

Peran Polisi Dalam Penegakan Hukum di Era Digitalisasi

¹Muhammad Fahrul Ikwan Ritonga, ²Ibrahim Fikma Edrisy,

^{1,2}Universitas Terbuka, Indonesia

E-mail: 1alungritonga7@gmail.com, 2ibrahimfikmaedrisy@gmail.com

Article History

Submission : 19-06-2026
Received : 10-08-2026
Revised : 16-08-2026
Accepted : 17-08-2026

Abstract

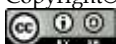
This study aims to normatively examine the role of the police in law enforcement in the digital era, including their preventive and repressive functions, the underlying legal framework, as well as the challenges and necessary measures for strengthening their role. This study employs a normative legal research method using a statutory approach, secondary data, and literature review (library research), which are analyzed descriptively and qualitatively. The results show that the role of the police in law enforcement in the digital era encompasses preventive and repressive functions. The preventive function is carried out through cyber patrols, increasing public digital legal literacy, and strengthening cooperation with the private sector and digital platforms. Meanwhile, the repressive function is carried out through the investigation and prosecution of cybercrime, the collection and securing of electronic evidence, the application of digital forensics, and cross-jurisdictional cooperation. The implementation of these two functions must continue to uphold legal certainty, human rights protection, and the principle of prudence in the use of digital technology. Therefore, law enforcement in the digital era requires strengthening police capacity in terms of technological capabilities, human resources, and cross-sectoral cooperation while upholding legal certainty and protecting human rights.

Keywords: Cybercrime, Digitalization, Police, Law enforcement

Abstrak

Penelitian bertujuan untuk mengkaji secara normatif keterlibatan kepolisian dalam penegakan hukum di era digital, mencakup fungsi preventif dan represifnya, landasan hukum yang mendasarinya, serta hambatan dan langkah-langkah penting untuk penguatan. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan (*statute approach*), menggunakan data sekunder, yang dikumpulkan melalui studi kepustakaan (*library research*) dan dianalisis secara deskriptif kualitatif. Hasil penelitian menunjukkan bahwa peran polisi dalam penegakan hukum di era digitalisasi mencakup fungsi preventif dan represif. Fungsi preventif dilakukan melalui patroli siber, peningkatan literasi hukum digital masyarakat, serta penguatan kerja sama dengan sektor swasta dan platform digital. Sementara itu, fungsi represif dilakukan melalui penyelidikan dan penyidikan tindak pidana siber, pengumpulan serta pengamanan alat bukti elektronik, penerapan forensik digital, dan kerja sama lintas yurisdiksi. Pelaksanaan kedua fungsi tersebut perlu tetap memperhatikan kepastian hukum, perlindungan hak asasi manusia, dan prinsip kehati-hatian dalam penggunaan teknologi digital. Dengan demikian, penegakan hukum di era digitalisasi memerlukan penguatan kapasitas kepolisian dalam aspek teknologi, sumber daya manusia, dan kerja sama lintas sektor dengan tetap menjunjung kepastian hukum dan perlindungan hak asasi manusia.

Kata Kunci: Digitalisasi, Penegakan hukum, Polisi, Tindak pidana siber



Pendahuluan

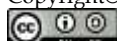
Kehadiran teknologi digital dalam kehidupan sehari-hari masyarakat Indonesia bukan lagi menjadi pelengkap melainkan telah berubah menjadi kebutuhan pokok yang menyentuh hampir seluruh dimensi kehidupan (Indonesia, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik, 2024). Perubahan ini terlihat dari semakin luasnya penggunaan internet dan perangkat *mobile* serta berbagai aplikasi digital yang mendukung aktivitas ekonomi, pendidikan, komunikasi, hingga pelayanan publik. Ruang digital kini menjadi tempat bertemunya kepentingan ekonomi, sosial, budaya, bahkan politik secara bersamaan. Interaksi manusia yang sebelumnya terbatas oleh ruang dan waktu kini menjadi tanpa batas dan masif. Di balik kemajuan yang ditawarkan oleh era digitalisasi ini, tersembunyi ancaman hukum yang terus berkembang secara dinamis dan tidak mengenal batas wilayah. Kondisi tersebut menempatkan institusi kepolisian pada posisi yang strategis sekaligus penuh tantangan dalam menjalankan fungsinya sebagai penegak hukum di era yang serba digital (Kementerian Komunikasi dan Informatika Republik Indonesia, 2023).

