Jurnal Fakta Hukum
e-ISSN: 2961-9734 | p-ISSN: 2962-2778
Volume 4, Nomor 2, Maret 2026
Available online at: https://ojsstihpertiba.ac.id/index.php/jfh

Tantangan Institusional dalam Penegakan Hukum: Studi Peran Kepolisian dalam Menangani Kejahatan Siber

Andini Gusdania [1*], Arri Vedercia [2]
[1] Fakultas Hukum Universitas Pertiba, Pangkalpinang, Indonesia
[2] Fakultas Hukum Universitas Pertiba, Pangkalpinang, Indonesia

[*]Corresponding Author: gusdaniaandini@gmail.com

Artikel Histori
Diterima: 10-01-2026
Direvisi: 15-02-2026
Diterbitkan: 06-03-2026

Abstrak: Penelitian ini membahas tantangan institusional dalam penegakan hukum oleh kepolisian dalam menangani kejahatan siber di Indonesia. Perkembangan teknologi digital menyebabkan peningkatan signifikan terhadap bentuk dan kompleksitas cybercrime, sementara kapasitas kelembagaan kepolisian sering kali belum mampu mengimbangi perubahan tersebut. Penelitian ini bertujuan untuk menganalisis kendala kelembagaan yang dihadapi kepolisian, serta menilai bagaimana persepsi masyarakat terhadap efektivitas penegakan hukum di ranah digital. Metode penelitian yang digunakan adalah pendekatan deskriptif kualitatif dengan analisis sosio-legal, memadukan data dari literatur, regulasi, dan hasil observasi. Temuan penelitian menunjukkan bahwa keterbatasan sumber daya manusia yang ahli, kurangnya infrastruktur digital, hambatan koordinasi antar lembaga, dan minimnya regulasi teknis merupakan kendala utama. Di sisi lain, masyarakat masih memandang penanganan kasus siber belum optimal. Kesimpulannya, dibutuhkan penguatan kelembagaan, peningkatan kapasitas teknologi, serta sinergi antar lembaga agar penegakan hukum siber lebih efektif.

Kata Kunci: Kejahatan Siber; Kepolisian; Institusional; Penegakan Hukum; Sosiologi Hukum

Abstract: *This study discusses institutional challenges in law enforcement by the police in handling cybercrime in Indonesia. The development of digital technology has led to a significant increase in the forms and complexity of cybercrime, while the institutional capacity of the police has often been unable to keep pace with these changes. This study aims to analyze the institutional constraints faced by the police and assess public perceptions of the effectiveness of law enforcement in the digital realm. The research method used is a qualitative descriptive approach with socio-legal analysis, combining data from literature, regulations, and observation results. The findings show that the main obstacles are limited human resources with expertise, lack of digital infrastructure, coordination barriers between institutions, and a lack of technical regulations. On the other hand, the public still views the handling of cyber cases as suboptimal. In conclusion, institutional strengthening, increased technological capacity, and synergy between institutions are needed to make cyber law enforcement more effective.*

Keywords: *Cybercrime; Police; Institutional; Law Enforcement; Sociology Of Law*

PENDAHULUAN

Perkembangan teknologi informasi dalam dua dekade terakhir telah mengubah hampir seluruh aspek kehidupan masyarakat Indonesia. Aktivitas yang sebelumnya bergantung pada interaksi fisik kini beralih ke ruang digital, menciptakan pola kehidupan baru yang serba

DOI: https://doi.org/10.58819/jfh.v4i2.241

terhubung melalui internet. Transaksi ekonomi berlangsung melalui e-commerce dan mobile banking, komunikasi dilakukan melalui media sosial dan aplikasi pesan instan, sementara layanan publik, pendidikan, dan administrasi berbagai instansi pemerintah turut bergeser ke platform digital.[1]

Perubahan ini memberikan banyak manfaat, seperti efisiensi waktu, kemudahan akses, dan peningkatan mobilitas ekonomi. Namun, bersamaan dengan kemajuan tersebut, muncul pula tantangan besar berupa meningkatnya tindak kejahatan siber yang memiliki karakteristik lebih kompleks dibandingkan kejahatan konvensional. Kejahatan siber (cybercrime) berkembang seiring pesatnya penetrasi internet dan perangkat digital yang digunakan masyarakat.[2] Fenomena seperti penipuan online, peretasan akun pribadi, penyalahgunaan data pribadi, phishing, pencurian identitas, serta penyebaran konten ilegal semakin sering terjadi.

