ISSN 1411-3813 | E-ISSN 2684-7191
DOI: 10.46976/litbangpolri.v28i2.307

Tinjauan Yuridis Terhadap Tindak Pidana Siber

Frans Tjahyono[1], Moch.Nurhasim[2], Bintang Dwitya Cahyono[2]
[1]*Pusat Penelitian dan Pengembangan Polri,* [2]*Badan Riset dan Inovasi Nasional*
[1]*bidgasbin14000@gmail.com*

ABSTRACT

The Indonesian National Police (Polri), as the vanguard in combating cybercrime, often face challenges with existing laws and regulations. For example, cyber investigators at the Regional Police (Polda) and Resort Police (Polres) require permission from central banking institutions in Jakarta to track the accounts of individuals suspected of cybercrime. This creates a legal gap, meaning that what is expected by law/regulations does not always align with what actually happens on the ground. This demonstrates that the Indonesian National Police (Polri) faces various challenges in the institutional, technical, and regulatory spheres. This study aims to map the dynamics of cybercrime handling at the regional and district police (Polres) levels, as well as identify legal gaps and operational obstacles that hinder effective investigations. Using a mixed methods approach, data was obtained through questionnaires, focus group discussions, and document studies in 11 regional police (Polda). The results indicate disparities in investigative capabilities between regions, limited digital forensic equipment, and regulatory barriers related to access to information from banking institutions and digital platform providers. There is an urgent need for internal reform of the National Police, including increasing human resource capacity, providing facilities and infrastructure, and strengthening cross-sectoral collaboration. On the regulatory side, it is recommended to revise the Electronic Information and Transactions (ITE) Law and the Banking Law, as well as the development of specific regulations to require digital service providers to support the investigation process. This study emphasizes the importance of addressing the increasingly complex development of cybercrime.

Keyword*: Cyber Crime, Polri, Law Enforcement.*

ABSTRAK

Polri sebagai garda terdepan dalam penindakan tindak pidana siber seringkali dihadapkan dengan permasalahan peraturan perundang-undangan yang berlaku. Seperti penyidik siber di Polda/ Polres membutuhkan izin dari lembaga/institusi perbankan pusat yang berada di Jakarta jika ingin melakukan pelacakan terhadap rekening seseorang yang diduga melakukan tindak pidana siber. Hal ini menjadi sebab kesenjangan hukum (*legal gap*), yaitu apa yang diharapkan oleh hukum/peraturan tidak selalu sama dengan apa yang terjadi di lapangan. Hal ini menunjukkan bahwa penegakan hukum terhadap tindak pidana siber oleh Polri menghadapi berbagai tantangan baik di bidang kelembagaan, teknis, dan regulatif. Penelitian ini bertujuan untuk memetakan dinamika penanganan tindak pidana siber di tingkat Polda dan Polres, serta mengidentifikasi kesenjangan hukum (*legal gap*) dan hambatan operasional yang menghambat efektivitas penyidikan. Dengan menggunakan pendekatan *mix method*, data diperoleh melalui penyebaran kuesioner, diskusi kelompok terpumpun dan studi dokumen di 11 Polda. Hasil penelitian menunjukkan adanya disparitas kemampuan penyidikan antarwilayah, keterbatasan peralatan digital forensik, serta hambatan regulasi terkait akses informasi dari lembaga perbankan dan penyedia *platform digital*. Terdapat kebutuhan mendesak untuk reformasi internal Polri, termasuk peningkatan kapasitas SDM, pemenuhan sarana dan prasarana, serta penguatan kerja sama lintas sektor. Di sisi regulasi, direkomendasikan revisi terhadap UU ITE, UU Perbankan, serta penyusunan aturan khusus untuk mewajibkan penyedia layanan digital mendukung proses penyidikan. Penelitian ini menegaskan pentingnya dalam menghadapi perkembangan kejahatan siber yang kian kompleks.

Kata kunci *:* Kejahatan Siber, Polri, Penegakan hukum.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi di era Society 5.0 telah membawa transformasi besar dalam berbagai aspek kehidupan manusia. Masyarakat modern kini sangat bergantung pada teknologi digital, termasuk internet dan perangkat cerdas yang menjadi bagian integral dalam aktivitas sehari-hari. Namun, kemajuan ini juga menghadirkan tantangan serius dalam bentuk kejahatan siber (cyber crime), yaitu bentuk kriminalitas baru yang memanfaatkan teknologi informasi sebagai sarana atau objek kejahatan. Fenomena ini tidak hanya terjadi secara lokal, tetapi juga bersifat lintas negara, sehingga menuntut respons hukum dan kelembagaan yang adaptif dan progresif.Tindak pidana siber merupakan fenomena yang relatif baru dan terus berkembang, baik dari sisi modus operandi maupun kompleksitas teknis dan yuridisnya. Ancaman ini telah muncul sejak dekade 1980-an dan terus berevolusi seiring dengan pertumbuhan eksponsial teknologi informasi. Kasus-kasus seperti peretasan terhadap sistem lembaga negara, penipuan daring, carding dan penyebarankonten ilegal menjadi tantangan nyata yang dihadapi aparat penegak hukum di berbagai negara, termasuk Indonesia. Dalam konteks Indonesia, penanggulangan tindak pidana siber telah mendapatkan perhatian melalui pembentukan berbagai regulasi, antara lain Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang kemudian diperbarui dengan Undang-Undang Nomor 19 Tahun 2016 serta Undang-Undang Nomor 1 Tahun 2024. Di samping itu, ketentuan dalam Kitab Undang-Undang Hukum Pidan (KUHP) dan Kitab Undang-Undang Hukum Acara Pidana (KUHAP) juga kerap digunakan dalam penanganan tindak pidana berbasis teknologi digital.

Meskipun regulasi telah tersedia, implementasinya di lapangan masih menghadapi banyak kendala. Mulai dari keterbatasan kewenangan penyidik, perbedaan kualitas sumber daya manusia antar wilayah, hingga belum optimalnya kerja sama lintas lembaga. Hal ini menciptakan kesenjangan hukum (*legal gap*) dan perbedaan perlakuan antar kasus yang dapat menurunkan efektivitas penegakan hukum. Oleh karena itu, perlu dilakukan tinjauan yuridis yang komprehensif terhadap regulasi dan pelaksanaan penanggulangan tindak pidana siber di Indonesia.

Tinjauan yuridis dalam konteks ini dimaknai sebagai proses pemeriksaan secara sistematis dan objektif terhadap ketentuan hukum yang berlaku, serta implementasinya oleh para aparat penegak hukum, khususnya Kepolisian Negara Republik Indonesia sebagai garda terdepan dalam penyidikan. Kajian ini akan mengkaji efektivitas regulasi yang ada, kewenangan aparat, dan kendala yang dihadapi dalam proses penanganan tindak pidana siber, baik secara normatif melalui analisis peraturan perundang-undangan, maupun secara empiris melalui observasi terhadap praktik di lapangan. Berdasarkan latar belakang tersebut, maka permasalahan yang diangkat dalam penelitian ini adalah:

1. Bagaimana dinamika penanganan tindak pidana siber oleh Polri di tingkat satuan kewilayahan?
2. Apa saja kendala utama yang dihadapi dalam proses penyidikan tindak pidana siber?
3. Bagaimana peran regulasi dan struktur organisasi dalam menunjang efektivitas penanggulangan kejahatan siber?

Tujuan dari penelitian ilmiah ini adalah:

1. Melakukan identifikasi dan pemetaan proses penyelidikan dan penyidikan kasus-kasus tindak pidana siber oleh Polisi Siber di satuan kewilayahan
2. Memetakan dan menganalisis upaya pengungkapan pembuktian tindak pidana siber di satuan kewilayahan
3. Menggambarkan kendala yang dihadapi dalam upaya pengungkapan pembuktian tindak pidana siber di satuan kewilayahan
4. Memberikan rumusan dan rekomendasi Strategi dan terobosan kebijakan seperti apa yang diperlukan dalam mempercepat pengungkapan pembuktian tindak pidana siber di satuan kewilayahan

Dengan menggunakan pendekatan normatif dan empiris secara terpadu, penelitian ini diharapkan dapat memberikan kontribusi terhadap pengembangan hukum pidana di Indonesia, khususnya dalam merespons dinamika dan tantangan hukum di era digital. Tujuannya adalah untuk memperkuat sistem penegakan hukum yang adaptif dan responsif terhadap perkembangan tindak pidana siber di Indonesia.

