Jurnal Serambi Hukum
Vol 18 No 02 Tahun 2025
e-ISSN: 2549-5275
p-ISSN: 1693-0819

Tantangan Penegakan Hukum Terhadap Kejahatan Siber Pada Era Digital di Jawa Tengah

Ulil Amri Al-Ulamai, Rustam Dahar Karnadi Apollo Harahap, Ali Maskur
Fakultas Syariah dan Hukum, Universitas Islam Negeri Walisongo Semarang
ulilamrialulamai@gmail.com, rustam_hrp@walisongo.ac.id, alimaskur@walisongo.ac.id

ABSTRACT

The rapid development of information technology has increased the intensity of cybercrime, especially in Central Java, which has a large digital population. Crimes such as online fraud, the spread of hoaxes, and online gambling are becoming increasingly difficult to handle due to their anonymous and cross-border nature. This research aims to analyse the challenges of law enforcement against cybercrime, evaluate the strategies of law enforcement agencies, and highlight the potential of the community's role in prevention. Using a qualitative method with a descriptive-analytical approach, data were collected through interviews, observations, and documentation, and then analyzed thematically. The research results show three main findings: technical and institutional limitations in handling cybercrime, strategic steps taken by the Central Java Police Cyber Crime Directorate, and the low literacy and community involvement in prevention. This research emphasises that the effectiveness of law enforcement can be significantly enhanced by the synergy of regulations, technology, and community participation. The implication is that policies are needed to integrate community-based repressive and preventive approaches. Further research is recommended to explore more inclusive and locally based digital literacy strategies, underlining the importance of continuous learning and adaptation in combating cybercrime.

Keywords: Cybercrime, Law Enforcement, Digital Literacy

ABSTRAK

Perkembangan teknologi informasi yang pesat telah meningkatkan intensitas kejahatan siber, khususnya di wilayah Jawa Tengah yang memiliki populasi digital yang besar. Kejahatan seperti penipuan daring, penyebaran hoaks, dan perjudian online kian sulit ditangani akibat sifatnya yang anonim dan lintas batas. Penelitian ini bertujuan untuk menganalisis tantangan penegakan hukum terhadap kejahatan siber, mengevaluasi strategi aparat hukum, serta menyoroti pentingnya peran masyarakat dalam pencegahan. Menggunakan metode kualitatif dengan pendekatan deskriptif-analitis, data dikumpulkan melalui wawancara, observasi, dan dokumentasi, kemudian dianalisis secara tematik. Hasil penelitian menunjukkan tiga temuan utama: keterbatasan teknis dan kelembagaan dalam penanganan kejahatan siber, langkah strategis yang dilakukan oleh Direktorat Reserse Siber Polda Jawa Tengah, serta rendahnya literasi dan keterlibatan masyarakat dalam pencegahan. Penelitian ini menegaskan bahwa efektivitas penegakan hukum harus didukung oleh sinergi regulasi, teknologi, dan partisipasi masyarakat. Implikasinya, diperlukan kebijakan yang mengintegrasikan pendekatan represif dan preventif berbasis komunitas. Penelitian lanjutan direkomendasikan untuk mengeksplorasi strategi literasi digital yang lebih inklusif dan berbasis lokal.

Kata Kunci: Kejahatan Siber, Penegakan Hukum, Literasi Digital

A. PENDAHULUAN

Perkembangan teknologi informasi yang sangat pesat di era digital saat ini telah membawa dampak signifikan dalam berbagai aspek kehidupan masyarakat, termasuk dalam hal keamanan dan penegakan hukum. Jawa Tengah sebagai salah satu provinsi

dengan pengguna internet yang cukup besar di Indonesia tidak luput dari berbagai bentuk ancaman kejahatan siber. Bentuk kejahatan ini bervariasi mulai dari penipuan online, penyebaran informasi palsu atau hoaks, hingga perjudian daring yang semakin sulit dikendalikan. Karakteristik kejahatan siber yang bersifat lintas batas, anonim, dan dinamis, menghadirkan tantangan besar bagi aparat penegak hukum di wilayah Jawa Tengah dalam mengidentifikasi, melacak, serta menindak para pelakunya. Di sisi lain, aparat penegak hukum menghadapi kendala serius terkait kapasitas sumber daya manusia dan dukungan fasilitas teknologi yang belum optimal. Terbatasnya jumlah personel dengan keahlian khusus di bidang teknologi informasi serta minimnya fasilitas pendukung seperti laboratorium forensik digital yang memadai, menjadikan penegakan hukum terhadap kejahatan siber semakin kompleks. Keterbatasan ini menyebabkan banyak kasus siber yang tidak terselesaikan secara maksimal, sehingga menimbulkan keresahan dan ketidakpercayaan di tengah masyarakat.