Bahkan bentuk kejahatan yang lebih serius, seperti ransomware, serangan terhadap sistem layanan publik, pemerasan digital, hingga manipulasi data elektronik, juga mulai muncul dan mengkhawatirkan. Sifat kejahatan siber yang tidak mengenal batas geografis membuat pelakunya bisa berasal dari mana saja, bahkan dari negara lain, sehingga penanganannya memerlukan strategi berbeda dari kejahatan yang terjadi di dunia nyata. Kompleksitas tersebut menuntut aparat penegak hukum, khususnya kepolisian, untuk memiliki kemampuan teknis, infrastruktur, dan sistem koordinasi yang sejalan dengan perkembangan teknologi.

Di Indonesia, peningkatan jumlah kasus siber menunjukkan bahwa sistem penegakan hukum belum sepenuhnya siap mengimbangi perubahan yang cepat di ranah digital. Kejahatan siber tidak hanya berdampak pada individu, tetapi juga pada keamanan nasional, integritas data, kepercayaan masyarakat terhadap teknologi, serta stabilitas ekonomi digital yang sedang berkembang. Lembaga kepolisian sebagai institusi yang bertanggung jawab untuk menegakkan hukum menghadapi tuntutan yang semakin besar untuk merespons ancaman ini.

Namun berdasarkan pengamatan dan penelitian berbagai pihak, kapasitas kelembagaan kepolisian masih memiliki banyak kekurangan, baik dari sisi sumber daya manusia, fasilitas pendukung, kesiapan sistem, maupun regulasi yang digunakan. Salah satu aspek yang menjadi perhatian utama dalam konteks ini adalah kesiapan sumber daya manusia. Penyidik dan aparat yang terlibat dalam penanganan cybercrime memerlukan keahlian teknis lanjutan seperti analisis forensik digital, pelacakan jejak elektronik, pemulihan data, serta pemahaman mengenai berbagai modus kejahatan digital yang terus berubah.

Namun pada kenyataannya, tidak semua satuan kepolisian memiliki personel yang terlatih secara memadai. Ketimpangan kemampuan antar satuan menyebabkan banyak kasus tidak dapat ditangani secara mandiri dan memerlukan bantuan dari unit khusus, sehingga proses penyelidikan menjadi lambat dan berisiko kehilangan bukti digital.[3] Selain persoalan sumber daya manusia, aspek kelembagaan lain yang turut menjadi hambatan adalah fasilitas dan infrastruktur yang belum merata. Peralatan digital forensik membutuhkan teknologi canggih dan pembaruan rutin untuk menyesuaikan dengan perkembangan sistem keamanan digital.

Namun peralatan tersebut sering kali hanya tersedia di beberapa wilayah tertentu. Ketimpangan ini memperlihatkan adanya ketidaksiapan institusi dalam menangani beban

[1] Eri Yanti Nasution et al., "Perkembangan Transaksi Bisnis E-Commerce Terhadap Pertumbuhan Ekonomi Di Indonesia," *Jesya* 3, no. 2 (2020): 506–19, https://doi.org/10.36778/jesya.v3i2.227.

[2] Mohamad Revaldy Fairuzzen et al., "Perkembangan Hukum Dan Kejahatan Siber 'Cybercrime' Di Indonesia," *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory* 2, no. 1 (2024): 139–53, https://doi.org/10.62976/ijijel.v2i1.372.

[3] Moh Riskiyadi, "Investigasi Forensik Terhadap Bukti Digital Dalam Mengungkap Cybercrime," *Cyber Security Dan Forensik Digital* 3, no. 2 (2020): 12–21, https://doi.org/10.14421/csecurity.2020.3.2.2144.

kasus yang semakin meningkat. Bukti digital yang bersifat sensitif dan mudah berubah juga menuntut keberadaan fasilitas penyimpanan yang aman serta sistem analisis yang cepat, tetapi hal ini masih belum tersedia di seluruh satuan kepolisian. Aspek kelembagaan lain yang tidak kalah penting adalah koordinasi antar instansi. Kejahatan siber melibatkan banyak pihak, seperti penyedia layanan internet, operator telekomunikasi, sektor perbankan, marketplace, serta platform media sosial yang beroperasi secara internasional.

Dalam banyak kasus, kepolisian membutuhkan akses terhadap data tertentu untuk mengungkap identitas pelaku. Namun, karena belum terdapat standar baku nasional mengenai mekanisme permintaan data, proses koordinasi sering berlangsung lama dan tidak efektif. Keterlambatan ini menjadi penghambat besar karena bukti digital dapat hilang dalam hitungan jam atau bahkan menit. Selain kelembagaan internal, kejahatan siber sangat dipengaruhi oleh dinamika sosial masyarakat, khususnya terkait persepsi publik terhadap efektivitas penegakan hukum digital.