METODE

Penentuan metodologi dalam penelitian ini merupakan komponen esensial yang menentukan validitas hasil dan keandalan interpretasi dari data yang diperoleh. Penelitian ini menggunakan pendekatan **metode gabungan (*mixed methods*)**, yaitu suatu pendekatan penelitian yang memadukan metode kualitatif dan kuantitatif secara sistematis guna memperoleh pemahaman yang lebih komprehensif, objektif, dan mendalam terhadap objek kajian.

Model ***mixed methods*** yang digunakan dalam penelitian ini adalah model **sekuensial beriringan (*concurrent sequential*)**, yaitu pengumpulan data kualitatif dan kuantitatif dilakukan secara paralel. Data kualitatif diperoleh melalui studi pustaka dan *Focus Group Discussion* (FGD), sedangkan data kuantitatif dikumpulkan melalui penyebaran kuesioner. Hasil awal dari kuesioner juga digunakan sebagai masukan untuk pendalaman lebih lanjut dalam tahap kualitatif, sehingga proses analisis berlangsung secara integratif dan berlapis. Pendekatan ini dipilih untuk menangkap kompleksitas isu yuridis dalam penanggulangan tindak pidana siber, serta memberikan pembobotan dan prioritas atas berbagai variabel hukum dan kelembagaan yang terlibat.

Pendekatan kualitatif digunakan untuk menggali persepsi, pengalaman, dan evaluasi dari para pemangku kepentingan terkait penanganan tindak pidana siber. Pengumpulan data dilakukan dengan metode sebagai berikut:

1. Studi Literatur (*Literature Review*)
   Menganalisis peraturan perundang-undangan seperti UU ITE, KUHP, KUHAP, serta dokumen hukum lain yang relevan.
2. *Focus Group Discussion* (FGD) dilakukan di dua tingkat kelembagaan, yakni:
   a. Tingkat Polda: Melibatkan pejabat dari Ditreskrimsus, Biro SDM, Bidlabfor, Bidkum, Subdit Siber, serta para penyidik siber.
   b. Tingkat Polres: Melibatkan Kapolres/Wakapolres, Kabag SDM, Kasat Reskrim, Kasikum, Kanit Tipiter, dan penyidik Tipiter.
3. Data Sekunder
   Informasi dikumpulkan dari dokumentasi resmi seperti rekapitulasi jumlah tindak pidana siber, data penyelesaian kasus (*clearance*), jumlah SDM siber, dan alokasi anggaran.

Data yang diperoleh dari 11 Polda (Polda Aceh, Polda Riau, Polda Daerah Istimewa Yogyakarta, Polda Kalimantan Selatan, Polda Sulawesi Barat, Polda Papua Barat, Polda Maluku, Polda NTB, Polda Kalimantan Timur, Polda Kepulauan Bangka Belitung dan Polda Gorontalo) yang menjadi objek penelitian akan dianalisis untuk memperoleh gambaran menyeluruh yang representatif secara nasional.

Pendekatan kuantitatif digunakan untuk mengukur persepsi dan efektivitas penegakan hukum terhadap tindak pidana siber melalui penyebaran kuesioner kepada anggota Polri yang bertugas pada fungsi siber, khususnya penyidik. Prosedur yang ditempuh meliputi:

1. Uji Validitas dan Reliabilitas :
   Sebelum disebarkan secara luas, kuesioner diuji coba kepada 53 responden dari jajaran Polda Jawa Timur (8 s.d. 10 Juni 2024). Hasil menunjukkan bahwa instrumen valid dan reliabel.
2. Teknik Sampling :
   Digunakan teknik ***purposive sampling non-probability***, yang menyasar penyidik siber di tingkat Polda dan Polres yang relevan dengan fokus penelitian.

3. Pengisian Kuesioner :
   Dilakukan secara daring menggunakan platform seperti *Google Forms*, untuk meningkatkan efisiensi distribusi dan pengumpulan data.

Secara umum metode analisis pada penelitian ini terbagi menjadi dua hal utama, yakni metode analisis penelitian kualitatif dan metode penelitian kuantitatif. Metode analisis penelitian kualitatif digunakan untuk memahami, menginterpretasikan, dan mengeksplorasi data yang bersifat tidak terstruktur atau kualitatif. Lebih lanjut, metode penelitian kualitatif yang digunakan pada penelitian ini berlandaskan pada peran filsafat *post positivisme* dan berfokus pada objek penelitian. Pada penelitian ini, peneliti berperan besar sebagai instrumen utama dalam pengumpulan data. Kemudian, teknik pengumpulan data pada penelitian kualitatif dilakukan dengan teknik triangulasi, yang melibatkan berbagai metode untuk mengumpulkan data. Sementara itu, analisis data dalam penelitian kualitatif bersifat induktif dan lebih menekankan pada pencarian makna daripada generalisasi.

Lebih lanjut, teknik penelitian kuantitatif pada penelitian ini lebih menekankan penyebaran kuesioner kepada anggota Polri, baik ditingkat Polda ataupun Polres. Analisis data dalam penelitian ini menggunakan metode *Analytical Hierarchy Process* (AHP). Secara umum, AHP kerap digunakan sebagai metode untuk memecahkan masalah dibanding metode lainnya dengan argumentasi sebagai berikut:

1. Struktur yang berhirarki, sebagai konsekuensi dari kriteria yang dipilih, sampai pada sub kriteria yang paling dalam.
2. Memperhitungkan validitas sampai dengan batas toleransi inkonsistensi berbagai kriteria dan alternatif yang dipilih oleh pengambil keputusan.
3. Memperhitungkan daya tahan output analisis sensitivitas pengambilan keputusan.

Prosedur AHP mencakup dekomposisi masalah, **p**enilaian kriteria dan sub-kriteria, **p**enyusunan matriks dan uji konsistensi, perhitungan prioritas global, pengambilan keputusan. Dengan pendekatan ini, prioritas atas berbagai strategi atau regulasi yang dapat memperkuat kewenangan penyidik dalam menangani tindak pidana siber dapat dirumuskan secara sistematis dan terstrukur.

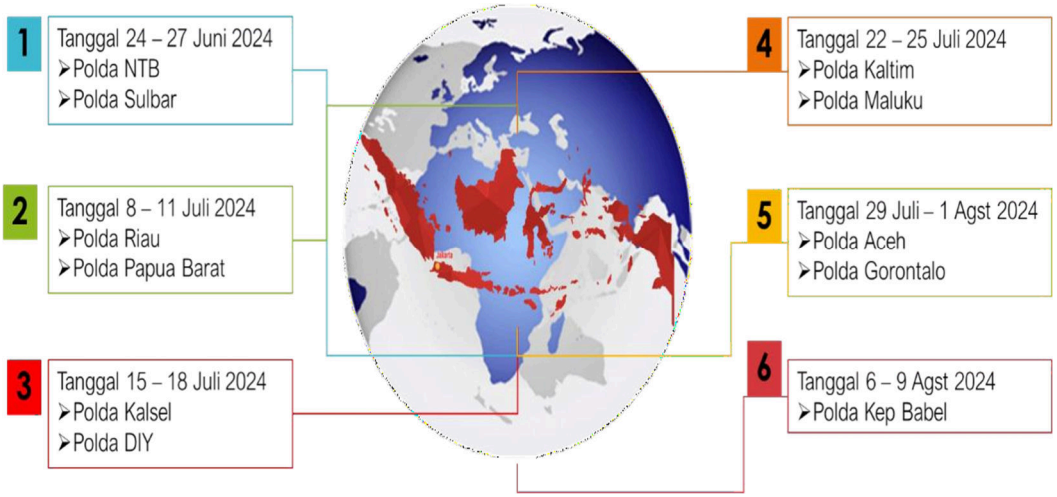
Penggunaan metode ***mixed methods*** dalam penelitian ini didasarkan atas kompleksitas fenomena hukum siber yang tidak hanya memerlukan kajian normatif, tetapi juga pengukuran empiris terhadap praktik dan efektivitas pelaksanaannya di lapangan. Pendekatan ini sejalan dengan karakteristik penelitian hukum yang bersifat multidisipliner, serta mendukung pengambilan keputusan berbasis bukti (*evidence-based policy*).