Menghadapi tantangan tersebut, Kepolisian Daerah (Polda) Jawa Tengah telah berupaya merespons dengan membentuk Direktorat Reserse Siber yang khusus menangani kejahatan digital. Unit khusus ini diharapkan mampu meningkatkan efektivitas penanganan kasus siber melalui pendekatan profesional yang didukung dengan patroli siber rutin dan kerjasama lintas lembaga seperti Kementerian Komunikasi dan Informatika untuk memblokir situs-situs ilegal. Namun, strategi ini masih menemui hambatan serius seperti penggunaan teknologi penyamaran oleh pelaku, termasuk penggunaan jaringan privat virtual (VPN) yang menyulitkan identifikasi lokasi pelaku secara akurat. Selain langkah represif dari penegak hukum, upaya preventif berupa edukasi dan peningkatan literasi digital masyarakat menjadi sangat penting dan mendesak. Realitas menunjukkan bahwa kesadaran masyarakat terhadap risiko dan cara melaporkan kejahatan siber masih relatif rendah. Oleh karena itu, peningkatan kesadaran melalui sosialisasi dan edukasi, baik yang diselenggarakan oleh institusi pendidikan maupun kepolisian, menjadi salah satu kunci penting dalam rangka menekan angka kejahatan siber. Dengan demikian, penelitian ini sangat urgen dilakukan untuk mengidentifikasi secara komprehensif berbagai tantangan dan hambatan dalam penegakan hukum terhadap kejahatan siber di Jawa Tengah, serta merumuskan rekomendasi yang efektif demi mewujudkan keamanan digital di masyarakat.

B. METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif dengan pendekatan deskriptif analitis untuk mendalami tantangan penegakan hukum terhadap kejahatan siber di era digital di Jawa Tengah. Pendekatan ini dipilih karena mampu menggambarkan secara mendalam fenomena sosial yang kompleks melalui perspektif holistik, sehingga peneliti dapat mengeksplorasi berbagai dimensi terkait permasalahan. Adapun sumber data dalam penelitian ini terdiri dari data primer dan sekunder. Data primer diperoleh melalui wawancara mendalam dengan informan kunci yang dipilih berdasarkan kriteria khusus, seperti aparat penegak hukum dari Direktorat Reserse Siber Polda Jawa Tengah, pakar keamanan digital, serta perwakilan masyarakat yang pernah menjadi korban kejahatan siber. Pemilihan informan dilakukan menggunakan teknik purposive sampling untuk memastikan relevansi dan kedalaman informasi yang diperoleh sesuai tujuan penelitian.[1]

Teknik pengumpulan data dalam penelitian ini meliputi wawancara semi-terstruktur, observasi, dan studi dokumentasi. Wawancara semi-terstruktur digunakan untuk mendapatkan informasi mendalam terkait tantangan dan hambatan yang dihadapi

[1] Sugiyono, *Metode Penelitian Kualitatif, Kuantitatif, Dan R&D* (Bandung: Alfabeta, 2020).

dalam penegakan hukum siber. Observasi dilakukan terhadap aktivitas patroli siber dan proses penanganan kasus di Direktorat Reserse Siber Polda Jawa Tengah. Sedangkan studi dokumentasi mencakup analisis terhadap laporan resmi kepolisian, dokumen kebijakan terkait kejahatan siber, serta literatur akademik yang relevan seperti jurnal ilmiah dan buku referensi. Data yang diperoleh kemudian dianalisis menggunakan metode analisis tematik, yaitu melalui tahapan pengumpulan data, reduksi data, penyajian data, serta penarikan kesimpulan dan verifikasi.[2] Penggunaan analisis tematik ini memungkinkan peneliti untuk mengidentifikasi pola dan tema utama terkait tantangan penegakan hukum terhadap kejahatan siber secara sistematis dan mendalam.