Persepsi masyarakat menjadi faktor penting dalam sosiologi hukum karena kepercayaan publik berperan besar dalam menentukan sejauh mana hukum dapat ditegakkan dengan baik. Dalam konteks kejahatan siber, banyak masyarakat yang merasa bahwa proses pelaporan kasus digital terlalu rumit atau tidak menghasilkan penyelesaian yang jelas. Keluhan semacam ini muncul karena kurangnya komunikasi dari aparat mengenai perkembangan kasus serta minimnya edukasi mengenai cara mengamankan bukti digital. Rendahnya literasi digital masyarakat turut menambah kompleksitas persoalan.

Banyak korban tidak memahami prosedur teknis untuk menyimpan bukti digital seperti rekaman layar, file log, atau data percakapan. Ketika bukti ini tidak dikumpulkan sejak awal, penyidikan tidak dapat berjalan optimal. Kondisi ini sering kali membuat masyarakat beranggapan bahwa aparat kepolisian tidak mampu menyelesaikan kasus, padahal sebagian hambatan justru datang dari ketidaksiapan masyarakat sendiri dalam memahami mekanisme keamanan digital. Siklus persepsi negatif ini dapat melemahkan efektivitas penegakan hukum, karena masyarakat yang tidak percaya akan cenderung tidak melaporkan kasus, dan akhirnya jumlah kasus yang sebenarnya terjadi tidak tercatat secara resmi.

Melihat situasi yang semakin kompleks ini, analisis terhadap tantangan kelembagaan serta persepsi masyarakat menjadi penting untuk memahami situasi penegakan hukum dalam menghadapi cybercrime. Penelitian ini berusaha menggambarkan dua hal: pertama, identifikasi kendala kelembagaan yang dialami kepolisian dalam menangani kejahatan siber; kedua, bagaimana masyarakat memandang efektivitas kepolisian dalam menegakkan hukum di ranah digital. Melalui analisis dua aspek ini, penelitian diharapkan dapat memberikan gambaran yang lebih utuh mengenai hambatan penegakan hukum digital di Indonesia serta memberikan pemahaman yang lebih dalam tentang hubungan antara teknologi, lembaga hukum, dan sikap masyarakat.

Dari uraian tersebut, jelas bahwa tantangan penegakan hukum digital di Indonesia tidak hanya berkaitan dengan kemampuan teknis aparat, tetapi juga mencakup persoalan institusional, regulasi, infrastruktur, serta kondisi sosial masyarakat. Oleh karena itu, penelitian ini memiliki tujuan yang penting untuk memberikan pemahaman kritis mengenai bagaimana sistem hukum Indonesia beradaptasi dan merespons kejahatan siber di era digital yang penuh dinamika.

METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif dengan karakter deskriptif untuk menggambarkan secara mendalam situasi penegakan hukum terhadap kejahatan siber di Indonesia. Metode kualitatif dipilih karena penelitian ini berfokus pada penjelasan sosial dan kelembagaan, bukan pada pengukuran angka atau statistik. Metode ini memungkinkan peneliti menguraikan realitas kelembagaan kepolisian serta pandangan masyarakat

berdasarkan sumber-sumber yang relevan. Data yang digunakan dalam penelitian ini berasal dari berbagai dokumen resmi, seperti peraturan perundang-undangan, kebijakan pemerintah, pedoman teknis kepolisian, laporan tahunan instansi, dan publikasi lembaga yang memiliki kewenangan di bidang teknologi informasi. Selain itu, penelitian ini juga mengkaji buku, artikel jurnal, berita terpercaya, serta hasil penelitian terdahulu yang membahas kejahatan siber dan penegakan hukum digital di Indonesia. Data tersebut membantu menggambarkan kondisi nyata yang sedang terjadi dan memberikan pemahaman lebih luas mengenai tantangan kelembagaan yang dihadapi aparat. Proses pengumpulan data dilakukan melalui pembacaan, pencatatan, dan penelaahan terhadap semua sumber yang relevan. Setiap dokumen dan literatur dianalisis untuk menemukan informasi mengenai kapasitas kepolisian, proses penyelidikan terhadap kasus siber, hambatan yang dialami aparat, serta pandangan masyarakat terkait penanganan cybercrime. Hasil penelusuran data kemudian disusun secara sistematis untuk mendapatkan gambaran yang utuh mengenai hubungan antara kelembagaan penegakan hukum dan kondisi sosial di masyarakat.

