Hal ini menjadi tantangan karena memerlukan biaya besar dan perencanaan yang matang. Oleh karena itu, sinergi antara pemerintah dan berbagai pihak menjadi penting dalam memperkuat infrastruktur keamanan siber (Fadhlin Ade Chandra & Fadhillatu Jahra Sinaga, 2021).

Ketersediaan sarana dan fasilitas dalam penegakan hukum *cyber crime* tidak hanya berfungsi sebagai alat pendukung, melainkan sebagai elemen strategis yang menentukan keberhasilan proses penanganan perkara. Kompleksitas kejahatan siber yang berbasis teknologi menuntut adanya infrastruktur yang tidak sekadar memadai, tetapi juga mutakhir dan terintegrasi. Dalam perspektif Soerjono Soekanto, keberadaan fasilitas yang tidak seimbang dengan tuntutan perkembangan kejahatan akan berimplikasi pada lemahnya daya jangkau penegakan hukum itu sendiri (Maskun, S.H., 2022).

Tuntutan terhadap modernisasi infrastruktur penegakan hukum juga mengarah pada kebutuhan sistem yang mampu mengelola dan menganalisis data dalam skala besar. Perangkat teknologi seperti *big data analytics*, sistem pemantauan jaringan, serta kecerdasan buatan menjadi instrumen penting dalam mendeteksi dan mencegah kejahatan siber secara lebih efektif. Hal ini menunjukkan bahwa orientasi penguatan sarana tidak lagi bersifat konvensional, melainkan telah bergeser ke arah digitalisasi yang komprehensif (Maskun, S.H., 2022).

Keterbatasan anggaran dan distribusi fasilitas yang belum merata menjadi tantangan struktural dalam penguatan sarana penegakan hukum. Oleh karena itu, diperlukan strategi kolaboratif yang melibatkan pemerintah, sektor swasta, dan lembaga internasional dalam membangun ekosistem keamanan siber yang berkelanjutan. Dengan demikian, sarana dan fasilitas tidak hanya berperan sebagai pendukung teknis, tetapi juga sebagai fondasi utama dalam menciptakan



efektivitas penegakan hukum di era digital. (Rahardjo, 2009).

Ketidakseimbangan antara tuntutan kompleksitas kejahatan siber dengan kesiapan infrastruktur penegakan hukum memperlihatkan adanya celah struktural dalam sistem hukum digital. Keterbatasan ini tidak hanya berimplikasi pada terhambatnya proses pembuktian, tetapi juga berpotensi menurunkan daya saing aparat dalam menghadapi kejahatan yang semakin berbasis teknologi tinggi. Dalam konteks ini, penguatan sarana dan fasilitas tidak dapat lagi dipahami sebagai kebutuhan tambahan, melainkan sebagai prasyarat utama bagi keberlangsungan penegakan hukum yang efektif di ruang siber (Maskun, S.H., 2022).

4. Faktor Masyarakat

Fenomena *cyber crime* tidak dapat dilepaskan dari kondisi masyarakat sebagai pengguna utama teknologi digital. Rendahnya literasi digital membuat masyarakat rentan terhadap berbagai bentuk kejahatan seperti penipuan online dan pencurian data pribadi. Situasi ini menunjukkan bahwa kesadaran hukum masyarakat masih berada pada tingkat yang perlu ditingkatkan (Waluyo, 2022).

Tidak hanya sebagai korban, masyarakat juga berpotensi menjadi pelaku, misalnya dalam penyebaran hoaks atau ujaran kebencian di media sosial. Hal ini menegaskan bahwa peran masyarakat sangat menentukan dalam keberhasilan penegakan hukum, sehingga edukasi digital menjadi langkah yang tidak dapat diabaikan (Setiawan, 2021).

Dinamika masyarakat digital memperlihatkan adanya relasi yang erat antara tingkat literasi dengan kerentanan terhadap kejahatan siber. Rendahnya kemampuan dalam memahami keamanan digital, verifikasi informasi, serta pengelolaan data pribadi memperbesar peluang terjadinya pelanggaran hukum di ruang siber. Dalam perspektif Soerjono Soekanto, kondisi ini menunjukkan bahwa efektivitas penegakan hukum tidak hanya ditentukan oleh aparat, tetapi juga oleh kualitas kesadaran hukum masyarakat itu sendiri (Waluyo, 2022).

Transformasi perilaku masyarakat di era digital juga menghadirkan kecenderungan baru, di mana batas antara pelaku dan korban menjadi semakin kabur. Kemudahan akses teknologi memungkinkan individu untuk terlibat dalam tindakan melanggar hukum tanpa disadari, seperti menyebarkan informasi yang tidak terverifikasi. Hal ini menandakan bahwa persoalan *cyber crime* tidak semata-mata bersifat kriminal, tetapi juga berkaitan dengan aspek sosial dan edukatif. (Widodo, 2011).

