ISSN: 2338 4638
Volume 8 Nomor 7 (2024)

'ADALAH
Buletin Hukum & Keadilan

Tantangan Aparat Penegak Hukum dalam Menangani Cybercrime di Indonesia: Kesenjangan Kapasitas, Regulasi, dan Kerjasama Lintas Batas

Gilang Rizki Aji Putra*
Universitas Islam Negeri Syarif Hidayatullah Jakarta

10.15408/adalah.v8i7.51881

Abstract:
Cybercrime has evolved into a sophisticated, transnational, and rapidly mutating form of criminality driven by technological advancement. Law enforcement agencies, as the frontline actors in combating these offenses, face complex multidimensional challenges. This article aims to comprehensively identify and analyze the challenges encountered by Indonesian law enforcement authorities—particularly the Police, the Prosecutor's Office, and related institutions—in addressing cybercrime. Employing a normative-sociological legal research method with statutory, conceptual, and case study approaches, the study reveals three principal clusters of challenges: (1) technical and human resource capacity gaps that lag behind technological developments; (2) procedural regulatory frameworks that remain insufficiently adaptive to modern cyber investigations; and (3) jurisdictional barriers and limited international cooperation in pursuing transnational offenders. Analysis of major cases, including ransomware attacks, cross-border online fraud syndicates, and dark web investigations, demonstrates persistent institutional constraints. The article concludes that comprehensive institutional reform, technological investment, and enhanced international collaboration are imperative.
Keywords: Law Enforcement Agencies, Cybercrime, Technical Capacity, Jurisdiction, International

* Peneliti pada Pusat Studi Konstitusi dan legislasi Nasional (Poskolegnas), Universitas Islam Negeri Syarif Hidayatullah Jakarta. Email: gilang.rizkiajiputra19@uinjkt.ac.id.

A. PENDAHULUAN

Aparat penegak hukum polisi, jaksa, dan hakim adalah ujung tombak yang menentukan efektivitas sistem peradilan pidana. Di era pra-digital, para aparat ini dibekali dengan kerangka hukum yang relatif stabil dan modus kejahatan yang secara fisik dapat diobservasi. Namun, era digital telah mengubah segalanya. *Cybercrime* yang mereka hadapi kini bersifat teknis, anonim, otomatis, dan transnasional. Pelaku tidak lagi berdiri di depan mereka dengan barang bukti di tangan; sebaliknya, ia bersembunyi di balik *Virtual Private Network* (VPN), server di negara ketiga, dan identitas digital palsu. Jejak yang ditinggalkannya adalah data biner di cloud, bukan sidik jari di gagang pintu.

Dalam konteks inilah pertanyaan tentang kesiapan aparat penegak hukum menjadi sangat krusial. Apakah penyidik di Kepolisian Resor di daerah terpencil memiliki kemampuan untuk mengamankan *log server* sebelum terhapus? Apakah jaksa penuntut umum mampu menerjemahkan temuan forensik digital menjadi dakwaan yang meyakinkan? Apakah hakim memiliki literasi teknis untuk menilai *chain of custody* bukti digital? Realitas di lapangan menunjukkan bahwa jarak antara tuntutan zaman dan kapasitas aparat masih sangat lebar. Data dari Mabes Polri menunjukkan bahwa jumlah penyidik siber bersertifikasi masih jauh dari ideal, sementara laboratorium forensik digital yang terakreditasi hanya terkonsentrasi di kota besar

(Bareskrim Polri, 2023). Di sisi lain, aparat juga dihadapkan pada regulasi prosedural yang dirancang untuk era fisik, seperti KUHAP yang tidak mengatur tentang penggeledahan data lintas batas, penyitaan aset kripto, atau penyadapan *end-to-end encrypted communication.*

Keadaan ini menuntut analisis yang jujur dan mendalam: apa sebenarnya tantangan-tantangan paling kritis yang dihadapi? Tanpa diagnosis yang akurat, solusi yang ditawarkan hanya akan bersifat tambal sulam. Rumusan masalah artikel ini adalah: Pertama, apa saja tantangan fundamental yang dihadapi oleh aparat penegak hukum Indonesia dalam menangani *cybercrime*? Kedua, bagaimana strategi penguatan kapasitas dan reformasi prosedural yang dapat ditempuh? Tujuannya adalah untuk memetakan kesenjangan antara tuntutan penanganan cybercrime modern dengan kapasitas dan kewenangan aparat saat ini, serta merumuskan rekomendasi strategis untuk menutup celah tersebut.