HASIL DAN PEMBAHASAN

Hasil

Penelitian ini menunjukkan bahwa kejahatan siber di Indonesia terus meningkat seiring dengan tingginya penggunaan teknologi dalam kehidupan sehari-hari. Aktivitas ekonomi digital, transaksi daring, perbankan elektronik, hingga penggunaan media sosial membuka peluang bagi pelaku kejahatan untuk mengeksploitasi celah keamanan digital.[4] Jenis kejahatan yang paling sering muncul meliputi penipuan online, pembobolan akun pribadi, pencurian identitas digital, peretasan data pribadi, serta penyebaran konten ilegal.[5]

Selain itu, bentuk cybercrime yang lebih kompleks seperti serangan ransomware, pencurian data layanan publik, hingga akses ilegal ke sistem komputasi lembaga pemerintah juga mulai banyak ditemukan dan membuat situasi semakin rumit untuk ditangani aparat penegak hukum. Hasil penelitian memperlihatkan bahwa kepolisian menghadapi kendala yang cukup serius dalam menanganinya. Salah satu temuan penting adalah keterbatasan kapasitas sumber daya manusia yang menguasai bidang teknologi informasi. Banyak personel kepolisian di daerah belum memiliki kemampuan digital forensik atau keahlian teknis untuk menelusuri jejak elektronik, memulihkan data, atau membaca pola kejahatan digital.

Kondisi ini berdampak pada lambatnya penanganan kasus karena satuan di daerah harus meminta bantuan unit yang lebih tinggi, yang menyebabkan proses penyidikan menjadi panjang dan tidak efisien. Selain itu, penelitian menemukan bahwa fasilitas dan infrastruktur pendukung penyelidikan siber belum merata di seluruh wilayah. Peralatan digital forensik, perangkat lunak pendeteksi jejak elektronik, server penyimpanan aman, dan perangkat analisis jaringan masih terbatas jumlahnya dan hanya tersedia di beberapa satuan tertentu.[6] Ketimpangan ini membuat kemampuan aparat berbeda secara signifikan antar daerah.

Satuan yang memiliki fasilitas lengkap dapat menindak kasus lebih cepat, sementara daerah lain harus menunggu alat dipinjamkan atau mengirim barang bukti ke lokasi yang lebih lengkap. Penelitian juga mengungkap bahwa koordinasi antar lembaga masih belum berjalan secara konsisten. Hampir setiap kasus siber membutuhkan dukungan data dari pihak

---

[4] Fazli Abdillah, "Dampak Ekonomi Digital Terhadap Pertumbuhan Ekonomi Di Indonesia," *Benefit: Journal of Bussiness, Economics, and Finance* 2, no. 1 (2024): 27–35, https://doi.org/10.70437/benefit.v2i1.335.

[5] Rabith Madah Khulaili Harsya, "Tinjauan Yuridis Terhadap Tanggung Jawab Platform Digital Atas Konten Ilegal Menurut Hukum Indonesia," *Sanskara Hukum Dan HAM* 4, no. 01 (2025): 276–86, https://doi.org/10.58812/shh.v4i01.609.

[6] Rizdqi Akbar Ramadhan et al., "Pelatihan Investigasi Digital Forensik," *Jurnal Pengabdian Masyarakat Dan Penerapan Ilmu Pengetahuan* 3, no. 2 (2022): 1–6, https://doi.org/10.25299/jpmpip.2022.11003.

luar, seperti operator telekomunikasi, perbankan, marketplace, atau platform digital internasional.[7] Namun, belum adanya prosedur baku mengenai tata cara permintaan data membuat prosesnya sering memakan waktu lama.

Keterlambatan ini berpengaruh besar karena bukti digital memiliki sifat yang mudah hilang atau berubah dalam waktu singkat. Dari sisi persepsi publik, hasil penelitian menunjukkan bahwa masyarakat belum sepenuhnya menaruh kepercayaan pada efektivitas kepolisian dalam menangani kasus siber. Banyak korban mengaku kebingungan tentang cara melapor, prosedur yang harus dijalani, serta langkah awal untuk mengamankan bukti digital. Beberapa dari mereka merasa prosesnya lambat dan tidak mendapatkan informasi perkembangan kasus yang jelas.

Rendahnya literasi digital masyarakat membuat banyak orang tidak menyadari bahwa bukti elektronik harus diamankan dengan tepat waktu agar bisa diproses secara hukum. Kurangnya edukasi publik dan minimnya transparansi penanganan kasus menambah ketidakpuasan masyarakat terhadap institusi penegak hukum.