Penguatan peran masyarakat dalam penegakan hukum menuntut adanya strategi yang berorientasi pada peningkatan literasi digital secara komprehensif. Edukasi mengenai etika digital, keamanan informasi, serta konsekuensi hukum dari aktivitas di ruang siber menjadi langkah penting dalam membangun kesadaran kolektif. Dengan demikian, masyarakat tidak hanya berfungsi sebagai objek perlindungan, tetapi juga sebagai subjek aktif dalam menciptakan ruang digital yang aman dan tertib (Waluyo, 2022).

Dualitas posisi masyarakat dalam ruang digital menegaskan bahwa dinamika *cyber crime* tidak dapat dipahami hanya sebagai persoalan pelanggaran hukum, tetapi

juga sebagai refleksi dari tingkat kematangan sosial dalam memanfaatkan teknologi. Kerentanan yang muncul bukan semata akibat faktor eksternal, melainkan berkaitan erat dengan rendahnya kemampuan individu dalam mengelola informasi dan memahami konsekuensi dari setiap aktivitas digital. Dalam konteks ini, penguatan peran masyarakat menuntut lebih dari sekadar peningkatan literasi, tetapi juga pembentukan kesadaran reflektif yang mampu mengarahkan perilaku digital secara bertanggung jawab (Waluyo, 2022).

5. Faktor Budaya Hukum

Realitas di ruang digital menunjukkan adanya perubahan pola perilaku yang berbeda dengan kehidupan di dunia nyata. Anonimitas yang ditawarkan internet sering kali mendorong individu untuk bertindak tanpa mempertimbangkan norma hukum yang berlaku. Kondisi ini mencerminkan lemahnya budaya hukum dalam konteks digital (Fadhlin Ade Chandra & Fadhillatu Jahra Sinaga, 2021).

Penguatan budaya hukum menjadi langkah penting untuk menciptakan kesadaran yang berasal dari dalam diri masyarakat. Melalui pendidikan dan penanaman nilai etika digital, diharapkan terbentuk perilaku yang lebih bertanggung jawab dalam penggunaan teknologi. Dengan demikian, budaya hukum berperan sebagai fondasi jangka panjang dalam penegakan hukum terhadap *cyber crime* (Maskun, S.H., 2022).

Transformasi interaksi sosial di ruang digital memperlihatkan adanya pergeseran nilai dan norma yang memengaruhi perilaku individu dalam berhadapan dengan hukum. Anonimitas dan minimnya kontrol sosial langsung menciptakan ruang yang memungkinkan terjadinya *disinhibition effect*, yaitu kecenderungan individu untuk bertindak di luar batas norma yang berlaku. Dalam kerangka Soerjono Soekanto, kondisi ini menunjukkan bahwa internalisasi nilai hukum dalam masyarakat digital belum terbentuk secara optimal (Fadhlin Ade Chandra & Fadhillatu Jahra Sinaga, 2021).

Kerapuhan budaya hukum di ruang siber juga tercermin dari rendahnya rasa tanggung jawab dalam penggunaan teknologi, seperti maraknya penyebaran konten negatif, pelanggaran privasi, hingga tindakan perundungan digital. Fenomena ini menegaskan bahwa keberadaan aturan hukum saja tidak cukup tanpa diimbangi dengan kesadaran moral yang kuat dari individu sebagai pengguna teknologi (Waluyo, 2022).

Penguatan budaya hukum dalam konteks digital memerlukan pendekatan yang bersifat edukatif dan berkelanjutan. Penanaman nilai-nilai etika digital, peningkatan kesadaran hukum, serta pembentukan sikap bertanggung jawab menjadi elemen penting dalam membangun kepatuhan yang bersifat intrinsik. Dengan demikian, budaya hukum tidak hanya berfungsi sebagai pelengkap, tetapi sebagai fondasi utama dalam menciptakan efektivitas penegakan hukum terhadap *cyber crime* dalam jangka panjang (Waluyo, 2022).



Rapuhnya internalisasi nilai hukum dalam ruang digital menandakan bahwa tantangan utama penegakan hukum tidak lagi terbatas pada aspek regulatif, melainkan menyentuh dimensi kultural yang lebih mendasar. Ketika norma hukum tidak terinternalisasi dalam kesadaran individu, maka keberadaan aturan hanya akan berfungsi secara formal tanpa daya ikat yang kuat dalam praktiknya. Dalam kerangka Soerjono Soekanto, kondisi ini memperlihatkan bahwa budaya hukum menjadi faktor penentu yang bersifat laten namun krusial dalam menentukan keberhasilan penegakan hukum. Oleh karena itu, penguatan budaya hukum di era digital harus diarahkan pada pembentukan kesadaran normatif yang mampu mengintegrasikan nilai hukum ke dalam perilaku sehari-hari masyarakat (Fadhlin Ade Chandra & Fadhillatu Jahra Sinaga, 2021).