Bedasarkan karakteristik kejahatan siber, kejahatan digital memiliki ciri-ciri yang secara tersirat berbeda dari kejahatan konvensional karena dilakukan dengan memanfaatkan sistem komputer, internet, dan berbagai platform digital. Pelaku kejahatan tidak perlu hadir secara langsung di lokasi untuk memanfaatkan kelemahan sistem dan kelalaian pengguna, akan tetapi kejahatan ini dapat dilakukan dari jarak jauh. Kondisi tersebut tentu dapat memungkinkan pelaku untuk bertindak secara anonim dan melintasi batas yurisdiksi hingga menggunakan metode yang sulit diidentifikasi dengan teknik pemantauan konvensional. Fleksibilitas dan kemudahan akses ranah digital secara signifikan membuat metode pengumpulan bukti dan pelacakan menjadi semakin sulit.

Penyebaran informasi yang cepat serta karakteristik jejak digital yang mudah diubah dan dimanipulasi oleh pelaku menjadi salah satu karakteristik kejahatan siber, terutama dalam upaya memperoleh atau menyalahgunakan data pribadi korban. Untuk melancarkan aksinya, pelaku dapat memanfaatkan kelemahan sistem keamanan maupun rendahnya literasi digital masyarakat. Data pribadi yang tersebar di berbagai platform digital sering kali menjadi pintu masuk utama bagi pelaku untuk melakukan berbagai tindak kejahatan mulai dari penipuan dan pencurian identitas hingga pemerasan. Hal tersebut mendorong munculnya bentuk-bentuk kejahatan baru yang semakin kompleks termasuk praktik pemerasan melalui media digital seperti *sextortion*, *doxing*, bahkan ancaman penyebaran data pribadi atau konten sensitif.

Kondisi ini tidak hanya menimbulkan kerugian finansial, tetapi juga dapat memberikan dampak psikologis yang signifikan terhadap korban. Rasa takut dan tekanan psikologis hingga kerusakan reputasi menjadi dampak yang harus dihadapi oleh korban. Ini menunjukkan bahwa penegakan hukum tidak hanya dituntut untuk mengidentifikasi dan menangkap pelaku, tetapi juga memberikan perlindungan yang memadai kepada korban. Hal tersebut menuntut agar petugas kepolisian tidak hanya memiliki keterampilan teknis akan tetapi juga kemampuan beradaptasi dengan laju kemajuan teknologi yang terus meningkat (Indonesia, Peraturan Pemerintah Nomor 28 Tahun 2024 tentang Pelaksanaan Undang-Undang Kesehatan, 2024).

Masalah dalam menangani kejahatan siber juga berkaitan dengan kerja sama lintas batas dan masalah regulasi. Lembaga penegak hukum dari berbagai negara harus bekerja sama secara erat, sedangkan regulasi juga perlu mengikuti kemajuan teknologi yang pesat untuk memerangi sifat kejahatan siber yang tidak mengenal batas. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) merupakan salah satu instrumen hukum utama



yang digunakan di Indonesia untuk memerangi kejahatan siber, akan tetapi undang-undang ini masih menghadapi berbagai tantangan dalam hal implementasi dan penyesuaian terhadap jenis-jenis kejahatan siber baru yang terus berkembang.

Penerapan teknologi digital memiliki kelebihan dan kekurangan yang tidak dapat dipisahkan. Digitalisasi memberikan kemudahan dan efisiensi dalam berbagai aspek kehidupan, tetapi di sisi lain juga membuka peluang bagi kejahatan untuk berkembang dengan pola dan modus yang semakin kompleks. Oleh karena itu, diperlukan upaya bersama dari pemerintah dan lembaga penegak hukum serta masyarakat umum untuk membangun ekosistem digital yang aman dan terpercaya. Strategi utama untuk menghadapi tantangan kejahatan siber di era digital saat ini meliputi peningkatan literasi digital dan penguatan langkah-langkah keamanan serta penegakan hukum dengan tegas dan fleksibel (Kempa et al., 2025).

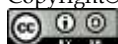
Bentuk nyata dari kejahatan digital yakni berupa penipuan, eksploitasi data pribadi, dan penyebaran konten yang melanggar kesusilaan hingga ancaman siber yang menasar layanan publik. Berbagai bentuk kejahatan tersebut menunjukkan bahwa ruang siber telah menjadi ranah baru yang rawan terhadap pelanggaran hukum dengan modus yang semakin kompleks dan terorganisir. Kejahatan-kejahatan tersebut memanfaatkan kelemahan manusia sebagai pengguna teknologi sekaligus celah dalam sistem keamanan digital sehingga penanganannya tidak dapat disamakan dengan kejahatan konvensional (United Nations Office on Drugs and Crime, 2023).