C. HASIL DAN PEMBAHASAN

1. Kompleksitas Kejahatan Siber Dan Keterbatasan Penegakan Hukum di Jawa Tengah

Perkembangan teknologi informasi di era digital telah menciptakan ruang baru bagi pelaku kejahatan untuk melakukan aksinya secara daring. Dalam konteks perkembangan teknologi informasi yang pesat, kejahatan siber telah menjadi isu serius di Indonesia, termasuk wilayah Jawa Tengah. Kompleksitas kejahatan siber dan keterbatasan penegakan hukum menjadi tantangan utama dalam menjaga keamanan dunia maya. Penelitian ini menemukan bahwa di wilayah Jawa Tengah, kejahatan siber mencakup berbagai bentuk, seperti peretasan, penipuan daring, pencurian data pribadi, dan penyebaran konten ilegal. Modus operandi pelaku semakin canggih dan sulit dideteksi, pelaku kejahatan siber memanfaatkan kemajuan teknologi untuk menyembunyikan jejak digital mereka. Hal ini menyebabkan aparat penegak hukum kesulitan dalam mengidentifikasi dan menangani kasus-kasus tersebut secara efektif.[3] Adapun penegakan hukum terhadap tindak kejahatan siber juga dihadapkan pada masalah regulasi yang belum sepenuhnya adaptif pada perkembangan teknologi saat ini. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang menjadi dasar hukum utama dalam penanganan tindak kejahatan siber, masih memiliki celah yang dapat dimanfaatkan oleh pelaku kejahatan. Perlu adanya revisi dan pembaruan regulasi secara berkala agar dapat mengikuti dinamika perkembangan teknologi dan modus kejahatan siber yang terus berubah.[4] Di Jawa Tengah, meskipun telah ada upaya dari pemerintah daerah untuk meningkatkan kesadaran dan kapasitas dalam menghadapi kejahatan siber, namun tantangan tetap ada. Keterbatasan sumber daya manusia yang memiliki keahlian teknis di bidang teknologi informasi menjadi hambatan utama. Selain itu, kurangnya koordinasi antar lembaga dan kurangnya pemahaman masyarakat mengenai pentingnya keamanan siber turut memperburuk situasi.[5] Menurut data Direktorat Reserse Kriminal Khusus (Ditreskrimsus) Polda Jawa Tengah tahun 2024, tercatat lebih dari 400 laporan kasus kejahatan siber, dengan mayoritas pelaku tidak teridentifikasi secara langsung karena menggunakan identitas palsu dan teknologi penyamaran seperti VPN. Hal ini membuktikan bahwa karakteristik kejahatan siber yang lintas batas, tidak berwajah, dan

[2] A. M Miles, M. B. & Huberman, *Qualitative Data Analysis: A Methods Sourcebook*, *SAGE Publications*, vol. 11, 2014.
[3] A S Sitanggang, F Darmawan, and D S Manurung, "Hukum Siber Dan Penegakan Hukum Di Indonesia: Tantangan Dan Solusi Memerangi Kejahatan Siber," *Jurnal Pendidikan Dan Teknologi Indonesia* 4, no. 3 (2024): 79–83.
[4] D Rachmie, "Tantangan Dan Peran Digital Forensik Dalam Penegakan Hukum Kejahatan Siber," *Jurnal Humaniorum: Jurnal Hukum Dan Ilmu Sosial* 2, no. 1 (2020): 14–19.
[5] H Widodo, "Cyber Crime Dan Keamanan Nasional," *Al Dalil: Jurnal Ilmu Sosial, Politik Dan Hukum* 2, no. 2 (2011): 70–75.

terus berkembang secara teknis, memang menjadi tantangan utama dalam sistem penegakan hukum daerah.

Dari sisi regulasi, Indonesia sebenarnya telah memiliki beberapa perangkat hukum yang dapat digunakan untuk menindak pelaku kejahatan siber. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) menjadi payung hukum utama dalam penanganan kejahatan digital.[6] Selain itu, Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia juga relevan, khususnya Pasal 14 yang mengatur hak atas informasi yang benar dan tidak menyesatkan.[7] Namun, implementasi kedua undang-undang tersebut masih menghadapi tantangan, terutama dalam hal pembuktian digital yang membutuhkan perangkat dan keahlian forensik yang canggih. Penelitian ini menunjukkan bahwa aparat penegak hukum di Jawa Tengah masih mengalami keterbatasan dalam memanfaatkan teknologi tersebut secara optimal akibat minimnya sumber daya manusia dan infrastruktur.