B. *PACING PROBLEM*, KESENJANGAN KAPASITAS, DAN TEORI *NODAL GOVERNANCE*

Untuk memahami tantangan aparat penegak hukum, kerangka teoretis yang digunakan terdiri dari tiga lapis. Pertama, konsep *pacing problem* yang dikemukakan oleh Marchant (2011) menggambarkan bahwa hukum selalu tertinggal di belakang teknologi. *Cybercrime* bermutasi dalam hitungan bulan, sementara undang-undang acara pidana baru

berubah dalam hitungan dekade. Aparat sebagai pelaksana hukum menjadi pihak yang paling merasakan dampak pacing problem ini: mereka harus menangani kejahatan yang modusnya belum diatur dalam prosedur baku, menggunakan alat yang mungkin belum dilegitimasi secara eksplisit oleh hukum. Kesenjangan ini menciptakan dilema: melangkah dengan risiko tindakannya dianggap ilegal di pengadilan, atau diam dan membiarkan pelaku lolos.

Kedua, teori kesenjangan kapasitas (*capacity gap*) dalam penegakan hukum menjelaskan bahwa efektivitas penanggulangan kejahatan tidak hanya ditentukan oleh kualitas norma, tetapi oleh ketersediaan sumber daya manusia, teknologi, dan anggaran yang dimiliki oleh institusi penegak hukum (Brenner, 2022). *Capacity gap* di Indonesia sangat nyata: rasio penyidik siber terhadap jumlah kasus sangat timpang, peralatan forensik ketinggalan versi, dan pelatihan seringkali tidak berkelanjutan.

Ketiga, teori nodal governance yang dikembangkan oleh Shearing dan Wood (2003) menekankan bahwa keamanan di era kompleks tidak dapat diwujudkan oleh negara sendirian. Penegakan hukum siber memerlukan kolaborasi antara pemerintah, swasta (penyelenggara platform, penyedia keamanan), akademisi, dan masyarakat sipil. Aparat yang bekerja secara terisolasi akan gagal karena kunci bukti seringkali berada di tangan

korporasi global seperti Google atau Meta. Kerangka ini menunjukkan bahwa kelemahan aparat tidak semata-mata bersumber dari internal, melainkan juga dari belum terbangunnya ekosistem penegakan hukum siber yang kolaboratif.

C. TIGA KLUSTER TANTANGAN FUNDAMENTAL APARAT PENEGAK HUKUM

1. Kesenjangan Kapasitas Teknis dan Sumber Daya Manusia

Tantangan pertama dan paling mendasar adalah kesenjangan antara kapasitas teknis aparat dengan kecanggihan *cybercrime* yang terus meningkat. *Cybercrime* saat ini bukan lagi dilakukan oleh peretas amatir, melainkan oleh sindikat terorganisasi yang memiliki spesialis: pembuat malware, operator botnet, pencuci uang kripto, dan ahli *social engineering*. Mereka menggunakan enkripsi militer, *artificial intelligence*, dan infrastruktur *dark web.* Untuk menghadapi ini, aparat idealnya memiliki kemampuan yang setara: memahami arsitektur *blockchain*, mampu melakukan analisis traffic jaringan terenkripsi, dan menguasai teknik OSINT (*Open Source Intelligence*) serta HUMINT digital. Namun, realitas di Indonesia sangat kontras.

Pusat Laboratorium Forensik (Puslabfor) Polri dan laboratorium BSSN memang memiliki sejumlah personel yang sangat terampil, tetapi jumlah mereka sangat terbatas. Di tingkat Polda dan Polres,

penyidik siber seringkali merupakan lulusan pendidikan hukum konvensional yang mendapat pelatihan singkat, bukan latar belakang ilmu komputer. Akibatnya, ketika menghadapi kasus *cryptojacking*, *ransomware*, atau SIM *swap fraud*, mereka kesulitan memahami substansi teknisnya. Kelemahan ini berimplikasi langsung pada kualitas penyidikan: bukti digital tidak diamankan dengan benar, analisis tidak tajam, dan laporan forensik tidak memenuhi standar yang dibutuhkan jaksa dan hakim (Santoso, 2023).

Keterbatasan peralatan juga krusial. Perangkat *write blocker*, perangkat lunak forensik berlisensi seperti *Cellebrite* atau *Oxygen Forensic*, serta perangkat untuk mengekstrak data dari perangkat IoT sangat mahal. Banyak satuan kerja yang tidak memilikinya dan terpaksa menggunakan tools gratisan yang kredibilitasnya mudah dipertanyakan di pengadilan. Selain itu, gaji dan kesejahteraan aparat siber yang tidak kompetitif dengan sektor swasta seringkali menyebabkan brain drain: talenta terbaik lebih memilih bekerja di perusahaan teknologi dengan remunerasi berkali-kali lipat (Prasetyo, 2024).