Gambar 1. Desain AHP Peningkatan Kewenangan Lidik dan Sidik Kasus tindak pidana Siber.

HASIL

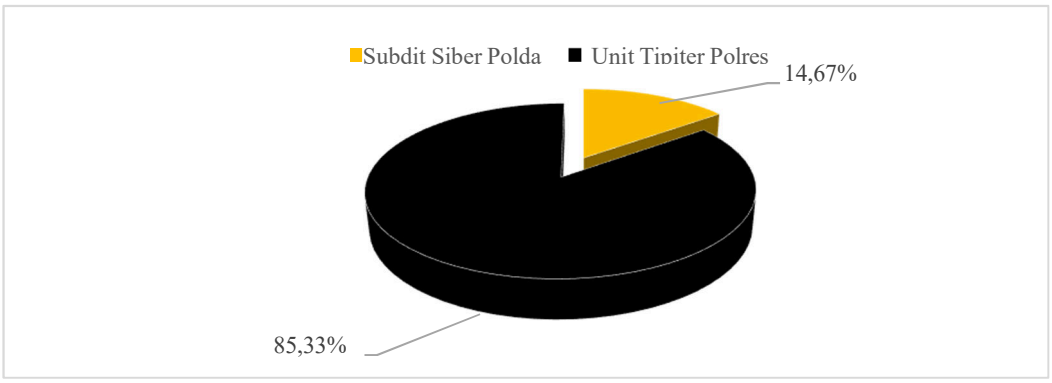
Kajian Tinjauan Yuridis Tindak Pidana Siber ini tidak memfokuskan pada bagaimana tindak pidana itu terjadi, tetapi lebih fokus pada bagaimana penanganannya. Oleh karena itu, laporan hasil kajian di 11 Polda ini secara garis besar akan digambarkan dalam beberapa sub-bab sebagai berikut: (1) Profil dan Gambaran Responden, (2) Proses Penyelidikan dan Penyidikan Tindak Pidana Siber, (3) Upaya Pembuktian Tindak Pidana Siber, (4) Kendala dan Tantangan dalam Pembuktian Tindak Pidana Siber, dan (5) Strategi dan Terobosan dalam Mempercepat Penanganan Tindak Pidana Siber.

Penelitian ini mengambil sampel di 11 Polda yang ada di Indonesia. Pelaksanaan penelitian berlangsung selama kurang lebih dua bulan dan dilakukan secara pararel terdiri dari dua tim yang bertugas, sebagian ke 5 (lima) Polda, dan 6 (enam) ke Polda yang lain. Dari 11 Polda yang dijadikan sampel dalam penelitian, lokasinya mewakili Kawasan Indonesia Bagian Barat, Bagian Tengah dan Kawasan Indonesia Bagian Timur. Pengumpulan data dilakukan melalui penyebaran kuesioner dan FGD (diskusi) dilakukan dengan sejumlah narasumber yang berasal dari 11 Polda tersebut yang meliputi: Dirreskrimsus, Karo SDM, Kabidkum, Kasat, Kanit, dan para penyidik, dilanjutkan ke minimal 30 % Polres dari setiap satuan kewilayahan (Polda).



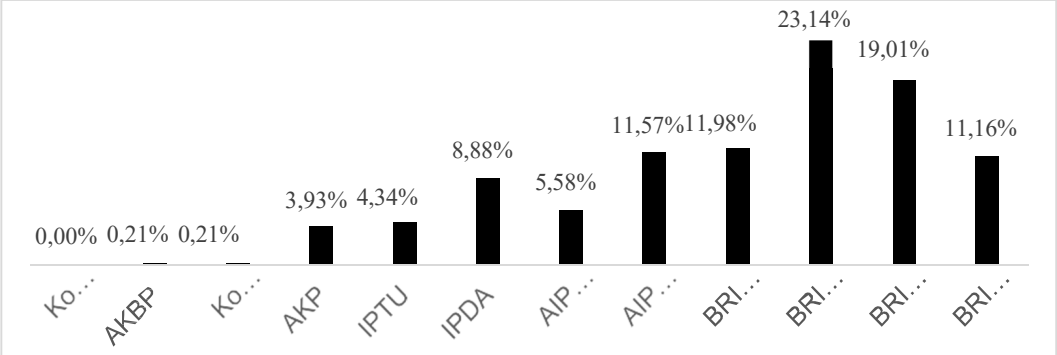
Gambar 2. Sebaran Wilayah Sampel Penelitian.

Dari 11 Polda yang dijadikan sampel penelitian, telah terhimpun sebanyak 484 responden yang merupakan penyidik siber. Dari jumlah tersebut terdapat 14,67% (71 responden) merupakan penyidik Subdit Siber Polda dan 85,33% (413 responden) merupakan penyidik dari Unit Tipiter Polres, meskipun pada sebagian kecil Polres masih ada di unit pidana umum.



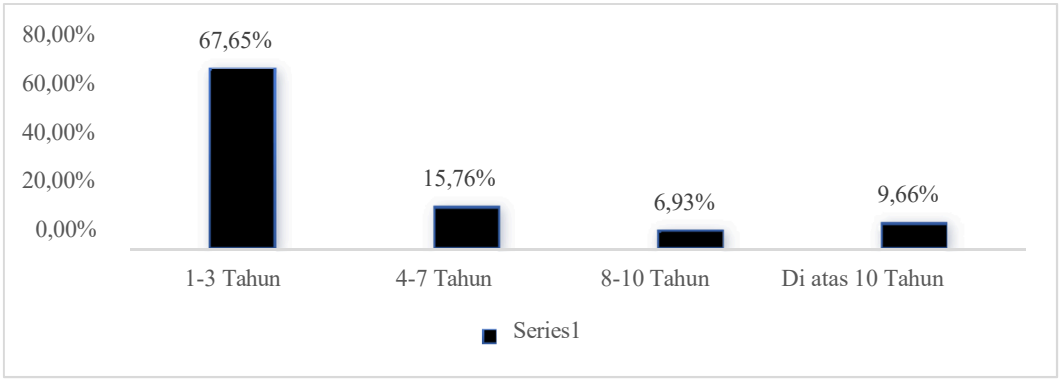
Gambar 3. Satuan kerja.
Sumber: Data yang diolah dari penyebaran kuesioner Puslitbang Polri, Juli - Agustus 2024

Responden yang menjadi objek dalam penelitian ini secara garis besar berpangkat relatif merata, tidak ada kepangkatan yang dominan. Sebanyak 23,14% berpangkat Brigppol; 19,01% Briptu, 11,16% Bripda; 11,98% Bripka; dan 11,57% Aipda. Sementara itu untuk anggota dengan pangkat Perwira Menengah sebesar 3,93% berpangkat AKP dan 0,21% berpangkat Kompol.