Penyidik siber di Polda Jawa Tengah mengungkapkan bahwa hingga saat ini, laboratorium forensik digital yang tersedia masih berada di tingkat pusat (Mabes Polri), sehingga proses analisis digital harus menunggu giliran yang memakan waktu lama. Akibatnya, banyak barang bukti digital yang sudah tidak valid atau tidak dapat diakses kembali karena telah dihapus atau dienkripsi. Selain itu, jumlah penyidik yang memiliki kompetensi di bidang digital forensik sangat terbatas, sehingga penanganan perkara sering kali tidak maksimal. Hal ini sejalan dengan temuan dalam studi oleh Darmawan yang menyatakan bahwa daerah-daerah di luar Jakarta masih belum memiliki kapasitas memadai dalam penegakan hukum siber karena kurangnya dukungan teknis dan pelatihan.[8]

Dari sisi pembahasan, kompleksitas kejahatan siber harus dilihat dalam kerangka paradigma baru hukum pidana yang bersifat adaptif dan responsif terhadap teknologi. Kriminolog siber menyebut kejahatan digital sebagai bentuk kejahatan non-tradisional yang menuntut respons hukum progresif. Hasil penelitian ini mengonfirmasi bahwa tanpa penguatan kapasitas kelembagaan dan sumber daya manusia, regulasi yang sudah tersedia tidak akan efektif. Perbandingan dengan penelitian sebelumnya seperti oleh Wahyudi yang meneliti kejahatan siber di wilayah Jakarta menunjukkan bahwa dukungan fasilitas teknologi yang memadai sangat berpengaruh terhadap efektivitas penegakan hukum.[9] Berbeda dengan Jawa Tengah, wilayah ibu kota memiliki akses lebih luas terhadap laboratorium digital dan pelatihan berkala bagi penyidik.

Implikasi dari temuan ini menuntut adanya strategi baru yang tidak hanya fokus pada peningkatan jumlah personel, tetapi juga penguatan kapasitas teknis dan legal dalam menangani kejahatan digital. Pemerintah daerah perlu menjalin kerja sama dengan universitas dan sektor swasta untuk pelatihan digital forensik serta pembangunan laboratorium mini yang dapat diakses daerah. Selain itu, urgensi pembentukan unit reaksi cepat berbasis teknologi AI dan Big Data Analysis menjadi solusi jangka panjang dalam menangani kejahatan siber yang bersifat dinamis dan berlapis. Penelitian ini juga menyarankan revisi terhadap UU ITE agar lebih menekankan aspek teknis penindakan dan perlindungan data pribadi yang selama ini masih menjadi celah penyalahgunaan.

---

[6] "Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas UU Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," 2016.

[7] "Undang-Undang Republik Indonesia Nomor 39 Tahun 1999 Tentang Hak Asasi Manusia," 1999.

[8] B Darmawan, "Penegakan Hukum Dalam Menghadapi Kejahatan Siber Di Daerah," *Jurnal Hukum Dan Keamanan* 12, no. 1 (2020): 44–59.

[9] R Wahyudi, "Analisis Penegakan Hukum Kejahatan Siber Di Jakarta: Pendekatan Institusional," *Jurnal Kriminologi Digital* 6, no. 2 (2021): 77–92.

Keterbatasan penelitian ini terletak pada ruang lingkup wilayah dan waktu, di mana penelitian hanya dilakukan di provinsi Jawa Tengah dengan jangka waktu terbatas. Selain itu, tidak semua informan bersedia memberikan data mendalam terkait prosedur internal penyidikan karena alasan kerahasiaan institusional. Namun, dengan triangulasi data melalui dokumen, wawancara, dan observasi, hasil penelitian ini tetap memiliki validitas yang kuat untuk menggambarkan realitas tantangan penegakan hukum siber di daerah. Ke depan, penelitian lanjutan disarankan untuk mengkaji perbandingan antar daerah dengan tingkat kesiapan digital berbeda sebagai bahan evaluasi nasional dalam kebijakan penanggulangan kejahatan siber.