2. Kelemahan Kerangka Regulasi Prosedural

Tantangan kedua bersumber dari kerangka hukum acara yang usang dan tidak adaptif. KUHAP yang disahkan pada tahun 1981 tidak mengenal konsep penggeledahan digital, penyitaan data di

cloud, atau penyadapan komunikasi terenkripsi. UU ITE memang memberikan landasan bagi pengakuan bukti digital dan kewenangan penyidik, tetapi tidak mengatur prosedur rincinya. Pertanyaan-pertanyaan praktis yang dihadapi penyidik setiap hari tidak terjawab oleh undang-undang: Bagaimana cara yang sah menyita data yang tersimpan di server Google di California? Apakah penyidik boleh menyamar sebagai pengguna di forum gelap untuk menangkap pedagang data ilegal? Apa dasar hukum untuk memaksa tersangka membuka kunci biometrik perangkatnya?

Ketiadaan aturan yang jelas ini menimbulkan dua risiko ekstrem. Di satu sisi, penyidik bisa terlalu berhati-hati dan tidak melakukan tindakan apa pun, sehingga bukti hilang. Di sisi lain, penyidik bisa bertindak progresif tetapi tindakannya kemudian dinyatakan tidak sah oleh pengadilan, sehingga bukti yang telah susah payah dikumpulkan menjadi tidak dapat digunakan. Beberapa yurisdiksi telah memiliki *Digital Evidence Act* atau panduan komprehensif tentang *lawful interception* dan *undercover cyber operations.* Indonesia belum memilikinya.

Selain itu, prosedur *Mutual Legal Assistance* (MLA) yang menjadi jalan utama untuk meminta data dari luar negeri atau mengekstradisi pelaku berjalan sangat birokratis dan lamban. Sebuah permintaan MLA bisa memakan waktu berbulan-bulan, sementara pelaku sudah menghapus jejak dan

berpindah lokasi dalam waktu kurang dari 24 jam (ID-SIRTII, 2023). Ketiadaan ratifikasi Konvensi Budapest juga membuat Indonesia tidak memiliki akses ke jalur cepat kerjasama internasional yang tersedia bagi 68 negara pihak.

3. Hambatan Yurisdiksi, Atribusi, dan Kerjasama Internasional

Cybercrime hampir selalu memiliki dimensi transnasional. Pelaku di negara A mengendalikan server di negara B untuk menipu korban di negara C, lalu menyimpan hasil kejahatan dalam mata uang kripto yang terdesentralisasi. Bagi aparat Indonesia, ini adalah mimpi buruk yurisdiksi. Berdasarkan asas teritorialitas yang dianut KUHP dan KUHAP, yurisdiksi hukum pidana Indonesia terbatas pada perbuatan yang terjadi atau akibat yang dirasakan di wilayah Indonesia. Namun, bagaimana jika pelaku, infrastruktur, dan hasil kejahatan semuanya berada di luar negeri?

Masalah atribusi (menentukan siapa pelaku sebenarnya di balik identitas digital) sangat sulit. Pelaku profesional menggunakan *proxy chain, Tor network*, VPN tanpa log, dan identitas curian. Kepolisian bisa saja berhasil melacak alamat IP, tetapi setelah ditelusuri melalui MLA, ternyata alamat IP tersebut milik korban peretasan yang tidak tahu-menahu, atau milik layanan *bulletproof hosting* di negara yang tidak kooperatif. Kegagalan atribusi ini menimbulkan impunitas, dan dalam beberapa

kasus, aparat akhirnya hanya menangkap "kaki tangan" lokal yang perannya sangat kecil, sementara otak kriminal tetap bebas beroperasi (Brenner, 2022).

Kerjasama antarnegara yang lemah memperparah situasi. Meskipun Indonesia memiliki beberapa perjanjian bilateral, jaringan kerjasama kepolisian di tingkat ASEAN seperti ASEANAPOL masih berfokus pada kejahatan konvensional, belum memiliki *cyber desk* yang efektif. Akibatnya, ketika menghadapi sindikat penipuan daring Tiongkok yang beroperasi di Kamboja dengan korban di Indonesia, koordinasi penanganannya membutuhkan diplomasi yang rumit dan mahal.