Keterkaitan antara faktor hukum, penegak hukum, sarana dan fasilitas, masyarakat, serta budaya hukum menunjukkan bahwa penegakan hukum dalam menghadapi *cyber crime* merupakan suatu sistem yang tidak dapat dipisahkan satu sama lain. Setiap faktor memiliki kontribusi sekaligus keterbatasan yang saling memengaruhi, sehingga kelemahan pada satu aspek akan berdampak pada efektivitas keseluruhan sistem penegakan hukum. Dalam kerangka pemikiran Soerjono Soekanto, dinamika ini menegaskan bahwa pendekatan parsial tidak lagi memadai untuk menjawab kompleksitas kejahatan siber yang terus berkembang (Maskun, S.H., 2022).

Kompleksitas tersebut memperlihatkan adanya pergeseran karakter penegakan hukum dari yang bersifat konvensional menuju pendekatan yang lebih adaptif, integratif, dan berbasis teknologi. Di satu sisi, tuntutan terhadap pembaruan regulasi dan peningkatan kapasitas aparat menjadi semakin mendesak, sementara di sisi lain, penguatan kesadaran masyarakat dan budaya hukum digital juga tidak dapat diabaikan. Oleh karena itu, efektivitas penegakan hukum terhadap *cyber crime* hanya dapat tercapai melalui sinergi antar seluruh faktor, yang mampu beradaptasi secara berkelanjutan terhadap perkembangan teknologi dan dinamika sosial di era digital (Maskun, S.H., 2022).

KESIMPULAN

Gelombang digitalisasi yang melanda dunia telah membuka tirai kejahatan jenis baru: *cyber crime*, sebuah momok tak kasat mata yang mengintai privasi, ekonomi, dan bahkan kedaulatan bangsa. Di tengah pusaran ancaman ini, teori lima faktor penegakan hukum Soerjono Soekanto terbukti bukan sekadar kerangka usang, melainkan sebuah kompas esensial yang menyingkap akar masalah penanganan *cyber crime* di Indonesia. Kegagalan kita bukanlah pada satu titik, melainkan pada ketidakselarasan orkestra penegakan hukum itu sendiri.

Undang-undang kita masih terengah-engah mengejar kecepatan inovasi digital, sering kali menghasilkan "pasal karet" yang multitafsir dan membiarkan batas-batas etika serta hukum kian kabur di dunia maya. Garda terdepan kita, para penegak hukum, sering kali harus bertarung dengan 'senjata' yang usang, menghadapi kejahatan canggih dengan kapasitas teknis yang jauh tertinggal. Infrastruktur digital yang

memadai, dari laboratorium forensik hingga perangkat pelacak IP, masih menjadi kemewahan, padahal ia adalah tulang punggung perjuangan ini. Ironisnya, masyarakat, benteng pertahanan terakhir, justru sering menjadi sasaran empuk, terjebak dalam jebakan *phishing* atau *social engineering* akibat rendahnya literasi digital dan rasa malu untuk melaporkan. Puncaknya, di alam maya, anonimitas sering disalahartikan sebagai impunitas, melahirkan "anarkisme digital" yang meruntuhkan etika dan norma, mengubah internet menjadi rimba tanpa hukum.

Oleh karena itu, penyelesaian *cyber crime* bukan sekadar menambal satu lubang, melainkan sebuah proyek nasional multidimensional. Ini menuntut sebuah simfoni kolaborasi yang harmonis: pendidikan digital adalah fondasi yang kokoh, pelatihan penegak hukum adalah pilar yang tak tergoyahkan, investasi teknologi adalah mesin pendorong yang tak henti, dan kolaborasi lintas sektor serta internasional adalah jembatan penghubung yang esensial. Transformasi hukum dari reaktif menjadi proaktif, dari penghukum menjadi pelindung, adalah sebuah keniscayaan. Hanya dengan merajut kelima elemen ini secara utuh, dengan fokus pada pencegahan dan penanaman etika digital, kita dapat membangun ekosistem siber yang berintegritas, mengembalikan kepercayaan publik, dan mewujudkan janji Indonesia akan masa depan digital yang aman dan berkeadaban.