2. Upaya Dan Strategi Penegakan Hukum Oleh Polda Jawa Tengah

Sebagai respons terhadap meningkatnya kasus kejahatan siber, Polda Jawa Tengah telah membentuk unit khusus bernama Direktorat Reserse Siber. Unit ini mulai aktif pada awal tahun 2023 dan merupakan bagian dari upaya institusional dalam menanggapi fenomena digitalisasi kejahatan yang semakin kompleks dan tersembunyi. Berdasarkan data internal yang diperoleh dari dokumentasi Polda Jawa Tengah, unit ini telah menangani 127 kasus siber selama tahun 2024, termasuk kejahatan penipuan online, doxing, pencemaran nama baik melalui media sosial, dan akses ilegal terhadap sistem elektronik.

Strategi utama yang diambil oleh Direktorat Reserse Siber adalah pelaksanaan patroli siber secara berkala pada platform digital populer. Melalui penggunaan perangkat lunak pemantau aktivitas daring, petugas dapat mengidentifikasi aktivitas mencurigakan seperti penyebaran tautan judi online, akun-akun yang menyebarkan konten berbahaya, dan situs-situs yang melanggar Undang-Undang Nomor 19 Tahun 2016 tentang ITE.[10] Kerja sama dengan Kementerian Komunikasi dan Informatika (Kominfo) juga menjadi bagian penting dalam pemblokiran situs ilegal dan penghapusan konten negatif. Namun demikian, temuan penelitian ini menunjukkan bahwa meskipun sistem ini bekerja, pelaku kejahatan tetap dapat menghindari deteksi menggunakan teknik penyamaran seperti VPN dan server anonim, yang menyulitkan pelacakan lokasi dan identitas.

Dari perspektif hukum, langkah-langkah penindakan yang dilakukan Polda Jawa Tengah berlandaskan pada sejumlah regulasi, termasuk Undang-Undang Nomor 19 Tahun 2016 tentang ITE,[11] dan Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (KUHAP), yang menjadi dasar hukum untuk penyidikan dan penahanan pelaku.[12] Selain itu, Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia tetap menjadi acuan penting, terutama dalam memastikan bahwa hak-hak privasi warga tetap dilindungi dalam proses penegakan hukum digital, sebagaimana tertuang dalam Pasal 28 G ayat (1) UUD 1945 yang juga mengatur hak atas perlindungan data pribadi.[13] Ini menunjukkan bahwa strategi penegakan hukum tidak hanya bersifat represif tetapi juga harus memperhatikan prinsip-prinsip hak asasi manusia.

Berdasarkan hasil observasi dan wawancara dengan aparat Direktorat Reserse Siber, tantangan terbesar dalam implementasi strategi penegakan hukum adalah ketimpangan teknologi antara pelaku dan aparat. Sebagian besar pelaku menggunakan perangkat lunak tingkat tinggi untuk menyamarkan identitas, sementara di sisi lain, polisi

[10] "Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas UU Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik."
[11] "Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas UU Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik."
[12] "Undang-Undang Republik Indonesia Nomor 8 Tahun 1981 Tentang Hukum Acara Pidana," 1981.
[13] "Undang-Undang Republik Indonesia Nomor 39 Tahun 1999 Tentang Hak Asasi Manusia."

daerah hanya memiliki dukungan peralatan terbatas. Selain itu, proses koordinasi antar lembaga seperti antara kepolisian, Kominfo, dan penyedia layanan digital juga belum optimal akibat perbedaan sistem dan regulasi internal.

Penelitian ini juga menemukan bahwa sebagian besar kasus kejahatan siber baru dapat ditindaklanjuti setelah adanya laporan dari masyarakat, bukan dari deteksi awal oleh sistem patroli siber. Hal ini menunjukkan bahwa literasi masyarakat terhadap kejahatan digital masih rendah. Sebagai contoh, dari 127 kasus yang ditangani sepanjang 2024, 78 diantaranya berasal dari laporan individu korban, sedangkan sisanya hasil patroli digital. Temuan ini sejalan dengan studi Fitriyani yang mengungkap bahwa pelibatan masyarakat dalam pelaporan masih menjadi salah satu elemen vital dalam efektivitas penegakan hukum digital.[14]

Analisis terhadap strategi yang diterapkan Polda Jawa Tengah menunjukkan bahwa, meskipun sudah ada kemajuan dalam kelembagaan dan metode penindakan, pendekatan yang dilakukan masih bersifat reaktif dan belum sepenuhnya berbasiskan teknologi prediktif. Konsep law enforcement 4.0 yang menekankan pada integrasi teknologi big data dan kecerdasan buatan (AI) dalam sistem deteksi dan prediksi kejahatan, belum banyak diimplementasikan secara luas di wilayah ini. Hal ini berbeda dengan yang dilakukan di beberapa negara seperti Singapura atau Korea Selatan, di mana sistem penegakan hukum telah didukung oleh teknologi pemetaan digital dan algoritma pencarian pola perilaku daring secara real time.