D. STUDI KASUS: REALITAS LAPANGAN YANG DIHADAPI APARAT

Penyidik dan Serangan Ransomware PDNS (2024)

Ketika Pusat Data Nasional Sementara diserang ransomware pada Juni 2024, aparat dari BSSN dan Polri langsung dikerahkan. Mereka menghadapi situasi di mana data vital pemerintahan tersandera, dan tuntutan publik untuk segera memulihkan layanan sangat tinggi. Di saat yang sama, investigasi harus berjalan untuk menemukan pelaku. Tim penyidik langsung berhadapan dengan tantangan teknis: *ransomware Brain Cipher* menggunakan enkripsi kuat, dan *command and control server* pelaku berada di luar negeri dengan server proxy berlapis. Upaya melacak aliran tebusan

yang diminta dalam Bitcoin memerlukan analisis blockchain yang tidak semua penyidik kuasai. Kasus ini menunjukkan bahwa aparat bekerja di bawah tekanan luar biasa: di satu sisi harus melakukan investigasi kompleks, di sisi lain mendengar kritik publik yang mempertanyakan kinerja. Ketiadaan perjanjian MLA yang cepat dengan negara tempat server pelaku berada menghambat penindakan (Nugroho, 2024).

Pengungkapan Sindikat Scamming Lintas Negara (2022)

Pada tahun 2022, Polri mengungkap sindikat penipuan daring yang menargetkan warga negara asing dan beroperasi dari Jakarta. Penyidik berhasil menangkap puluhan tersangka dan menyita perangkat elektronik. Namun, analisis forensik digital mengungkap bahwa server utama sindikat berada di Kamboja, dan pemimpin sindikat adalah warga negara Tiongkok yang tidak pernah menginjakkan kaki di Indonesia. Proses untuk meminta bantuan penangkapan melalui MLA dengan Tiongkok dan Kamboja berjalan lambat. Sementara itu, tersangka yang ditangkap hanyalah operator yang digaji rendah, bukan aktor intelektual. Jaksa kesulitan membangun dakwaan pencucian uang karena aliran dana tersebar di berbagai bursa kripto luar negeri yang tidak memiliki kewajiban pelaporan ke PPATK Indonesia. Kasus ini menunjukkan bahwa aparat, meskipun telah bekerja keras, seringkali hanya mampu menyentuh

permukaan dari gunung es kejahatan transnasional (Mulyadi, 2023).

Kegagalan Investigasi karena *Chain of Custody* di Daerah

Di tingkat daerah, situasinya lebih parah. Seorang penyidik Polres di Sumatra pernah menangani kasus penipuan online shop di media sosial. Korban memberikan bukti tangkapan layar percakapan. Pelaku berhasil diidentifikasi dan ditangkap. Namun, di pengadilan, penasihat hukum pelaku mempertanyakan keaslian bukti. Penyidik tidak melakukan imaging forensik terhadap ponsel pelaku; ia hanya membuka dan membaca percakapan, lalu mencetaknya tanpa pendampingan ahli. Tidak ada *chain of custody* yang memadai. Akibatnya, hakim membebaskan pelaku. Kasus sederhana ini menunjukkan bahwa kelemahan pemahaman prosedur forensik di tingkat akar rumput dapat menggagalkan seluruh proses penegakan hukum, bahkan untuk kejahatan yang pelakunya sudah tertangkap (Santoso, 2023).

E. KAPASITAS, REGULASI, DAN KOLABORASI

Untuk mengatasi tantangan-tantangan ini, dibutuhkan strategi yang sistematis dan berani. Pertama, reformasi kapasitas. Pemerintah harus melakukan investasi besar pada sumber daya manusia aparat penegak hukum siber. Ini termasuk meningkatkan jumlah rekrutmen khusus untuk

lulusan teknik informatika dan *cybersecurity*, menyelenggarakan pelatihan dan sertifikasi internasional secara berkelanjutan, serta memberikan tunjangan khusus yang memadai untuk mencegah brain drain. Setiap Polda harus memiliki satuan siber dengan laboratorium forensik digital minimum yang mampu menangani akuisisi dasar. Anggaran khusus untuk peralatan dan software berlisensi mutlak diperlukan.

Kedua, reformasi regulasi prosedural. Revisi KUHAP harus segera dilakukan untuk mengintegrasikan pengaturan tentang penggeledahan digital, penyitaan data di cloud, penyadapan komunikasi terenkripsi, *undercover cyber operations*, dan prosedur penyitaan aset kripto. Selain itu, perlu disusun Peraturan Pemerintah atau Peraturan Bersama yang memberikan panduan rinci tentang lawful access dan penanganan bukti digital lintas batas. Ratifikasi Konvensi Budapest dan Protokol Tambahannya harus menjadi prioritas diplomatik agar aparat memiliki akses ke mekanisme kerjasama internasional yang lebih cepat dan efektif (Kusumawardhani, 2024).