Proses penegakan hukum oleh kepolisian di dunia digital harus berlandaskan prinsip-prinsip hak asasi manusia. Setiap kegiatan penegakan hukum harus tetap mengedepankan hak atas keamanan dan perlindungan privasi serta kebebasan berekspresi sebagai landasan utama. Hal ini sangatlah penting mengingat adanya potensi penyalahgunaan wewenang dalam pengawasan dunia maya, yang apabila tidak diatur dan diawasi secara cermat maka akan mengakibatkan terjadinya pelanggaran hak-hak individu. Keseimbangan antara keamanan dan kebebasan merupakan komponen penting dalam pemberantasan kejahatan digital (National Institute of Standards and Technology, 2022).

Tingginya tingkat kerumitan kejahatan digital menuntut strategi penegakan hukum yang didasarkan pada kerja sama lintas sektor, penghormatan terhadap hak asasi manusia, hingga pemahaman teknologi yang memadai, tidak hanya mengandalkan kewenangan regulasi. Ancaman kejahatan siber akan terus meluas di era digital dan bahkan berpotensi mengancam keamanan nasional serta stabilitas sosial dan ekonomi, jika tidak dilakukan upaya yang komprehensif dan berkelanjutan (Suhariyanto, 2023). Berdasarkan data dari Kementerian Komunikasi dan Informatika, pada tahun 2023 terdapat lebih dari 215 juta pengguna internet aktif di Indonesia dengan tingkat penetrasi sekitar 78% dari populasi negara. Hal ini menunjukkan bahwa dunia maya kini menjadi bagian tak terpisahkan dari kehidupan sehari-hari dan masyarakat telah mengadopsi teknologi digital secara luas. Koneksi internet yang luas dan berkelanjutan pada era sekarang sangat diperlukan untuk hampir segala macam aktivitas termasuk transaksi ekonomi dan pendidikan, komunikasi hingga layanan pemerintah.

Meningkatnya potensi risiko kejahatan siber beriringan dengan tingginya persentase penduduk yang mengakses internet. Tidak semua pengguna memiliki tingkat literasi digital yang memadai sehingga kerentanan terhadap berbagai bentuk kejahatan seperti penipuan online dan *phishing*, pencurian data hingga pemerasan digital menjadi semakin tinggi. Kondisi tersebut menunjukkan adanya ketidakseimbangan antara laju perkembangan teknologi dengan kesiapan masyarakat dalam menghadapinya.

Banyaknya masyarakat Indonesia yang menggunakan internet menandakan



kemajuan digital menjadi suatu tantangan besar dalam mewujudkan ruang siber yang aman. Sangat diperlukan adanya upaya terpadu yang mencakup pendidikan masyarakat dan peraturan yang lebih ketat serta peningkatan sistem keamanan digital guna mengurangi risiko kejahatan siber dan melindungi kepentingan publik secara luas (Kementerian Komunikasi dan Informatika Republik Indonesia, 2023). Semakin banyak orang yang terlibat dalam dunia digital maka semakin besar pula kemungkinan terjadinya pelanggaran hukum sehingga memerlukan perhatian dari lembaga penegak hukum terutama kepolisian yang berada di garis depan sistem peradilan pidana (Kepolisian Negara Republik Indonesia, 2023).

Kepolisian di Indonesia secara normatif memiliki wewenang yang cukup kuat untuk berperan dalam penegakan hukum di ranah digital. Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia memberikan landasan kewenangan yang bersifat umum, sementara pembaruan UU ITE melalui Undang-Undang Nomor 1 Tahun 2024 memperjelas ruang lingkup tindak pidana elektronik beserta mekanisme penanganannya (Hamzah, 2015). Akan tetapi, regulasi semata tidak pernah cukup. Efektif atau tidaknya penegakan hukum ditentukan oleh sejauh mana norma hukum tersebut mampu diimplementasikan secara konsisten dan proporsional serta berkeadilan di lapangan. Berdasarkan kompleksitas permasalahan tersebut, penelitian ini berfokus pada bagaimana peran kepolisian dalam penegakan hukum di era digitalisasi. Fokus tersebut mencakup landasan kewenangan kepolisian dalam penegakan hukum di ruang digital serta pelaksanaan fungsi preventif dan represif dalam menghadapi berbagai bentuk kejahatan digital.

Metode Penelitian

Kajian ini menggunakan metode penelitian hukum normatif dengan menggunakan data sekunder yang terdiri atas bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier (Muladi & Arief, 2022). Pendekatan penelitian yang digunakan adalah pendekatan perundang-undangan (*statute approach*) untuk mengkaji peraturan perundang-undangan yang berkaitan dengan peran polisi dalam penegakan hukum di era digitalisasi.

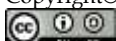
Bahan hukum primer yang digunakan meliputi Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia (Indonesia, Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia, 2002), Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), serta peraturan internal kepolisian seperti Peraturan Kapolri dan Surat Edaran Kapolri yang mengatur mekanisme patroli siber dan penanganan tindak pidana digital. Jurnal hukum, literatur akademis, risalah, temuan penelitian, dan laporan kinerja dari organisasi terkait merupakan contoh bahan hukum sekunder. Ensiklopedia hukum, kamus, dan sumber daya internet yang relevan merupakan contoh sumber hukum tersier.