Pembahasan

Pembahasan jurnal ini menyoroti dua aspek utama yang secara langsung berkaitan dengan rumusan masalah penelitian, yaitu kendala kelembagaan dalam menangani kejahatan siber serta persepsi masyarakat terhadap efektivitas kepolisian dalam penegakan hukum digital. Kedua aspek ini tidak dapat dipisahkan karena saling memengaruhi dan memberikan gambaran menyeluruh mengenai sejauh mana kepolisian mampu merespons ancaman kejahatan siber yang semakin berkembang. Melalui pendekatan sosiologi hukum, pembahasan ini menunjukkan bahwa penegakan hukum terhadap cybercrime tidak hanya bergantung pada aturan tertulis, tetapi juga pada kesiapan institusi penegak hukum serta sikap masyarakat terhadap proses hukum tersebut.

Pembahasan pertama berkaitan dengan kendala kelembagaan dalam menangani kejahatan siber. Dari hasil penelitian, terlihat bahwa hambatan utama terletak pada kapasitas sumber daya manusia. Penanganan kasus siber membutuhkan penyidik yang tidak hanya memahami hukum, tetapi juga menguasai aspek teknis yang berhubungan dengan teknologi informasi. Cybercrime tidak dapat ditangani dengan pendekatan konvensional karena pelakunya sering menggunakan metode yang rumit seperti penyamaran digital, enkripsi, tunneling, botnet, hingga pemanfaatan server luar negeri.

Namun kenyataannya, sebagian besar satuan kepolisian di daerah belum memiliki penyidik yang memiliki pelatihan digital forensik atau pengalaman dalam menganalisis bukti elektronik. Kekurangan kompetensi ini membuat aparat sering bergantung pada unit khusus yang berada di tingkat pusat, sehingga proses penyelidikan membutuhkan waktu lebih panjang dan berpotensi kehilangan jejak digital penting. Selain aspek sumber daya manusia, kelembagaan dalam menangani kejahatan siber juga dipengaruhi oleh keterbatasan sarana dan teknologi pendukung.

Penanganan bukti digital memerlukan perangkat lunak berlisensi, alat forensik khusus, server penyimpanan yang aman, hingga jaringan komputer yang memenuhi standar analisis digital. Namun fasilitas tersebut tidak tersedia secara merata di seluruh wilayah. Beberapa satuan memiliki peralatan lengkap, sementara satuan lainnya harus menggunakan perangkat yang sangat terbatas. Ketimpangan ini menimbulkan perbedaan kemampuan dalam menangani kasus. Bukti digital seperti log aktivitas, metadata, file terenkripsi, atau rekaman jaringan membutuhkan alat analisis tertentu yang tidak dimiliki semua satuan.

[7] Arry Bainus and Junita Budi Rachman, "Editorial: Hubungan Internasional Digital (Digital International Relations)," *Intermestic: Journal of International Studies* 8, no. 1 (2023): 1, https://doi.org/10.24198/intermestic.v8n1.1.

Ketika perangkat tersebut tidak tersedia, penyidikan membutuhkan proses tambahan untuk mengirim bukti ke unit lain, sehingga meningkatkan risiko kerusakan bukti. Koordinasi antar lembaga juga menjadi bagian penting dari kendala kelembagaan. Hampir semua kasus siber membutuhkan data dari pihak ketiga seperti penyedia layanan internet, operator telekomunikasi, platform media sosial, lembaga keuangan, maupun marketplace. Namun proses koordinasi dengan pihak-pihak ini tidak selalu berjalan lancar. Belum adanya standar baku mengenai prosedur pemberian data menyebabkan penyidik sering harus menunggu lama untuk memperoleh informasi yang dibutuhkan.[8]

Padahal data digital memiliki batas waktu tertentu sebelum hilang atau berubah. Kurang efektifnya koordinasi ini menunjukkan bahwa sistem penegakan hukum belum memiliki integrasi yang kuat untuk menghadapi kejahatan digital yang bersifat lintas sektor. Selain faktor teknis dan koordinasi, aspek regulasi juga menjadi bagian dari masalah kelembagaan. Walaupun terdapat aturan yang mengatur aktivitas digital seperti Undang-Undang Informasi dan Transaksi Elektronik, isi regulasi tersebut belum sepenuhnya mengakomodasi kebutuhan teknis penyidikan siber.[9]

Misalnya, belum ada aturan yang mengatur standar penyimpanan bukti digital, batas waktu penyedia layanan harus menyerahkan data, atau pedoman baku untuk kerja sama antar negara dalam kasus yang melibatkan server luar negeri. Akibatnya, penyidik sering harus menafsirkan sendiri prosedur yang digunakan, dan hal ini membuat proses penanganan kasus berbeda-beda antar wilayah. Ketidakselarasan prosedur ini melemahkan konsistensi penegakan hukum dan berdampak langsung pada efektivitas kepolisian dalam menangani kasus siber.