DAFTAR PUSTAKA

- 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. <https://ulilalbabinstitute.id/index.php/PESHUM/article/view/8311/6317>
- Adinda Lola Sariyani. (2024). Efektivitas Penegakan Hukum Terhadap Kejahatan Siber di Indonesia. *Al-Dalil, Jurnal Ilmu Sosial, Politik, Dan Hukum*, 2(2).
- Fadhlin Ade Chandra, & Fadhillatu Jahra Sinaga. (2021). Peran Penegak Hukum dalam Penegakan Hukum di Indonesia. *Edu Society: Jurnal Pendidikan, Ilmu Sosial, Dan Pengabdian Kepada Masyarakat*, 1(1), 41–50.
- Haoping, Z., & System, C. (n.d.). *No 主観的健康感を中心とした在宅高齢者における健康関連指標に関する共分散構造分析* Title. 98–106.
- Herfindo, R. (2025). Analisis Sosiologi Hukum Atas Tindak Pidana ITE: Studi Kasus Pemerasan Dan Pengancaman Yang Merugikan Hak Orang Lain. *Judge : Jurnal Hukum*, 6(03), 379–384. <https://doi.org/10.54209/judge.v6i03.1491>



- Khabiru, A. (2026). *Efektivitas Penegakan Hukum terhadap Kejahatan Siber oleh Polri dalam Perspektif Kitab Undang-Undang Hukum Pidana KUHP Baru di Kota Samarinda*. 2(April), 70–82.
- Maskun, S.H., L. M. (2022). *Kejahatan Siber (Cyber Crime): Suatu Pengantar*. KENCANA.
[https://books.google.co.id/books?id=b1S6EAAAQBAJ&lpg=PA88&ots=qbXtguExKz&dq=Maskun%2C S. H. \(2022\). Kejahatan Siber \(Cyber Crime\)%3A Suatu Pengantar. Prenada Media.&lr&hl=id&pg=PR4#v=onepage&q=Maskun, S. H. \(2022\). Kejahatan Siber \(Cyber Crime\): Suatu Pengantar. Prenada Media.&f=false](https://books.google.co.id/books?id=b1S6EAAAQBAJ&lpg=PA88&ots=qbXtguExKz&dq=Maskun%2C%20S.H.%20(2022).%20Kejahatan%20Siber%20(Cyber%20Crime)%3A%20Suatu%20Pengantar.%20Prenada%20Media.&lr&hl=id&pg=PR4#v=onepage&q=Maskun,S.H.(2022).KejahatanSiber(CyberCrime):SuatuPengantar.PrenadaMedia.&f=false)
- Putri, A., Sari, N., Fajrina, P., & Aisyah, S. (2024). Keamanan Online dalam Media Sosial: Pentingnya Perlindungan Data Pribadi di Era Digital (Studi Kasus Desa Pematang Jering). *Jurnal Pengabdian Nasional (JPN) Indonesia*, 6(1), 38–52. <https://doi.org/10.35870/jpni.v6i1.1097>
- R., W. B. (2025). Tantangan Penegakan Hukum terhadap Kejahatan Berbasis Teknologi AI. *INNOVATIVE: Journal of Social Science Research*, 5(1), 3436–3451. <https://doi.org/10.31004/innovative.v5i1.17519>
- Rangkuty, P. R., Sinaga, A. P., Abdillah, M., Yoga, A. R., Sahriyan, I., Telaumbanua, R. N., & Tanjung, W. N. (2025). Peran Literasi Digital dalam Mencegah Kejahatan Siber di Kalangan Generasi Muda. *Jurnal Penelitian Ilmiah Multidisipliner*, 1(04), 1116–1127.
- Setiawan, M. N. (2021). Mengkritisi Undang-Undang ITE Pasal 27 Ayat (3) dilihat dari Sosio-Politik Hukum Pidana Indonesia. *Datin Law Jurnal*, 2(1), 1–21. <http://dx.doi.org/10.36355/dlj.v1i1OpenAccessat:https://ojs.umb-bungo.ac.id/index.php/DATIN/index>
- Waluyo, B. (2022). *PENEGAKAN HUKUM DI INDONESIA*. SINAR GARFIKA.
[https://books.google.co.id/books?id=LA5zEAAAQBAJ&lpg=PP1&ots=9Nx5qffqy&dq=penegakanhukum &lr&hl=id&pg=PP1#v=onepage&q=penegakanhukum &f=false](https://books.google.co.id/books?id=LA5zEAAAQBAJ&lpg=PP1&ots=9Nx5qffqy&dq=penegakanhukum&lr&hl=id&pg=PP1#v=onepage&q=penegakanhukum&f=false)
- Yustitiana, R. (2021). Pelaksanaan Pengaturan Hukum Tindak Kejahatan Fraud Phishing Transaksi Elektronik Sebagai Bagian Dari Upaya Penegakan Hukum Di Indonesia Dikaitkan Dengan Teori Efektivitas Hukum. *Jurnal Hukum Visio Justisia*, 1, 98–126. <file:///C:/Users/anton/Downloads/3802-12185-4-PB.pdf>