Teknik pengumpulan data dilakukan melalui studi kepustakaan (*library research*) dan kajian dokumen secara sistematis. Analisis data menggunakan metode deskriptif kualitatif, yaitu memaparkan temuan secara sistematis, menafsirkan kesesuaian norma terhadap praktik penerapan hukum, serta merumuskan penilaian normatif terhadap permasalahan yang diteliti (Tahir et al., 2023).

Hasil dan Pembahasan

Peran Polisi dalam Penegakan Hukum di Era Digitalisasi

Penegakan hukum merupakan suatu proses perwujudan ide-ide hukum dari yang bersifat abstrak menjadi kenyataan yang konkret dan dapat dirasakan oleh seluruh anggota masyarakat. Penegakan hukum di era digital telah melampaui ranah fisik dan merambah ke



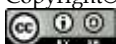
dunia maya melintasi batas-batas yurisdiksi tradisional. Kepolisian sebagai bagian penting dari sistem peradilan pidana, memiliki tanggung jawab untuk mengatasi masalah-masalah ini dengan menerapkan strategi yang terukur dan sesuai hukum serta fleksibel. Transformasi ruang kejahatan dari fisik ke digital menuntut perubahan sudut pandang dalam praktik penegakan hukum. Lembaga penegak hukum di dunia maya berperan sebagai analis dan pengelola risiko. Hal tersebut menuntut pemahaman yang mendalam tentang teknologi informasi dan kemampuan untuk menganalisis data dalam jumlah besar serta pemahaman secara menyeluruh terhadap tren kejahatan siber yang terus berubah. Tanpa kemampuan tersebut, penegakan hukum berpotensi tertinggal dari kecepatan inovasi yang dimanfaatkan oleh pelaku kejahatan.

Karakter lintas batas (*borderless*) dari kejahatan siber menjadi tantangan tersendiri dalam aspek yurisdiksi hukum. Suatu tindak pidana dapat dilakukan di satu negara menggunakan server di negara lain dan menimbulkan kerugian di negara yang berbeda. Kondisi ini menuntut adanya kerja sama internasional yang kuat, baik dalam bentuk perjanjian bilateral maupun multilateral agar dapat mempermudah proses penyelidikan dan penyidikan hingga penegakan hukum terhadap pelaku. Upaya penegakan hukum akan menghadapi tantangan besar tanpa kerja sama internasional, terutama dalam hal pertukaran data dan alih yurisdiksi. Akan tetapi untuk menghindari pelanggaran hak asasi manusia, strategi proaktif juga harus diimbangi dengan prinsip kehati-hatian. Teknologi seperti penyadapan dan pelacakan digital hingga pengumpulan data harus digunakan oleh kepolisian secara seimbang dan sah serta dapat dipertanggung jawabkan. Sangat penting untuk menjaga kepercayaan masyarakat terhadap lembaga penegak hukum dan memastikan bahwa upaya untuk mengurangi kejahatan tidak mengakibatkan pelanggaran baru.

Urgensi penguatan peran kepolisian dalam penegakan hukum di ruang digital dapat dilihat dari tingginya ancaman dan laporan kejahatan siber di Indonesia. Berdasarkan data Badan Siber dan Sandi Negara (BSSN), tercatat sebanyak 3,64 miliar anomali serangan siber pada periode Januari hingga Juli 2025 (Verihubs, 2026). Sementara itu, data Patroli Siber mencatat 8.614 laporan terkait ancaman kekerasan, 6.556 laporan pencemaran nama baik, 952 laporan pornografi, serta berbagai bentuk pelanggaran lainnya (Siber, n.d.). Tingginya angka tersebut menunjukkan bahwa ruang digital tidak hanya menjadi sarana aktivitas masyarakat, tetapi juga menjadi ruang terjadinya berbagai bentuk pelanggaran dan tindak pidana yang memerlukan respons penegakan hukum yang adaptif.

Pencegahan dan penindakan merupakan dua fungsi penting dalam penegakan hukum di era digital. Pendekatan pencegahan dapat diterapkan dengan memberikan pendidikan literasi digital kepada masyarakat dan meningkatkan kesadaran akan keamanan data serta memperkuat sistem keamanan siber nasional. Pendekatan represif juga tetap diperlukan untuk memberikan efek jera kepada pelaku melalui penindakan hukum yang tegas dan adil. Keseimbangan antara kedua pendekatan ini menjadi kunci dalam menciptakan ruang digital yang aman dan kondusif (Rifai, 2011). Peran kepolisian dalam penegakan hukum di era digital mencakup dua hal yang saling berkaitan yaitu Tindakan preventif dan represif. Tindakan preventif bertujuan untuk mengurangi kemungkinan terjadinya kejahatan sebelum kejahatan tersebut terjadi, sedangkan tindakan represif dilakukan melalui penegakan hukum dan penerapan sanksi setelah kejahatan terjadi.