Pembahasan selanjutnya menyoroti persepsi masyarakat terhadap efektivitas kepolisian dalam menangani kejahatan siber sebagai bagian dari rumusan masalah kedua. Persepsi masyarakat merupakan elemen penting dalam sosiologi hukum karena keberhasilan penegakan hukum sangat dipengaruhi oleh tingkat kepercayaan publik. Berdasarkan temuan penelitian, sebagian masyarakat menilai bahwa proses penanganan kasus siber masih belum berjalan dengan cepat dan efektif. Banyak korban yang merasa bahwa laporannya tidak mendapatkan respon yang memadai atau mengalami keterlambatan dalam proses tindak lanjut.

Kurangnya komunikasi dari aparat terkait perkembangan kasus membuat masyarakat merasa bahwa penyidikan tidak dijalankan secara serius. Rendahnya literasi digital masyarakat turut memperkuat persepsi negatif ini. Banyak korban tidak memahami bahwa bukti digital harus diamankan dengan cara tertentu agar dapat digunakan dalam proses hukum. Misalnya, banyak korban yang menghapus pesan, tidak menyimpan tangkapan layar, atau tidak mencatat bukti elektronik sebelum melapor. Ketika laporan mereka tidak dapat ditindaklanjuti karena kurangnya bukti yang valid, masyarakat menganggap bahwa kepolisian tidak mampu menyelesaikan kasus, padahal sebagian besar hambatan muncul sebelum proses hukum dimulai.

Ketidakseimbangan pemahaman ini menyebabkan masyarakat menyalahkan aparat tanpa mengetahui kendala teknis yang sebenarnya dihadapi. Selain itu, persepsi negatif masyarakat juga dipengaruhi oleh minimnya edukasi publik mengenai prosedur pelaporan dan penanganan kejahatan siber. Tidak adanya sosialisasi yang terstruktur membuat masyarakat tidak mengerti langkah awal yang harus dilakukan ketika menjadi korban,

[8] Yedija Otniel Purba and Agus Mauluddin, "Kejahatan Siber Dan Kebijakan Identitas Kependudukan Digital: Sebuah Studi Tentang Potensi Pencurian Data Online," *JCIC : Jurnal CIC Lembaga Riset Dan Konsultan Sosial* 5, no. 2 (2023): 55–66, https://doi.org/10.51486/jbo.v5i2.113.

[9] Nabila Aulia Agustin and Refania Meilani Firdos, "Studi Literatur : Ancaman Cybercrime Di Indonesia Dan Pentingnya Pemahaman Akan Fenomena Kejahatan Digital," *Jurnal Mahasiswa Teknik Informatika* 3, no. 1 (2024): 126–31, https://doi.org/10.35473/jamastika.v3i1.2841.

sehingga kasus tidak dapat diproses secara maksimal. Ketika masyarakat merasa tidak dibantu atau tidak diberikan arahan yang jelas, kepercayaan terhadap kepolisian semakin menurun.[10]

Ketidakpercayaan ini kemudian menjadi bagian dari budaya hukum, di mana masyarakat menganggap bahwa melaporkan kasus siber adalah hal yang sia-sia karena tidak akan mendapat penyelesaian. Dari sudut pandang sosiologi hukum, persepsi masyarakat yang rendah terhadap institusi penegak hukum dapat melemahkan efektivitas sistem hukum secara keseluruhan. Ketika masyarakat tidak percaya, mereka cenderung enggan melapor. Akibatnya, banyak kasus tidak tercatat, sehingga kepolisian tidak memiliki data yang akurat mengenai perkembangan kejahatan siber.

Kekurangan data ini membuat aparat sulit memetakan pola kejahatan dan mengembangkan strategi pencegahan yang efektif. Siklus ini menunjukkan bahwa persepsi publik bukan hanya persoalan psikologis, tetapi menjadi bagian penting dari struktur penegakan hukum itu sendiri. Melalui pembahasan ini, terlihat jelas bahwa kendala kelembagaan dalam menangani kejahatan siber dan persepsi masyarakat terhadap efektivitas kepolisian saling berkaitan dan memengaruhi proses penegakan hukum digital.

Keterbatasan internal kepolisian menghasilkan proses penyidikan yang lambat, sementara persepsi negatif masyarakat memperburuk efektivitas penegakan hukum karena rendahnya tingkat pelaporan dan kerja sama publik. Untuk memperkuat upaya penegakan hukum di era digital, kepolisian tidak hanya membutuhkan peningkatan kapasitas teknis dan kelembagaan, tetapi juga harus membangun kembali kepercayaan masyarakat melalui transparansi, komunikasi yang baik, serta edukasi digital yang berkelanjutan.