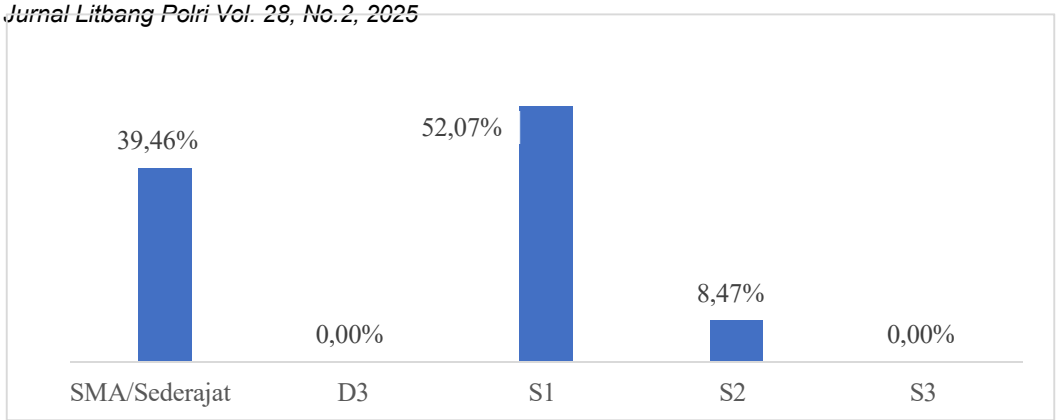
Gambar 4. Kepangkatan Responden.
Sumber: Data yang diolah dari penyebaran kuesioner Puslitbang Polri, Juli - Agustus 2024

Masa kerja (lama berdinas) responden penelitian didominasi oleh penyidik yang berdinas antara 1-3 tahun sebanyak 67,65%, 4-7 tahun berjumlah 15,76%, sedangkan 6,93% berdinas antara 8 sampai di atas tahun dan terakhir sebesar 9,66% telah berdinas selama lebih dari 10 tahun. Lama dinas ini umumnya terkait dengan pengalaman sebagai penyidik dalam menangani kasus tertentu, khususnya kasus tindak pidana siber. Seperti di singgung di atas, rata-rata penyidik di tingkat Polres, untuk fungsi siber masih digabung dengan Unit Tipiter dan belum ada unit khusus yang fokus hanya menangani kasus tindak pidana siber.



Gambar 5. Lama Berdinas Responden.
Sumber: Data yang diolah dari penyebaran kuesioner Puslitbang Polri, Juli - Agustus 2024

Tim Puslitbang Polri pada Februari-Maret 2024 telah melakukan kajian yang terkait dengan Strategi Pengembangan SDM Pelaksana Fungsi Siber. Kondisi SDM Penyidik siber di jajaran Polda yang menjadi sampel relatif mirip, meskipun objek Polda yang digunakan berbeda. Dari sisi tingkat pendidikannya, SDM penyidik siber di 11 Polda objek penelitian menunjukkan 52,07 % berpendidikan S1, dan SMA/Sederajat sebanyak 39,46 %, dan sudah menempuh pendidikan S2 sebanyak 8,47 %.



Gambar 6. Tingkat Pendidikan Responden.
Sumber: Data yang diolah dari penyebaran kuesioner Puslitbang Polri, Juli - Agustus 2024

Data di atas menunjukkan sebenarnya dari tingkat pendidikannya sudah sangat memadai. Namun demikian, tingkat pendidikan umum yang ditempuh terkadang tidak terkait dengan latar belakang di bidang siber, tetapi lebih pada latar belakang pendidikan umum.

Proses Penyelidikan dan Penyidikan Tindak Pidana Siber di Indonesia, seperti di banyak negara lain, angka tindak pidana siber terus meningkat seiring dengan meningkatnya penggunaan teknologi digital. Laporan dari pihak kepolisian dan lembaga terkait menunjukkan bahwa kasus-kasus kejahatan siber, terutama yang berkaitan dengan penipuan dan pencurian data pribadi, semakin banyak dilaporkan, sebagaimana telah disinggung pada latar belakang. Meskipun jumlah kasus meningkat, proses penyelidikan dan penyidikan terhadap tindak pidana siber sering kali menghadapi berbagai tantangan. Salah satu tantangan utama adalah minimnya pemahaman di kalangan penegak hukum tentang teknologi yang digunakan dalam kejahatan siber.

Proses penyelidikan dan penyidikan tindak pidana siber melibatkan berbagai langkah penting, dari pengumpulan bukti digital hingga analisis forensik. Ketepatan dan ketelitian dalam setiap tahap sangat diperlukan untuk memastikan bahwa bukti yang dikumpulkan dapat dipertanggungjawabkan secara hukum. Oleh karena itu, diperlukan peningkatan kapasitas dan pelatihan bagi aparat penegak hukum untuk memahami dan menangani kasus-kasus siber secara lebih efektif.

Secara umum jenis kejahatan tindak pidana siber yang banyak teradi di Polda dan Polres yang menjadi sampel penelitian yakni: 1) penipuan *online*, 2) pencemaran nama baik, 3) pornografi, dan 4) akses ilegal. Tindak pidana kejahatan siber yang terjadi pada umumnya merupakan jenis tindak pidana siber yang tergolong tidak sulit untuk dilakukan proses penyidikan dan penyelidikan.

Kondisi yang berbeda ditemukan pada Polda DI Yogyakarta dan jajaran dan juga beberapa Polda lain terkait dengan ilegal akses. Pada Polda tersebut, marak terjadi kasus akses ilegal (pembobolan akun), di mana kasus ini sangat jarang terjadi di Polda lainnya, khususnya di kawasan Timur Indonesia. Lebih lajut, kondisi penanganan kasus kejahatan siber masih belum menggambarkan hal yang memuaskan. Hal ini terkait dengan banyaknya kasus Pengaduan Masyarakat (Dumas), namun belum seluruhnya bisa menjadi Laporan Informasi (LI) yang kemudian menjadi Laporan Polisi (LP). Sebagian penyidik siber di tingkat Polda relatif sudah memadai pada proses penyelidikan dan penyidikan tindak pidana siber. Namun, ada semacam kesenjangan dengan para penyidik siber di tingkat Polres. Kondisi penanganan tindak pidana siber di tingkat polres-polres, rata-rata sangat kecil penyelesaian kasus-kasus tindak pidana sibernya, apalagi jumlah kasus yang hingga P-21 atau dipersidangkan. Faktor-faktor yang memengaruhi capaian penanganan kasus tindak pidana siber tersebut lebih lanjut akan dianalisis pada sub-bab lain, dan dalam pembahasan mengenai kendala-kendala yang dihadapi dalam proses Lidik dan Sidik tindak pidana siber. Umumnya, para penyidik di tingkat Polres kesulitan dalam pengembangan awal sebelum hingga bisa ditingkatkan pada penyelidikan dan pada tahapan-tahapan selanjutnya. Meskipun untuk beberapa kasus yang ringan, para penyidik di tingkat Polres sudah mulai bisa melakukan penyelesaian kasus.

Dari proses penyelidikan di setiap Polda, tampak bahwa rata-rata Crime Total (CT) masih belum selaras dengan Dumas. Di Tingkat Polda, range target dan penanganan dari dumas menjadi CT masih berkisar antara 30-60 kasus. Sementara di tingkat Polres, pengaduan masyarakat yang ditindaklanjuti menjadi LP antara 10-25 kasus, tergantung dari kondisi tiap Polres, karena terkait dengan rasio jumlah SDM dan juga anggaran yang dimiliki. Sebagai ilustrasi, beberapa data berikut bisa menjadi gambaran:

"*Tindak pidana siber yang dilaporkan pada Subdit V/Siber Polda Aceh tergolong masing cukup sedang, karena rata-rata catatan per tahun dumas kurang teridentifikasi dengan baik, yang ada hanya data kasus-kasus yang sudah menjadi Laporan Polisi (LP). Demikian pula dengan Dumas di beberapa Polres, jumlahnya tidak dilakukan identifikasi. Data yang ada menunjukkan di Polda yang menjadi LP di tahun 2023 sebanyak 32 LP, dan Crime Clearance (CC)nya sebanyak 52 LP (162 %) karena ada penyelesaian kasus pada tahun-tahun sebelumnya. Terbanyak dari kasus yang diselesaikan (CC) adalah kasus pencemaran nama baik berjumlah 27 kasus (207%) dan penipuan ada 10 kasus (142%), serta pornografi sebanyak 7 kasus (100%). Pencemaran nama baik umumnya diselesaikan dengan pendekatan restorative justice. Dari kasus perjudian di tahun 2023 LPnya sebanyak 2 kasus, 1 kasus dapat diselesaikan, namun umumnya menggunakan Qanun Aceh Nomor 6 Tahun 2014 tentang Hukum Jinayat khususnya Pasal 18 sampai Pasal*