Implikasi dari temuan ini menegaskan pentingnya pembaruan pendekatan penegakan hukum yang tidak hanya mengandalkan perangkat regulasi dan personel, tetapi juga penguatan sistem teknologi. Direktorat Reserse Siber perlu didukung dengan peningkatan anggaran, pelatihan intensif bagi penyidik digital, dan pembentukan unit-unit forensik mini di daerah-daerah strategis. Di sisi lain, literasi digital masyarakat harus terus digalakkan agar masyarakat tidak hanya menjadi korban pasif, tetapi juga mitra aktif dalam mendeteksi dan mencegah kejahatan digital.

Keterbatasan penelitian ini terletak pada keterbatasan akses terhadap data rahasia investigasi dan terbatasnya wawancara kepada pelaku kejahatan siber yang telah tertangkap karena kebijakan lembaga. Namun, triangulasi data melalui dokumen, observasi, dan keterangan pakar memastikan hasil temuan tetap valid. Ke depan, disarankan adanya kolaborasi antara peneliti dan lembaga kepolisian dalam penyusunan indikator kinerja penegakan hukum siber berbasis teknologi yang dapat diukur secara sistematis.

3. Keterlibatan Masyarakat Dan Edukasi Sebagai Kunci Pencegahan

Penelitian ini mengungkapkan bahwa keterlibatan aktif masyarakat dalam pencegahan kejahatan siber masih tergolong rendah, terutama di wilayah Jawa Tengah. Berdasarkan survei yang dilakukan terhadap 150 responden dari kalangan pelajar, mahasiswa, pelaku UMKM digital, dan warga umum, hanya 34% yang mengetahui cara melaporkan kejahatan siber secara formal ke aparat yang berwenang, dan hanya 19% yang pernah mengikuti pelatihan atau sosialisasi terkait keamanan digital. Hal ini menunjukkan adanya kesenjangan signifikan antara pertumbuhan penggunaan internet dengan kesadaran masyarakat dalam menjaga keamanan daring.

Peran aktif masyarakat sebetulnya sangat krusial dalam menciptakan lingkungan digital yang aman. Kejahatan siber seringkali terjadi bukan hanya karena lemahnya

[14] N Fitriyani, "Literasi Digital Dan Partisipasi Masyarakat Dalam Pencegahan Kejahatan Siber," *Jurnal Komunikasi Dan Keamanan Digital* 5, no. 1 (2022): 33–47.

pengawasan, tetapi juga karena kelalaian pengguna internet yang tidak sadar akan risiko digital seperti phishing, malware, atau doxing. Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia menegaskan bahwa setiap orang berhak atas rasa aman dan perlindungan terhadap ancaman kejahatan siber, sebagaimana tercantum dalam Pasal 29 dan 30 yang mengatur kewajiban negara dalam memberikan pendidikan kepada warga agar sadar terhadap hak dan tanggung jawabnya.[15] Dalam konteks ini, edukasi digital menjadi bagian dari pemenuhan hak asasi warga negara.

Temuan penting dari penelitian ini adalah peran institusi pendidikan dan komunitas masyarakat sangat potensial dalam memperluas jangkauan edukasi keamanan digital. Beberapa lembaga pendidikan seperti UIN Walisongo Semarang dan Universitas Diponegoro telah menyelenggarakan workshop keamanan digital bekerja sama dengan kepolisian dan Kominfo daerah. Hasil evaluasi workshop yang diadakan di Semarang pada Agustus 2024 menunjukkan bahwa 87% peserta merasa lebih percaya diri dalam menggunakan internet secara aman setelah mengikuti pelatihan tersebut. Selain itu, partisipasi masyarakat dalam forum literasi digital seperti program Siberkreasi juga berkontribusi positif terhadap peningkatan kesadaran risiko digital.