Kewenangan polisi secara normatif dalam penegakan hukum di ruang digital bersumber dari Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia. Pasal 13 menekankan tanggung jawab pokok Polri yang meliputi menjaga ketertiban umum dan memastikan keamanan masyarakat, menegakkan hukum serta memberikan dukungan, bimbingan, dan layanan kepada masyarakat. Ketentuan tersebut



menjadi dasar bagi Polri dalam menjalankan fungsi penegakan hukum, termasuk terhadap tindak pidana yang dilakukan melalui ruang digital. Selain itu, UU ITE memberikan landasan hukum yang lebih khusus dalam penanganan tindak pidana di bidang teknologi informasi dan transaksi elektronik.

Dalam menghadapi tantangan digitalisasi, Polri juga telah melakukan penguatan kapasitas kelembagaan Pembentukan Dittipidsiber Bareskrim Polri merupakan langkah konkret dalam memperkuat kapasitas institusional untuk menangani tindak pidana siber secara profesional. Dittipidsiber bertugas melakukan penyelidikan dan penyidikan terhadap berbagai jenis kejahatan digital mulai dari penipuan daring, penyebaran konten ilegal, peretasan sistem informasi, hingga tindak pidana yang berkaitan dengan data pribadi (Wibowo et al., 2023).

Adanya respon yang cepat dan tepat serta berbasis pada pendekatan yang adaptif terhadap perkembangan teknologi sangat diperlukan dalam proses penegakan hukum yang berlaku. Aparat penegak hukum terkhusus kepolisian dituntut untuk mampu memahami pola-pola kejahatan siber yang terus berkembang termasuk teknik manipulasi psikologis dalam *social engineering* dan metode infiltrasi sistem dalam peretasan serta mekanisme distribusi konten ilegal di berbagai platform digital. Dalam mengungkap kasus-kasus kejahatan siber, kemampuan untuk melakukan *digital forensic* dan analisis data serta pelacakan jejak digital menjadi suatu hal yang sangat penting.

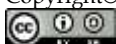
Bertambahnya jumlah kejahatan siber serta penyebaran informasi keliru dan negatif menuntut aparat penegak hukum tidak hanya melakukan penindakan, tetapi juga mampu memprediksi dan mencegah potensi gangguan di ruang digital. Penerapan pemolisian dalam praktiknya tidak hanya menggunakan satu model melainkan mengombinasikan pendekatan modern dan konvensional secara bersamaan agar tercipta strategi pencegahan yang lebih efektif terhadap kejahatan siber (Ismail, 2023).

Peran Preventif Pencegahan Berbasis Sistem Digital

Pendekatan preventif dalam teori penegakan hukum modern dipandang sebagai strategi yang paling efisien karena dinilai mampu mencegah kerugian sebelum terjadi dan bukan sekadar memberikan respons setelah kerusakan muncul. Fungsi preventif polisi di era digital memerlukan reorientasi yang mendasar karena karakteristik ruang maya sangat berbeda dengan ruang fisik konvensional yang selama ini menjadi arena utama penegakan hukum (Huliselan, 2023).

Aspek pertama dari peran preventif polisi di ruang digital adalah pelaksanaan patroli siber secara terstruktur dan berkelanjutan. Patroli siber bukan sekadar pemantauan konten media sosial melainkan sebuah proses aktivitas digital yang mencakup identifikasi potensi kejahatan, pemantauan pola pergerakan data yang mencurigakan, deteksi dini terhadap narasi-narasi yang berpotensi memecah belah masyarakat, serta pelacakan aktivitas kelompok-kelompok yang diidentifikasi memiliki niat untuk melakukan kejahatan siber (Suseno, 2022). Patroli siber yang efektif memerlukan personel yang tidak hanya memahami prosedur hukum, tetapi juga fasih dalam membaca ekosistem digital dengan segala kerumitannya.

Aspek kedua adalah penguatan literasi hukum digital di tengah masyarakat. Realitas di lapangan menunjukkan bahwa sebagian besar pelanggaran di ruang digital terjadi bukan karena niat jahat yang disengaja melainkan karena ketidaktahuan pelaku tentang batasan-batasan hukum yang berlaku dalam beraktivitas di internet (Wahid & Labib, 2022). Program sosialisasi hukum yang selama ini didominasi oleh pendekatan tatap muka perlu beradaptasi dengan menggunakan kanal-kanal digital yang justru menjadi habitat keseharian



masyarakat termasuk media sosial melalui *podcast* hukum dan konten edukasi berbasis video yang mudah dicerna oleh berbagai lapisan masyarakat.