22 terkait perjudian, baik yang perjudian online maupun yang konvensional. Sementara di tahun 2024, dari dumas yang ada sebanyak 30 kasus menjadi LP, dan sudah diselesaikan sebanyak 22 kasus (73%). Kasus terbanyak terkait penipuan online dengan CT sebanyak 9 kasus, dan CCnya sebanyak 7 kasus (78%). Pada tahun 2024 juga ada penyelesaian kasus akses ilegal sebanyak 2 kasus, meskipun CTnya tidak ada. Kasus terbanyak kedua yang menjadi LP adalah pornografi

dan pencemaran nama baik, masing-masing sebanyak 7 kasus, dan rata-rata bisa diselesaikan 5 kasus (71 %). Sedangkan untuk perjudian telah dapat diselesaikan, dari CT sebanyak 2 kasus, diselesaikan seluruhnya".

Gambaran yang hampir mirip misalnya juga terjadi di Polda Kaltim sebagai berikut:

"…Tindak pidana siber yang dilaporkan pada Subdit V/Siber Polda Kaltim tergolong masing cukup sedang, karena rata-rata per tahun hanya ada dumas sekitar 92 kasus dan tahun 2024 sebanyak 72 kasus. Namun di beberapa Polres, dumasnya cukup tinggi, seperti di Polresta Balikpapan pada 2023 mencapai 313 kasus dan tahun 2024 sebanyak 228 kasus. Demikian pula dengan dumas di beberapa Polres lainnya, dumas di Kuker tahun 2023 sebanyak 46 dan tahun 2024 berjumlah 64. Demikian juga dengan dumas kasus siber di Polres Bontang, pada tahun 2023 sebanyak 61 dan tahun 2024 sebesar 40. Di Polresta Samarinda, dumas kasus siber sangat tinggi, tahun 2023 sebanyak 242 dan tahun 2024 hingga bulan juni sebanyak 68, sedangkan di Kotim agak sedang, dumas tahun 2023 27 dan 2024 sebanyak 15 pengaduan. Ukurannya memang bukan dumas, namun laporan polisi (LP). Ternyata LPnya juga tidak banyak, di tingkat Polda misalnya LP tahun 2023 sebanyak 30 dan tahun 2024 berjumlah

20. Sedangkan di Polres-Polres, rata-rata LPnya sangat rendah, antara 1-4 LP dalam satu tahun, tergantung pada tindak pidana

siber yang ditangani (Hasil FGD di Jajaran Polda Kaltim dan Polres-Polres, 22-24 Juli 2024). Dari 20 LP di Ditreskrimsus Subdit V/Siber Polda Kaltim, crime clerence (CC)-nya berjumlah sembilan (9) kasus. Dan pada tahun 2023, CC-nya sebanyak 27 kasus dari 30 LP…".

Cuplikan kutipan di atas, juga hampir terjadi di beberapa Polda lain yang menjadi objek penelitian. Umumnya, di tingkat Polda target CT masih didasarkan pada besar anggaran DIPA, sementara di tingkat Polres-Polres diklasifikasi berdasarkan kasus ringan, sedang dan berat. Secara garis besar, penanganan di tingkat Polda masih tergolong sedang, meskipun ada beberapa yang masih rendah. Proses lidik dan sidik sepertinya terjadi kesenjangan, antara di tingkat Polda dengan

yang dilakukan di tingkat Polres. Kesenjangan ini terkait dengan capaian jumlah kasus yang harus ditangani, dan juga SDM siber, dukungan anggaran dan juga pemahaman terhadap penanganan tindak pidana siber.

Upaya pembuktian tindak pidana siber Proses penyelidikan tindak pidana siber di jajaran Polda dilakukan melalui beberapa tahapan utama, yaitu: penerimaan pengaduan, pembuatan laporan, pengelolaan administrasi, serta pemeriksaan saksi, termasuk saksi ahli dan terlapor. Untuk dapat menaikkan status laporan menjadi penyidikan (sidik), penyidik diwajibkan memiliki minimal dua alat bukti awal.

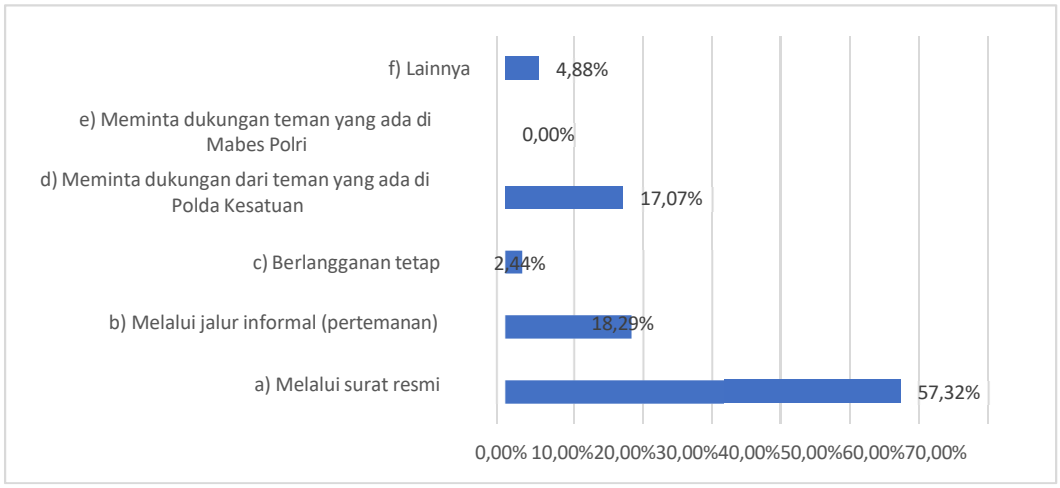
Hasil FGD menunjukkan perbedaan kesiapan antara penyidik di tingkat Polda dan Polres. Penyidik di Subdit Siber Polda umumnya telah memiliki pelatihan khusus dan beberapa sertifikasi terkait kejahatan siber, sedangkan di tingkat Polres, penyidik mayoritas hanya memiliki sertifikasi sebagai penyidik umum. Hal ini berdampak pada terbatasnya kemampuan Polres dalam menangani kasus siber yang kompleks.

Selain itu, sebagian besar penyidik masih belum menggunakan digital forensik secara optimal. Hambatan utama bukan pada pemahaman teknis penyidik, melainkan pada ketersediaan alat, laboratorium forensik digital, serta tenaga ahli analisis data. Dalam praktiknya, penyidik sangat bergantung pada bantuan Labfor Polda dan Kementerian Kominfo dalam proses pembuktian menggunakan perangkat digital (HP, kamera, laptop). Proses pengumpulan bukti awal seperti data CDR (Call Data Record) atau transaksi pos juga masih sering mengalami hambatan teknis dan birokrasi.

Efektivitas proses penyelidikan dan penyidikan Rata-rata waktu yang dibutuhkan penyidik dari tahap laporan masyarakat hingga pemberkasan dinyatakan lengkap (P21) adalah 2–4 bulan. Hal ini ditemukan secara konsisten di beberapa Polda yang menjadi sampel, seperti Polda Kepulauan Bangka Belitung, Polda Aceh, dan Polda Nusa Tenggara Barat, di mana lebih dari 80% kasus yang ditangani memerlukan waktu tersebut.

Lambannya proses ini disebabkan oleh kombinasi dari faktor teknis dan struktural, antara lain: keterbatasan tenaga ahli digital, proses koordinasi antarinstansi yang memakan waktu, serta kurangnya fasilitas teknologi informasi yang memadai di tingkat Polres. Sebagian besar perkara yang ditangani juga masih tergolong tindak pidana siber ringan seperti pencemaran nama baik, penipuan daring, perjudian online, dan konten pornografi.