KESIMPULAN

Penelitian mengenai tantangan penegakan hukum dalam menghadapi kejahatan siber ini menunjukkan bahwa dinamika keamanan digital di Indonesia tidak dapat dipisahkan dari kesiapan kelembagaan kepolisian dan bagaimana masyarakat memandang efektivitas aparat dalam menjalankan tugasnya. Kejahatan siber yang terus berkembang dengan pola yang semakin canggih menuntut aparat penegak hukum untuk memiliki kemampuan teknis, dukungan infrastruktur, serta sistem koordinasi yang mampu mengikuti cepatnya perubahan teknologi.

Namun hasil penelitian memperlihatkan bahwa kondisi tersebut belum sepenuhnya terpenuhi, sehingga upaya penegakan hukum sering kali tidak berjalan sejalan dengan tingkat kompleksitas ancaman yang muncul di ruang digital. Dari sisi kelembagaan, penelitian ini menemukan bahwa keterbatasan sumber daya manusia menjadi hambatan paling mendasar dalam proses penanganan kasus siber. Banyak personel yang belum memiliki kompetensi teknis yang dibutuhkan untuk melakukan penyelidikan digital secara komprehensif.

Keahlian khusus seperti analisis forensik elektronik, pelacakan aktivitas jaringan, pemahaman tentang metode penyembunyian identitas digital, serta kemampuan membaca pola serangan siber masih dimiliki oleh jumlah personel yang terbatas. Kondisi ini menyebabkan proses penyelidikan tidak dapat dilakukan secara cepat dan mandiri di berbagai daerah, sehingga memperpanjang waktu penanganan dan meningkatkan risiko hilangnya bukti elektronik. Selain keterbatasan kompetensi, kelemahan sarana dan kemampuan teknologi juga menjadi bagian yang sangat mempengaruhi efektivitas penegakan hukum.

Peralatan digital forensik tidak tersedia secara merata dan banyak satuan masih bergantung pada peralatan dasar yang tidak memadai untuk menghadapi kasus dengan tingkat kesulitan tinggi. Ketidakseimbangan fasilitas ini membuat kualitas penanganan kasus tidak seragam antara satu wilayah dengan wilayah lainnya. Bukti digital yang bersifat sensitif dan

[10] Klarisa Desi Ananta et al., "Pengaruh Media Sosial Terhadap Peningkatan Kejahatan Siber Di Indonesia," *Islamic Law: Jurnal Siyasah* 9, no. 2 (2024), https://doi.org/10.53429/iljs.v9i2.858.

mudah berubah seharusnya diproses dengan cepat menggunakan teknologi yang tepat, tetapi keterbatasan tersebut membuat aparat tidak selalu dapat menindaklanjuti laporan masyarakat secara optimal.

Koordinasi antar institusi juga merupakan hambatan signifikan yang ditemukan dalam penelitian ini. Kejahatan siber hampir selalu melibatkan pihak ketiga yang memegang data penting, seperti penyedia layanan internet, operator telekomunikasi, lembaga perbankan, serta platform digital internasional. Namun tidak adanya standar baku mengenai mekanisme permintaan data membuat proses koordinasi berjalan lambat dan tidak efektif. Keterlambatan ini menyebabkan banyak potensi bukti digital tidak dapat dimanfaatkan, sehingga semakin menurunkan efektivitas penegakan hukum.

Di sisi lain, penelitian ini juga menegaskan bahwa persepsi masyarakat terhadap efektivitas kepolisian memainkan peran penting dalam keberhasilan penegakan hukum digital. Banyak masyarakat merasa bahwa laporan cybercrime ditangani secara lambat dan tanpa kejelasan perkembangan kasus. Minimnya komunikasi dan transparansi dari aparat membuat masyarakat menganggap bahwa kasus mereka tidak menjadi prioritas. Persepsi ini diperparah oleh rendahnya literasi digital masyarakat yang membuat banyak korban tidak tahu cara mengamankan bukti elektronik sebelum melapor.

Kondisi ini menyebabkan aparat sulit melanjutkan penyidikan, tetapi masyarakat sering memaknainya sebagai bentuk ketidakmampuan kepolisian. Rendahnya kepercayaan publik terhadap efektivitas aparat penegak hukum akhirnya menimbulkan siklus negatif. Ketika masyarakat merasa bahwa melaporkan kejahatan siber tidak memberikan hasil, tingkat pelaporan menurun. Rendahnya angka pelaporan ini mengurangi kemampuan aparat untuk mengidentifikasi pola kejahatan dan mengembangkan strategi penanganan yang lebih baik.