Penanganan kejahatan siber juga memerlukan kerja sama dari berbagai macam pihak seperti pemerintah dan perusahaan swasta hingga masyarakat umum. Masyarakat harus dibekali literasi digital yang baik agar dapat terhindar dari kejahatan siber dan juga penyedia layanan digital memegang peranan penting dalam menjaga keamanan sistem serta melindungi data para pengguna. Pemerintah harus memperkuat regulasi serta meningkatkan kemampuan lembaga penegak hukum dalam menangani masalah-masalah yang ditimbulkan oleh kejahatan digital yang semakin kompleks dan melintasi batas-batas negara.

Aspek ketiga adalah pembangunan kemitraan strategis antara kepolisian dengan sektor swasta khususnya perusahaan teknologi dan platform digital. Polisi tidak memiliki kemampuan teknis dan sumber daya yang cukup untuk menjangkau seluruh sudut ruang digital sendirian. Kerja sama dengan penyedia platform dalam hal pelaporan konten ilegal dan pembekuan akun yang teridentifikasi sebagai pelaku kejahatan hingga berbagi data intelijen yang diperlukan untuk proses penyidikan menjadi komponen penting dalam ekosistem pencegahan kejahatan digital yang menyeluruh.

Peran Represif dalam Penyidikan dan Pembuktian Elektronik

Fungsi represif kepolisian dalam konteks penegakan hukum digital mencakup rangkaian tindakan mulai dari penyelidikan awal, penyidikan mendalam, pengumpulan dan pengamanan alat bukti elektronik, hingga penyelesaian berkas perkara yang siap diajukan ke penuntut umum. Setiap tahapan ini mengandung kompleksitas teknis dan yuridis yang memerlukan penanganan khusus dan tidak dapat disamakan dengan prosedur standar pada perkara pidana konvensional (Rasiwan, 2025). Secara normatif, pelaksanaan penyidikan tindak pidana di bidang teknologi informasi dan transaksi elektronik didasarkan pada Pasal 43 UU ITE. Ketentuan tersebut menegaskan kewenangan Penyidik Polri dalam penyidikan tindak pidana di bidang teknologi informasi dan transaksi elektronik serta mengatur bahwa proses penyidikan harus memperhatikan perlindungan privasi, kerahasiaan, kelancaran layanan publik, dan integritas data (Undang-Undang Nomor 1 Tahun 2024, 2024).

Inti dari penyidikan tindak pidana digital adalah kemampuan mengidentifikasi, mengumpulkan, menganalisis, dan memperlihatkan alat bukti elektronik secara sah di persidangan. Hal ini tercantum dalam Pasal 5 ayat (1) dan ayat (2) UU ITE yang mengakui Informasi Elektronik dan/atau Dokumen Elektronik beserta hasil cetaknya sebagai alat bukti hukum yang sah dan sebagai perluasan dari alat bukti yang sah berdasarkan hukum acara yang berlaku di Indonesia. Dalam penerapannya, ketentuan tersebut memungkinkan penyidik menggunakan data digital yang relevan, seperti dokumen elektronik, rekaman elektronik, atau data dalam sistem elektronik, sebagai bagian dari proses pembuktian sepanjang memenuhi ketentuan hukum yang berlaku. Oleh karena itu, penerapan forensik digital menjadi penting untuk menjaga keaslian, integritas, dan keterlacakan alat bukti elektronik sejak diperoleh hingga digunakan dalam proses peradilan (Hiariej, 2020).

Selain pengumpulan alat bukti, penyidikan tindak pidana siber dapat melibatkan tindakan penggeledahan dan penyitaan terhadap sistem elektronik. Pasal 43 ayat (3) UU ITE mengatur bahwa penggeledahan dan/atau penyitaan terhadap Sistem Elektronik yang berkaitan dengan dugaan tindak pidana dilakukan sesuai dengan ketentuan hukum acara pidana. Ketentuan ini menunjukkan bahwa karakteristik digital tidak menghilangkan kewajiban penyidik untuk mengikuti prosedur hukum acara dalam melakukan upaya paksa. Dalam praktiknya, penyidik perlu memastikan bahwa tindakan terhadap perangkat atau sistem elektronik dilakukan berdasarkan kewenangan yang sah serta tetap menjaga



integritas data yang diperoleh.