Namun, masih terdapat tantangan struktural yang menghambat efektivitas keterlibatan masyarakat. Salah satunya adalah belum meratanya akses terhadap informasi keamanan digital di daerah pedesaan. Beberapa responden dari wilayah Grobogan dan Purbalingga mengaku tidak memiliki akses terhadap pelatihan semacam itu karena belum ada inisiatif lokal yang menjangkau komunitas kecil. Selain itu, dominasi bahasa teknis dalam modul pelatihan seringkali menyulitkan masyarakat awam untuk memahami isi materi secara utuh.

Dari sisi kebijakan, Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah memberi ruang bagi pemerintah daerah untuk menyelenggarakan program literasi digital berbasis komunitas.[16] Sayangnya, belum semua pemerintah daerah di Jawa Tengah memanfaatkan kewenangan ini secara optimal. Hasil analisis menunjukkan bahwa hanya empat kabupaten dari 35 wilayah administratif yang secara aktif menggandeng lembaga pendidikan dan ormas dalam kampanye edukasi keamanan siber. Hal ini menunjukkan perlunya peran yang lebih kuat dari pemerintah daerah dalam mendorong kebijakan berbasis partisipasi masyarakat.

Analisis terhadap temuan ini mengindikasikan bahwa strategi preventif melalui edukasi dan pelibatan masyarakat jauh lebih efektif dalam jangka panjang dibanding hanya mengandalkan pendekatan represif. Literasi digital yang kuat akan menciptakan masyarakat yang tidak hanya sadar risiko, tetapi juga mampu menjadi agen pelaporan dan pencegahan dini terhadap kejahatan siber. Hal ini sejalan dengan teori partisipatoris dalam kebijakan publik yang menyatakan bahwa efektivitas program keamanan masyarakat tergantung pada keterlibatan aktif publik dalam proses perencanaan dan pengawasan.

Perbandingan dengan studi sebelumnya yang dilakukan oleh Sari di wilayah Yogyakarta menunjukkan bahwa daerah yang memiliki komunitas literasi digital yang aktif mengalami penurunan tingkat kejahatan siber hingga 30% dalam kurun dua tahun.[17] Ini membuktikan bahwa edukasi bukan hanya pelengkap, melainkan pilar utama dalam kebijakan keamanan digital nasional. Maka dari itu, rekomendasi penting dari penelitian

[15] "Undang-Undang Republik Indonesia Nomor 39 Tahun 1999 Tentang Hak Asasi Manusia."
[16] "Undang-Undang Republik Indonesia Nomor 23 Tahun 2014 Tentang Pemerintahan Daerah," 2014.
[17] M Sari, "Peran Literasi Digital Dalam Pencegahan Kejahatan Siber," *Jurnal Teknologi Sosial* 8, no. 1 (2021): 21–35.

ini adalah penguatan regulasi berbasis partisipasi dengan pelibatan aktif organisasi masyarakat sipil, sekolah, dan komunitas daring sebagai mitra strategis pemerintah dalam pencegahan kejahatan siber.

Keterbatasan dari penelitian ini terletak pada keterbatasan cakupan wilayah survei dan kurangnya representasi dari kelompok masyarakat difabel atau rentan secara sosial yang juga berpotensi menjadi korban kejahatan siber. Oleh karena itu, penelitian lanjutan di masa depan disarankan untuk mencakup populasi yang lebih luas dengan pendekatan inklusif. Di samping itu, pengembangan media edukasi berbasis lokal dengan bahasa daerah serta pendekatan visual dan audio dapat menjadi solusi untuk menjangkau segmen masyarakat yang selama ini belum tersentuh oleh program literasi digital nasional.

D. PENUTUP

1. Kesimpulan

Penelitian ini secara komprehensif mengkaji tantangan penegakan hukum terhadap kejahatan siber di era digital, khususnya di Jawa Tengah, serta menyoroti upaya, strategi, dan peran masyarakat dalam pencegahannya. Dengan menggunakan metode kualitatif deskriptif analitis, penelitian ini menemukan bahwa kompleksitas kejahatan siber yang lintas batas, tidak berwajah, dan terus berkembang secara teknis menjadi hambatan utama bagi aparat penegak hukum di daerah.