Pada tahap ini terlihat bahwa efektivitas penegakan hukum digital tidak hanya ditentukan oleh kekuatan institusi, tetapi juga oleh bagaimana masyarakat berpartisipasi dan merespons proses hukum yang berlangsung. Berdasarkan keseluruhan temuan tersebut, penelitian ini menyimpulkan bahwa penanganan kejahatan siber di Indonesia membutuhkan perbaikan yang menyeluruh. Penguatan kapasitas sumber daya manusia, pemerataan fasilitas digital forensik, pembentukan standar koordinasi antar lembaga, serta penyempurnaan regulasi teknis menjadi langkah yang sangat penting untuk meningkatkan kemampuan kelembagaan kepolisian.

Di sisi lain, peningkatan literasi digital masyarakat, sosialisasi prosedur pelaporan, serta transparansi dalam proses penyidikan diperlukan untuk membangun kembali kepercayaan publik. Dengan memperbaiki kedua aspek tersebut secara bersamaan, sistem penegakan hukum di ranah digital dapat berjalan lebih efektif, adaptif, dan mampu menghadapi ancaman kejahatan siber yang terus berkembang.

DAFTAR PUSTAKA

Abdillah, Fazli. “Dampak Ekonomi Digital Terhadap Pertumbuhan Ekonomi Di Indonesia.” *Benefit: Journal of Bussiness, Economics, and Finance* 2, no. 1 (2024): 27–35. https://doi.org/10.70437/benefit.v2i1.335.

Bainus, Arry, and Junita Budi Rachman. “Editorial: Hubungan Internasional Digital (Digital International Relations).” *Intermestic: Journal of International Studies* 8, no. 1 (2023): 1. https://doi.org/10.24198/intermestic.v8n1.1.

Desi Ananta, Klarisa, Triyo Ambodo, and Agus Tohawi. “Pengaruh Media Sosial Terhadap Peningkatan Kejahatan Siber Di Indonesia.” *Islamic Law: Jurnal Siyasah* 9, no. 2 (2024). https://doi.org/10.53429/iljs.v9i2.858.

Khulaili Harsya, Rabith Madah. “Tinjauan Yuridis Terhadap Tanggung Jawab Platform Digital Atas Konten Ilegal Menurut Hukum Indonesia.” *Sanskara Hukum Dan HAM* 4, no. 01 (2025): 276–86. https://doi.org/10.58812/shh.v4i01.609.

Mohamad Revaldy Fairuzzen, Abil Arya Putra, Akmal Reihan, and Lilik Prihatini S.H, M.H. "Perkembangan Hukum Dan Kejahatan Siber 'Cybercrime' Di Indonesia." *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory* 2, no. 1 (2024): 139–53. https://doi.org/10.62976/ijijel.v2i1.372.

Nabila Aulia Agustin and Refania Meilani Firdos. "Studi Literatur : Ancaman Cybercrime Di Indonesia Dan Pentingnya Pemahaman Akan Fenomena Kejahatan Digital." *Jurnal Mahasiswa Teknik Informatika* 3, no. 1 (2024): 126–31. https://doi.org/10.35473/jamastika.v3i1.2841.

Nasution, Eri Yanti, Prawidya Hariani, Lailan Safina Hasibuan, and Wita Pradita. "Perkembangan Transaksi Bisnis E-Commerce Terhadap Pertumbuhan Ekonomi Di Indonesia." *Jesya* 3, no. 2 (2020): 506–19. https://doi.org/10.36778/jesya.v3i2.227.

Otniel Purba, Yedija, and Agus Mauluddin. "Kejahatan Siber Dan Kebijakan Identitas Kependudukan Digital: Sebuah Studi Tentang Potensi Pencurian Data Online." *JCIC : Jurnal CIC Lembaga Riset Dan Konsultan Sosial* 5, no. 2 (2023): 55–66. https://doi.org/10.51486/jbo.v5i2.113.

Ramadhan, Rizdqi Akbar, Abdul Kudus Zaini, and Jerika Mardafora. "Pelatihan Investigasi Digital Forensik." *Jurnal Pengabdian Masyarakat Dan Penerapan Ilmu Pengetahuan* 3, no. 2 (2022): 1–6. https://doi.org/10.25299/jpmpip.2022.11003.

Riskiyadi, Moh. "Investigasi Forensik Terhadap Bukti Digital Dalam Mengungkap Cybercrime,." *Cyber Security Dan Forensik Digital* 3, no. 2 (2020): 12–21. https://doi.org/10.14421/csecurity.2020.3.2.2144.