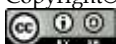
Tantangan terbesar dalam penyidikan tindak pidana siber adalah dimensi lintas yurisdiksi. Kejahatan yang dilakukan oleh seseorang yang berada di luar wilayah Indonesia terhadap korban yang berada di dalam negeri atau sebaliknya menciptakan persoalan hukum internasional yang tidak dapat diselesaikan hanya dengan pengumpulan data hukum nasional (Sitompul, 2022). Persoalan tersebut juga telah diantisipasi dalam Pasal 43 ayat (8) UU ITE yang memungkinkan penyidik bekerja sama dengan penyidik negara lain untuk berbagi informasi dan alat bukti sesuai dengan ketentuan peraturan perundang-undangan. Dalam penerapannya, ketentuan tersebut menjadi dasar bagi penyidik untuk melakukan kerja sama lintas negara ketika informasi atau alat bukti yang dibutuhkan berada di yurisdiksi negara lain. Mekanisme kerja sama internasional melalui jalur *Mutual Legal Assistance in Criminal Matters* (MLAT) dan jaringan *International Criminal Police Organization* (INTERPOL) menjadi jalan yang tersedia meskipun dalam praktiknya seringkali memakan waktu yang panjang dan tidak selalu menghasilkan kerja sama yang memuaskan dari negara-negara yang dimintai bantuan.

Sejumlah besar informasi dihasilkan oleh banyaknya pengguna internet dalam keseharian. Informasi pribadi yang tersebar di berbagai *platform* digital telah berubah menjadi aset yang sangat diminati sekaligus sasaran utama para penjahat siber. Kebocoran data tidak hanya disebabkan oleh serangan eksternal akan tetapi juga oleh sistem keamanan yang lemah dan kurangnya kesadaran pengguna akan pentingnya melindungi data pribadi mereka. Hal tersebut tentu semakin menekankan bahwa keamanan siber merupakan tanggung jawab bersama. Agar kejahatan siber dapat diminimalisir, penegak hukum dan organisasi terkait lainnya harus memperkuat kemampuan forensik digital mereka dan mendorong kerja sama lintas sektor dan lintas batas serta merancang teknik berbasis teknologi. Jika langkah-langkah pengamanan ini tidak diterapkan, kesenjangan antara kapasitas penegak hukum dan pertumbuhan kejahatan siber akan terus melebar (Badan Siber dan Sandi Negara, 2023).

Selama proses penyidikan digital berlangsung aspek yang tidak boleh diabaikan dalam fungsi represif kepolisian adalah perlindungan hak-hak tersangka. Kemudahan akses terhadap informasi digital tidak boleh dijadikan pembenaran untuk mengabaikan prinsip-prinsip hukum acara pidana yang menjamin hak atas privasi dan asas praduga tidak bersalah serta larangan penggeledahan dan penyitaan yang sewenang-wenang (Bahri, 2024). Hal tersebut sejalan dengan Pasal 43 ayat (2) UU ITE yang mewajibkan penyidikan tindak pidana di bidang teknologi informasi dan transaksi elektronik memperhatikan perlindungan privasi, kerahasiaan, kelancaran layanan publik, serta integritas atau keutuhan data. Dengan demikian, kewenangan represif Polri dalam penyidikan tindak pidana siber tidak bersifat tanpa batas, melainkan harus dilaksanakan berdasarkan hukum dan dengan memperhatikan perlindungan terhadap hak individu serta keamanan data.

Kesimpulan

Berdasarkan hasil penelitian, peran kepolisian dalam penegakan hukum di era digitalisasi dilaksanakan melalui fungsi preventif dan represif yang didukung oleh landasan kewenangan dalam peraturan perundang-undangan. Secara preventif, kepolisian berperan dalam melakukan patroli siber, meningkatkan literasi hukum digital masyarakat, serta membangun kerja sama dengan sektor swasta dan penyedia platform digital untuk mencegah terjadinya tindak pidana di ruang digital. Sementara itu, fungsi represif dilaksanakan melalui penyelidikan dan penyidikan tindak pidana siber, pengumpulan serta pengamanan alat bukti elektronik, penerapan forensik digital, penggeledahan dan penyitaan terhadap sistem elektronik sesuai hukum acara, serta kerja sama lintas yurisdiksi dalam memperoleh

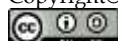


informasi dan alat bukti.

Oleh karena itu, diperlukan penguatan kapasitas kepolisian dalam menghadapi perkembangan kejahatan siber, khususnya melalui peningkatan kompetensi sumber daya manusia di bidang teknologi informasi dan forensik digital, penguatan sarana dan prasarana penyidikan, serta peningkatan koordinasi antarlembaga dan kerja sama lintas yurisdiksi. Selain itu, pembaruan regulasi yang adaptif terhadap perkembangan teknologi dan penguatan literasi hukum digital masyarakat perlu dilakukan secara berkelanjutan untuk mendukung terciptanya penegakan hukum di ruang digital yang efektif, proporsional, dan tetap memperhatikan perlindungan hak asasi manusia.