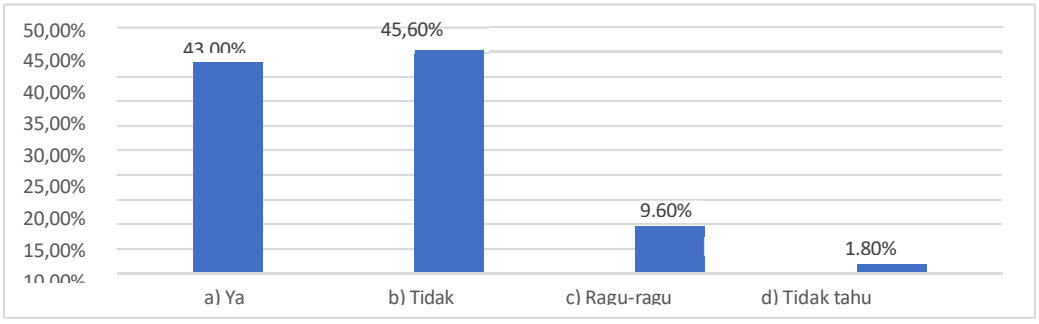
Upaya Pembuktian Tindak Pidana Siber melalui Upaya-upaya dalam pembuktian tindak pidana siber dapat dikatakan sebagai faktor kunci, sekaligus krusial dalam menyelesaikan kasus kejahatan siber yang terjadi. Pembuktian alat bukti dunia maya bukanlah hal yang mudah. Grafik di bawah menunjukkan bahwa dalam upaya pembuktian, 57,32 % data diperoleh melalui surat resmi kepada sejumlah pihak eksternal, dan 18,29 diperoleh melalui jalur pertemanan. Data ini menunjukkan tingkat ketergantungan dalam pembuktian tindak pidana siber yang bersumber dari data eksternal sangat terlihat. Data kuantitatif ini selaras dengan data kualitatif hasil FGD di 11 Polda dan Polres jajaran, di mana sebagian besar data dalam pembuktian sangat tergantung dari ekstrak data dan analisis data dari Kemenkominfo, dan sebagian diperoleh dengan meminta dukungan teman yang ada di Polda, dan sumber lainnya.



Gambar 7. Informasi dari Pihak Eksternal.
Sumber: Data yang diolah dari penyebaran kuesioner Puslitbang Polri, Juli - Agustus 2024

Penyidik tindak pidana siber di 11 Polda yang diteliti masih sangat bergantung pada sumber data eksternal, seperti data perbankan, analisis forensik dari Kemenkominfo, dan bantuan dari satuan kewilayahan lain. Kemandirian dalam memperoleh data pembuktian sangat rendah, dengan hanya sedikit yang bisa diperoleh melalui aplikasi berlangganan tetap. Dukungan dari lembaga eksternal, terutama perbankan dan OJK, juga sangat minim. Secara kuantitatif, 46,34% tidak memberikan dukungan, dan jika dilihat dari akumulasi penilaian, sekitar 78,05% tergolong tidak mendukung. Hal ini menjadikan akses terhadap informasi rekening yang penting dalam pembuktian kejahatan siber sebagai hambatan utama, di mana penyidik kerap mengalami kesulitan besar untuk mendapatkan data tersebut.

Proses penyelidikan dan penyidikan tindak pidana siber di 11 Polda masih berjalan lambat dan tidak sesuai dengan kerangka waktu cepat sebagaimana diatur dalam KUHAP. Waktu 1 x 24 jam dari penangkapan hingga penahanan dinilai tidak realistis untuk kasus siber, bahkan waktu 3 x 24 jam seperti pada kasus narkotika dan terorisme pun masih dianggap kurang. Penanganan kejahatan siber rata-rata memerlukan waktu 3 hingga 7 hari hanya untuk proses awal. Data menunjukkan 45,60% responden menilai waktu 1 x 24 jam tidak mencukupi, sementara 43% menganggap masih memungkinkan tergantung kasusnya. Sebagian besar narasumber menyarankan batas waktu 7 x 24 jam sebagai waktu yang paling rasional untuk penanganan efektif kasus tindak pidana siber.



Gambar 8. Kecukupan Jangka Waktu 1 x 24 Jam.
Sumber: Data yang diolah dari penyebaran kuesioner Puslitbang Polri, Juli - Agustus 2024

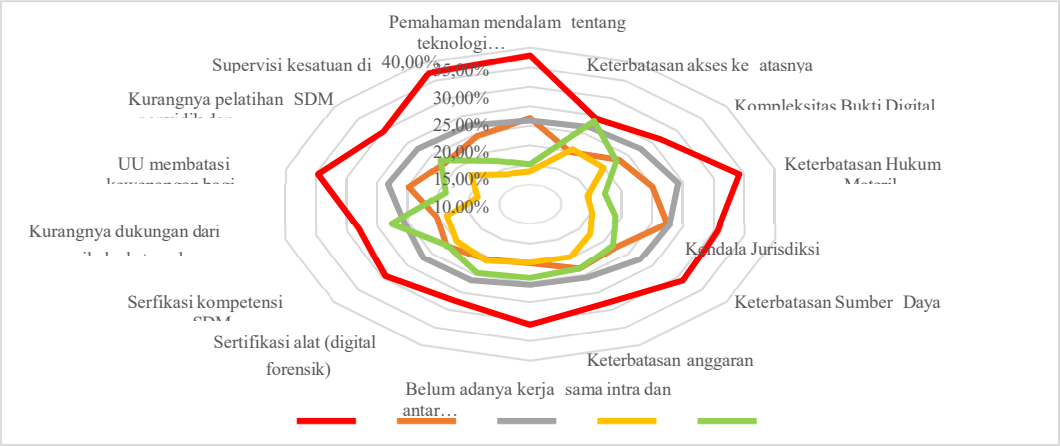
Grafik di atas menunjukan bahwa jangka waktu 1x24 jam dirasakan kurang cukup untuk menangani kasus kejahatan siber, sehingga hal ini menjadi wajar ketika penyindik menginginkan

penambahan waktu lebih dari 1x24 jam. Secara umum, hasil FGD terkait jangka waktu tersebut dirangkum dalam tabel di bawah ini.

Penanganan kasus tindak pidana siber memerlukan waktu yang relatif lama karena kesulitan dalam pengumpulan dan pembuktian awal. Hanya 27% kasus yang dapat diselesaikan dalam waktu kurang dari satu bulan, sementara mayoritas (56%) membutuhkan waktu 2–4 bulan. Sebagian lainnya bahkan memerlukan waktu 5–7 bulan (10,2%), 8–10 bulan (2,2%), dan lebih dari 10 bulan (4,6%). Hal ini menunjukkan bahwa tidak ada jaminan pengaduan masyarakat dapat segera ditindaklanjuti. Hasil FGD di 11 Polda dan Polres memperkuat temuan ini, bahwa proses Lidik dan Sidik sangat bergantung pada kompleksitas kasus, terutama dalam memenuhi dua alat bukti, seperti bukti digital forensik dan keterangan saksi ahli. Bahkan, banyak kasus yang memerlukan lebih dari empat bulan, dan sebagian tidak dapat diungkap meskipun telah berjalan lebih dari satu tahun.

Pengelolaan barang bukti dalam kasus tindak pidana siber masih menjadi tantangan karena tidak semua penyidik, baik di Polda maupun Polres, telah mendapat pelatihan khusus. Padahal, penanganan yang tepat sangat penting agar perangkat digital (seperti komputer, HP, dan media penyimpanan) tidak rusak dan tetap valid sebagai alat bukti di persidangan. Berbeda dengan tindak pidana umum, bukti dalam kejahatan siber lebih bersifat digital dan rentan rusak atau hilang. Dari 484 responden, sebanyak 48,8% mengaku pernah mendapat pelatihan pengelolaan barang bukti siber, sementara 41,2% belum pernah. Sisanya, 4% ragu-ragu dan 6% tidak tahu. Data ini menunjukkan bahwa masih ada kesenjangan signifikan dalam kapasitas penyidik untuk menangani barang bukti digital secara profesional.