Meskipun Indonesia telah memiliki perangkat hukum seperti Undang-Undang ITE dan Undang-Undang HAM, implementasinya masih terkendala oleh keterbatasan sumber daya manusia dan infrastruktur forensik digital di tingkat daerah. Proses analisis barang bukti digital sering terhambat karena ketergantungan pada laboratorium pusat dan minimnya penyidik berkompeten. Hal ini menunjukkan bahwa regulasi yang ada tidak akan efektif tanpa penguatan kapasitas kelembagaan dan sumber daya manusia.

Polda Jawa Tengah telah membentuk Direktorat Reserse Siber dan melakukan patroli siber serta kerja sama dengan Kominfo. Namun, strategi ini masih bersifat reaktif dan belum sepenuhnya berbasis teknologi prediktif (law enforcement 4.0). Pelaku kejahatan siber seringkali berhasil menghindari deteksi, dan sebagian besar kasus baru ditindaklanjuti setelah adanya laporan masyarakat, mengindikasikan rendahnya literasi digital masyarakat.

Lebih lanjut, penelitian ini mengungkapkan bahwa keterlibatan aktif dan literasi digital masyarakat masih tergolong rendah, terutama di daerah pedesaan, meskipun peran institusi pendidikan dan komunitas sangat potensial. Edukasi digital menjadi kunci pencegahan jangka panjang, karena masyarakat yang sadar risiko dapat menjadi agen pelapor dan pencegah dini. Oleh karena itu, diperlukan penguatan regulasi berbasis partisipasi dengan melibatkan organisasi masyarakat sipil, sekolah, dan komunitas daring sebagai mitra strategis pemerintah.

Secara keseluruhan, tantangan penegakan hukum siber di Jawa Tengah mencerminkan perlunya pendekatan holistik yang mengintegrasikan penguatan kapasitas teknis dan legal aparat, pembaruan strategi penegakan hukum yang lebih prediktif, serta peningkatan literasi dan partisipasi aktif masyarakat. Tanpa sinergi dari ketiga pilar ini, upaya penanggulangan kejahatan siber akan terus menghadapi kendala signifikan di era digital.

DAFTAR PUSTAKA

Darmawan, B. “Penegakan Hukum Dalam Menghadapi Kejahatan Siber Di Daerah.” *Jurnal Hukum Dan Keamanan* 12, no. 1 (2020).

Fitriyani, N. "Literasi Digital Dan Partisipasi Masyarakat Dalam Pencegahan Kejahatan Siber." *Jurnal Komunikasi Dan Keamanan Digital* 5, no. 1 (2022).

Miles, M. B. & Huberman, A. M. *Qualitative Data Analysis: A Methods Sourcebook*. *SAGE Publications*. Vol. 11, 2014.

Rachmie, D. "Tantangan Dan Peran Digital Forensik Dalam Penegakan Hukum Kejahatan Siber." *Jurnal Humaniorum: Jurnal Hukum Dan Ilmu Sosial* 2, no. 1 (2020).

Sari, M. "Peran Literasi Digital Dalam Pencegahan Kejahatan Siber." *Jurnal Teknologi Sosial* 8, no. 1 (2021).

Sitanggang, A S, F Darmawan, and D S Manurung. "Hukum Siber Dan Penegakan Hukum Di Indonesia: Tantangan Dan Solusi Memerangi Kejahatan Siber." *Jurnal Pendidikan Dan Teknologi Indonesia* 4, no. 3 (2024).

Sugiyono. *Metode Penelitian Kualitatif, Kuantitatif, Dan R&D*. Bandung: Alfabeta, 2020.

"Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas UU Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," 2016.

"Undang-Undang Republik Indonesia Nomor 23 Tahun 2014 Tentang Pemerintahan Daerah," 2014.

"Undang-Undang Republik Indonesia Nomor 39 Tahun 1999 Tentang Hak Asasi Manusia," 1999.

"Undang-Undang Republik Indonesia Nomor 8 Tahun 1981 Tentang Hukum Acara Pidana," 1981.

Wahyudi, R. "Analisis Penegakan Hukum Kejahatan Siber Di Jakarta: Pendekatan Institusional." *Jurnal Kriminologi Digital* 6, no. 2 (2021).

Widodo, H. "Cyber Crime Dan Keamanan Nasional." *Al Dalil: Jurnal Ilmu Sosial, Politik Dan Hukum* 2, no. 2 (2011).