Daftar Pustaka

- Bahri, Assadul. *Dinamika Hukum Acara Pidana: Pembaruan, Tantangan, Dan Praktik Di Era Digital*. Mahalisan Legal Development, 2024.
- Badan Siber dan Sandi Negara (BSSN). (2024). Laporan Tahunan Keamanan Siber Indonesia 2023. Diakses 15 Maret 2025 dari <https://www.bssn.go.id/laporan-tahunan-keamanan-siber-2023/>
- Hamzah, Andi. *Delik-Delik Tertentu (Speciale Delicten) Di Dalam KUHP*. Jakarta: Sinar Grafika, 2015.
- Hiariej, Eddy O.S. *Teori Dan Hukum Pembuktian*. Erlangga. Jakarta, 2020.
- Huliselan, Pramawi Nicolas. "Peran Intelijen Kepolisian Sebagai Tindakan Preventif Dalam Menanggulangi Tindak Pidana Cyber Crime." *Paulus Law Journal* 5, no. 1 (2023): 64–87.
- Ismail, Marzuki. "Digital Policing; Studi Pemanfaatan Teknologi Dalam Pelaksanaan Tugas Intelijen Kepolisian Untuk Mencegah Kejahatan Siber (Cybercrime)." *Jurnal Ilmu Kepolisian* 17, no. 3 (2023): 15–15.
- Kementerian Komunikasi dan Informatika RI. (2024). Statistik Pengguna Internet Indonesia 2024. Diakses 18 Maret 2025 dari <https://kominfo.go.id/content/detail/statistik-internet-2024>
- Kempa, Analtasia, Muhamad Amin Hamid, &, and Maria Yeti Andrias. "Pemerasan Digital Melalui Media Sosial : Analisis Yuridis Terhadap Penegakan Hukum Di Indonesia." *Journal of Law Review* 4, no. 2 (2025): 128–39.
- Labib, Abdul Wahid & Mohammad. "Kejahatan Mayantara (Cyber Crime)." In 2022, hlm. 144. Bandung: Refika Aditama, n.d.
- Muladi, and Barda Nawawi Arief. *Teori Dan Kebijakan Pidana*. Jakarta: Prenada Media Group, 2022.
- Rasiwan, Iwan. "Penegakan Hukum Pidana Di Indonesia Penegakan Hukum Pidana Di Indonesia," 1–267. AMU Press, 2025.
- RI, Kementerian Komunikasi dan Informatika. "Indeks Masyarakat Digital Indonesia (IMDI) 2023." Jakarta, 2023.
- Rifai, Ahmad. *Penemuan Hukum Oleh Hakim: Dalam Perspektif Hukum Progresif*. Jakarta: Sinar Grafika, 2011.
- Republik Indonesia. (2024). Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik (UU ITE).
- Republik Indonesia. (2023). Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan.
- Republik Indonesia. (2002). Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia.
- Republik Indonesia. (2024). Peraturan Pemerintah Nomor 28 Tahun 2024 tentang Pelaksanaan



Undang-Undang Kesehatan.

- Siber, P. (n.d.). *Jumlah laporan polisi yang dibuat masyarakat. Patroli Siber*.
<https://patrolisiber.id/statistic>
- Sitompul, Josua. *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*. Jakarta: Tatanusa, 2022.
- Suhariyanto, Budi. *Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan Dan Celah Hukumnya*. Jakarta: RajaGrafindo Persada, 2023.
- Suprihanto, Eko. *Pembaruan Model Penegakan Hukum Tindak Pidana Lalu Lintas Berbasis Elektronik Untuk Mewujudkan Keadilan Restoratif*. Jakarta: PT RajaGrafindo Persada, 2025.
- Suseno, Sigid. *Yurisdiksi Tindak Pidana Siber*. Bandung: Refika Aditama, 2022.
- Tahir, R., I. G. P. Astawa, A. Widjajanto, M. L. Panggabean, M. M. Rohman, N. P. P. Dewi, and S. R. Paminto. *Metodologi Penelitian Bidang Hukum: Suatu Pendekatan Teori Dan Praktik*. PT Sonpedia Publishing Indonesia, 2023.
- Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia, Pasal 13.
- Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).
- Verihubs. (2026, Maret 22). *Statistik Cybercrime Indonesia 2025-2026: Data dan Tren Terbaru*. Verihubs. <https://verihubs.com/blog/statistik-cybercrime-indonesia>
- Wibowo, A., Wangsajaya, Y., Surahmat, and A. *Pemolisian Digital Dengan Artificial Intelligence*. Jakarta: PT RajaGrafindo Persada (Rajawali Pers), 2023.