Pembuktian tindak pidana siber dihadapkan pada dua jenis kendala utama, yaitu kendala internal dan eksternal. Kendala internal meliputi kurangnya alat pendukung penyelidikan, ketiadaan laboratorium forensik digital tersertifikasi di setiap Polda, serta keterbatasan pemahaman teknologi di kalangan penyidik. Dibutuhkan kebijakan nasional berupa road map yang mencakup penguatan SDM, peralatan IT, anggaran, dan struktur organisasi penyidik siber secara menyeluruh. Secara kuantitatif, kendala terbesar menurut responden adalah keterbatasan pemahaman teknologi informasi (38%), diikuti oleh lemahnya supervisi dari satuan atas (37,2%), serta masalah yurisdiksi dan kewenangan (masing-masing 30,6%). Kendala-kendala ini juga mengemuka dalam diskusi FGD, menunjukkan bahwa upaya percepatan penanganan kejahatan siber masih terhambat oleh kapasitas internal yang belum optimal.



Gambar 9. Kendala Proses Lidik – Sidik.
Sumber: Data yang diolah dari penyebaran kuesioner Puslitbang Polri, Juli - Agustus 2024

Kendala eksternal dalam pembuktian tindak pidana siber, terdapat dua kendala eksternal utama yang menghambat pembuktian tindak pidana siber. Pertama, keterbatasan saksi ahli khususnya di bidang ITE, pidana, dan bahasa yang kompetensinya harus tersertifikasi. Ketersediaan saksi ahli ITE yang umumnya berasal dari Kemenkominfo Jakarta masih sangat terbatas. Kedua,

pada kasus penipuan online, penyidik sering mengalami hambatan karena data perbankan dianggap rahasia menurut UU Perbankan dan hanya dapat diakses setelah ada tersangka. Ironisnya, penetapan tersangka sendiri memerlukan data tersebut sebagai bukti awal.

Selain itu, pembuktian melalui bukti digital juga terkendala akses terhadap platform seperti WhatsApp, Facebook, dan Telegram, yang sering kali menolak membuka data karena alasan privasi atau karena menganggap kasusnya tidak melanggar hukum. Akibatnya, penyidik kesulitan menelusuri identitas pelaku siber.

Kendala yang Paling Mendesak Ditangani Berdasarkan analisis metode AHP dan FGD di 11 Polda, terdapat empat kendala paling urgen yang harus segera diatasi yaitu:

1. Kurangnya dukungan sarana IT untuk proses Lidik dan Sidik menjadi kendala paling dominan di hampir semua Polda.
2. Ketiadaan laboratorium digital forensik, menyebabkan proses pembuktian memakan waktu lama.
3. Ketentuan KUHAP yang belum akomodatif, terutama terkait penyitaan bukti digital dan batas waktu penahanan 1×24 jam, yang dirasa tidak realistis untuk kasus siber.
4. Keterbatasan anggaran, terutama di wilayah seperti Polda Kalimantan Selatan dan Maluku, karena sifat kejahatan siber yang lintas wilayah (borderless), sehingga membutuhkan biaya besar untuk penanganan kasus lintas provinsi.

Polda Aceh menekankan urgensi revisi UU dan KUHAP, sedangkan beberapa Polda lain lebih fokus pada peningkatan alat IT dan dukungan teknis. Perbedaan ini menunjukkan bahwa setiap wilayah memiliki tantangan tersendiri, meskipun secara umum seluruh Polda menghadapi persoalan yang serupa dalam hal pembuktian dan penyidikan kejahatan siber.

Kendala eksternal pembuktian tindak pidana siber terdapat dua kendala eksternal utama:

1. Keterbatasan saksi ahli bersertifikasi, terutama di bidang ITE, pidana, dan bahasa—jumlahnya terbatas dan mayoritas hanya tersedia di Kemenkominfo Jakarta.
2. Akses data perbankan terhambat oleh UU Perbankan yang mengatur kerahasiaan identitas nasabah, yang hanya bisa dibuka setelah ada tersangka, padahal data tersebut dibutuhkan untuk menetapkan tersangka.

   Selain itu, penyidik kesulitan mengakses data dari platform digital seperti *WhatsApp, Facebook*, dan Telegram karena alasan privasi, yang memperlambat penelusuran pelaku siber.

Kendala Paling Mendesak dari Hasil FGD dan analisis AHP terhadap 11 Polda menunjukkan empat kendala utama yang perlu segera ditangani:

1. Minimnya sarana IT untuk mendukung proses Lidik dan Sidik.
2. Tidak tersedianya laboratorium digital forensik yang memadai di daerah.
3. Keterbatasan regulasi, terutama dalam KUHAP yang belum mengatur secara jelas penyitaan bukti digital dan batas penahanan 1×24 jam.
4. Keterbatasan anggaran, terutama di daerah dengan pelaku lintas wilayah (borderless).

Polda Aceh memprioritaskan revisi regulasi, sementara Polda lainnya lebih menekankan pada dukungan teknis dan peralatan. Ini menunjukkan tantangan bersifat lokal namun memiliki pola umum yang serupa di seluruh wilayah.

Prioritas strategi yang perlu dilakukan dari hasil kajian ini menunjukkan bahwa prioritas strategi dari berbagai strategi yang diharapkan sebagaimana telah disinggung di atas prioritas pertama adalah perubahan UU Perbankan (0,23) dan perlunya SOP Polri dalam penanggulangan (Lidik/Sidik) tindak pidana siber (0,19) sebagai priortias kedua. Ini tercermin dari hasil AHP dari para penyidik yang berjumlah 484 personel di Subdit V/Siber di Polda dan Polres jajaran.

SIMPULAN

Dinamika penanganan tindak pidana siber oleh Polri di tingkat satuan kewilayahan antara lain Terdapat kesenjangan kemampuan antara penyidik di tingkat Polda dan Polres. Beberapa Polda sudah memiliki kemampuan yang relatif memadai dalam melakukan proses penyelidikan dan penyidikan tindak pidana siber.Sebagian penyidik di tingkat Polda memiliki kemampuan yang "sedang" karena minimnya sertifikat internasional dan alat pendukung. Adapun kendala utama yang dihadapi dalam proses penyidikan tindak pidana siber antara lain:

1. Keterbatasan SDM yang terlatih
2. Kurangnya sarana digital forensik
3. Dukungan regulasi yang masih kurang
4. Anggaran yang terbatas
5. Kesulitan dalam pengumpulan data awal dan data bukti digital forensik
6. Platform penyedia ISP tidak ada perwakilannya di Indonesia dan tidak merespon surat

Peran regulasi dan struktur organisasi dalam menunjang efektivitas penanggulangan kejahatan siber yaitu:

1. Regulasi yang ada masih membatasi ruang gerak penyidik dalam menangani kasus siber.
2. Diperlukan reformasi struktural dan substantif, termasuk peningkatan status Subdit Siber menjadi Direktorat Siber di Polda.
3. Diperlukan penyusunan regulasi baru yang adaptif terhadap karakteristik kejahatan siber. Tindak pidana siber telah menjadi fenomena kejahatan yang umum dan berkembang pesat di berbagai wilayah, dengan pola dan modus yang relatif seragam serta memanfaatkan jaringan internet dan perangkat digital.