Ketiga, pengembangan model *cybercrime task force* terintegrasi. Mengingat *cybercrime* multidimensi, penanganannya tidak bisa hanya oleh Polri. Dibutuhkan gugus tugas tetap yang beranggotakan penyidik Polri, jaksa, analis BSSN, intelijen keuangan PPATK, serta perwakilan dari sektor swasta (penyedia layanan internet, platform digital,

perbankan). Gugus tugas ini memiliki protokol bersama, pusat data ancaman terintegrasi, dan mekanisme fast-track untuk respons insiden yang memerlukan tindakan kurang dari 24 jam. Model ini telah berhasil di Singapura dengan *Cybercrime Command*-nya.

Keempat, membangun kemitraan publik-swasta yang kuat. Aparat tidak bisa melawan cybercrime sendirian. Platform digital global seperti Meta, Google, dan Microsoft menyimpan kunci bukti dari jutaan kejahatan. Perjanjian kerjasama formal harus dibuat untuk mempercepat respons *takedown* dan penyediaan data. Di sisi lain, perusahaan keamanan siber dan perbankan harus dilibatkan dalam pertukaran informasi ancaman secara *real-time* melalui *Information Sharing and Analysis Center* (ISAC).

F. KESIMPULAN

Aparat penegak hukum Indonesia menghadapi tantangan berat dalam menangani cybercrime yang bersumber dari tiga kluster utama: kesenjangan kapasitas teknis dan SDM yang kronis, kelemahan kerangka regulasi prosedural yang usang, serta hambatan yurisdiksi dan kerjasama internasional yang belum efektif. Menjawab rumusan masalah, tantangan ini bukan sekadar soal kurangnya alat, melainkan persoalan struktural yang mencakup rekrutmen, pendidikan, anggaran, legislasi, dan diplomasi. Studi kasus menegaskan

bahwa di tengah keterbatasan, aparat seringkali bekerja dalam kondisi mission impossible, dan ketika gagal, publik menyalahkan mereka tanpa memahami kompleksitas di baliknya.

Rekomendasi yang diajukan mencakup: pertama, investasi nasional pada pengembangan SDM dan infrastruktur forensik digital yang merata hingga ke daerah; kedua, percepatan revisi KUHAP dan penyusunan regulasi prosedural siber yang komprehensif; ketiga, pembentukan Cybercrime Task Force nasional yang terintegrasi; keempat, ratifikasi Konvensi Budapest dan penguatan diplomasi penegakan hukum siber; serta kelima, pengembangan kemitraan strategis dengan sektor swasta teknologi. Tanpa langkah-langkah ini, aparat penegak hukum akan terus menjadi David yang bertarung melawan Goliath digital, berjuang dengan ketapel di tengah perang cyber.

REFERENSI:

Bareskrim Polri. (2023). Laporan Tahunan Penanganan Kejahatan Siber 2022. Jakarta: Dittipidsiber.

Brenner, S. W. (2022). Cybercrime: Criminal Threats from Cyberspace (2nd ed.). Praeger.

ID-SIRTII. (2023). Laporan Aktivitas Kejahatan Siber terhadap Pengguna Indonesia 2022. Indonesia

Security Incident Response Team on Internet Infrastructure.

Kusumawardhani, A. (2024). Rekonsepsi Hukum Acara Pidana dalam Menghadapi Kejahatan Digital. Jurnal Hukum Siber, 6(1), 15–32.

Marchant, G. E. (2011). The Growing Gap Between Emerging Technologies and the Law. The International Library of Ethics, Law and Technology, 7, 19–33.

Mulyadi, L. (2023). Social Engineering dan Evolusi Penipuan Digital: Perspektif Hukum Pidana. Jurnal Legislasi Hukum, 20(3), 412–428.

Nugroho, A. (2024). Serangan Ransomware terhadap Infrastruktur Publik: Pembelajaran dari Kasus PDNS. Jurnal Ketahanan Informasi, 5(2), 88–105.

Prasetyo, B. (2024). Dilema Kapasitas Aparat dalam Penegakan Hukum Siber di Daerah. Jurnal Hukum dan Masyarakat, 16(1), 88–107.

Santoso, L. (2023). Chain of Custody Bukti Digital dalam Sistem Peradilan Pidana Indonesia. Jurnal Yudisial, 16(3), 301–322.

Shearing, C., & Wood, J. (2003). Nodal Governance, Democracy, and the New 'Denizens'. Journal of Law and Society, 30(3), 400–419.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Tahun 2024 Nomor 1, Tambahan Lembaran Negara Nomor 6905).