Kejahatan ini bersifat anonim, menggunakan identitas palsu, dan memanfaatkan kelemahan sistem perbankan serta platform digital untuk menghindari pelacakan. Proses penyelidikan dan penyidikan masih menghadapi tantangan serius, khususnya pada tingkat Polres, seperti keterbatasan SDM yang terlatih, sarana digital forensik, dukungan regulasi, serta anggaran. Secara garis besar, proses penyelidikan dan/atau penyidikan tindak pidana siber di 11 Polda yang menjadi objek penelitian dapat digambarkan pada 3 (tiga) kondisi, yaitu:

1. beberapa Polda sudah memiliki kemampuan yang relatif memadai dalam melakukan proses penyelidikan dan/atau penyidikan tindak pidana siber. Hal ini dapat dilihat dari sejumlah kasus tindak pidana siber yang sudah menjadi LP dan dapat diselesaikan hingga P21 untuk dilanjutkan dalam proses peradilan, dengan dukungan peralatan yang masih kurang (seadanya). Harus diakui sebagian besar masih didominasi oleh kasus-kasus kejahatan tindak pidana siber yang ringan dan sedang, seperti pencemaran nama baik, pornografi, penipuan-pemerasan *online,* dan perjudian *online.*
2. sebagian penyidik di tingkat Polda bisa dianggap memiliki kemampuan yang “sedang”, akibat beberapa hal, seperti minimnya sertifikat internasional terkait tindak pidana siber, kurangnya alat pendukung seperti DF, cellebrite dan laboratorium forensik siber. Kalaupun ada sarana pendukung IT terkait fungsi siber, rata-rata masih kurang memadai, dan sebagian kurang terpelihara (maintenance software, lisensi dan lainnya tidak ter- update). Akibatnya, kekurangan SDM, anggaran dan peralatan menyebabkan target (CT/CC) yang ditargetkan juga lebih rendah.
3. beberapa penyidik “belum” mampu untuk menangani tindak pidana siber, akibat kurangnya pemahaman akan pentingnya bukti digital (digital forensik) dalam penanganan tindak pidana siber. Kondisi ini umumnya terjadi di tingkat Polres-Polres, kecuali Polres di Aceh yang menggunakan Qanun (perda syariah) dalam kasus perjudian online, dan jinayat yang lain, karena ada keharusan menggunakan Perda Syariah. Tingkat kesulitan para penyidik lebih

pada pengumpulan data awal dan data bukti khususnya digital forensik, karena pada beberapa kasus tindak pidana siber bersifat anonim, akun palsu, rekening palsu, dan umumnya para penyidik juga kesulitan dalam melakukan *profiling WhatsApp* yang sering digunakan karena WhatsApp aktif, dan nomor teleponnya mati, sehingga ketika dilakukan cek pos atau profiling tidak bisa dideteksi. Apalagi beberapa platform penyedia ISP tidak ada perwakilannya di Indonesia dan ketika dikirimi surat tidak merespon.

Kesenjangan kemampuan antara penyidik di tingkat Polda dan Polres cukup signifikan, kondisi ini juga dipengaruhi oleh belum optimalnya dukungan eksternal dari perbankan, ISP, dan lembaga peradilan. Di sisi lain, regulasi yang ada, seperti UU ITE, UU Perbankan, dan KUHAP, masih membatasi ruang gerak penyidik dalam menangani kasus siber, terutama dalam tahap awal penyelidikan. Prosedur hukum konvensional dianggap belum sesuai dengan kebutuhan penanganan kejahatan siber yang bersifat kompleks, lintas batas, dan berbasis bukti digital.

Untuk mengatasi berbagai tantangan tersebut, diperlukan reformasi struktural dan substantif, termasuk peningkatan status Subdit Siber menjadi Direktorat Siber di Polda, penguatan kapasitas SDM melalui pelatihan dan sertifikasi, serta penyusunan regulasi baru yang adaptif terhadap karakteristik kejahatan siber. Kolaborasi lintas sektor serta roadmap pengembangan SDM dan sarana prasarana juga menjadi hal mendesak guna mendukung efektivitas penegakan hukum terhadap tindak pidana siber.

DAFTAR PUSTAKA

Badri, A. (2021). Efektivitas Kebijakan Pembatasan Sosial Berskala Besar (PSBB) di Indonesia Ditinjau dari Perspektif Hukum. Jurnal Analisis Hukum, 1-6.

Boonying, Varinthorn.(2007). U*sing proactive evaluation to develop a policy for public sector training programs in emotional intelligence in Thailand*. Victoria University.

Cheng, L.Y. (2008) *Development And Initial Validation Of An Instrument Measuring Training Design Competences Of Human Resource Development Professionals In Taiwan. Feng Chia University*.

Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches. Los Angles: Sage.

Gilley, J., and Eggland, S. A. (2002). *Principles Of Human Resource Development. Addison Wesley publishing Company.*

https://nasional.kompas.com/read/2015/12/19/19450071/Polisi Cyber Crime RI Cuma 18 Personel Polisi China Geleng-geleng Kepala.

https://www.antaranews.com/berita/3613461/polri presisi mengabdi di tengah tantangan police 4.0 dan society 5.0

https://www.kominfo.go.id/content/detail/49482/memenuhi layanan digital hingga pelosok Data APJII menyebutkan pengguna internet, sebanyak 320 juta pengguna.

Kautsar, I. A., & Muhammad, D. W. (2022). Sistem Hukum Modern Lawrance

M. Friedman: Budaya Hukum dan Perubahan Sosial Masyarakat dari Industrial ke Digital. Sapientia Et Virtus, 84-99.

Muslih, M. (2013). Negara Hukum Indonesia Dalam Perspektif Teori Hukum Gustav Radbruch. Legalitas, 130-152.

Neumann, W. Lawrence (2014), *Social Research Method: Qualitative and Quantitative Approach, Seventh Edition, Pearson Education, Inc.*

Nicodemus, A. A. (2023). Tantangan dalam Penegakan Hukum Pidana terhadap Kejahatan Siber di Era Digital. Jakarta: Sekolah Tinggi Ilmu Hukum IBLAM.

Peraturan Kepolisian Nomor 14 Tahun 2018 tentang Susunan Organisasi dan Tata Kerja Pada Tingkat Kepolisian Daerah

Peraturan Kepolisian Nomor 2 Tahun 2021 tentang Susunan Organisasi dan Tata Kerja Pada Tingkat Kepolisian Resor dan Kepolisian Sektor

Peraturan Kepolisian Nomor 6 Tahun 2022 Perubahan atas Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 6 Tahun 2017 tentang SOTK Mabes Polri

Peraturan Menteri Kominfo Nomor 21 Tahun 2016 Tentang Keamanan Siber

Peraturan Pemerintah Nomor 58 Tahun 2010 Perubahan atas Peraturan Presiden Nomor 27 Tahun 1983 tentang Pelaksanaan Kitab Undang- Undang Hukum Acara Pidana

Prianto, Y., Fuzain, N. A., & Farhan, A. (2021). Kendala Penegakan Hukum Terhadap Cyber Crime Pada Masa Pandemi Covid-19. Pengembangan Ekonomi Bangsa Melalui Inovasi Digital . Bandung: Universitas Taruma Negara.

Rafif, M., & Zakki, A. (2023). Tinjauan Penerapan E-Court Di Pengadilan Negeri Yogyakarta Berdasarkan Teori Hukum Lawrence M. Friedman. Verstek, 685-695.

Saaty, T. L. (1993). *Decision Making for Leader : The Analytical Hierarchy Process for Decisions in Complex World. Pittburgh: University of Pittsburgh.*

Saputra, A., Kristiawanto, & Ismed, M. (2024). Rekonstruksi Penegakan Hukum Tindak Pidana Siber di Indonesia. SEIKAT: JURNAL ILMU SOSIAL, POLITIK DAN HUKUM., 63-70.

Saragih, Y. M., & Azis, D. A. (2020). Perlindungan Data Elektronik Dalam Formulasi Kebijakan Kriminal Di Era Globalisasi. Soumatera Law Review, 265-279.

Thamrin, C. (2008). Pemetaan Kebutuhan Pendidikan dan Pelatihan Pada Badan Pengembangan Sumber Daya Manusia (BPSDM) Kementerian Hukum dan Hak Asasi Manusia. FISIP Universitas Indonesia.

Undang Undang Nomor 1 Tahun 2024 tentang Perubahan Atas Undang- Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik

Undang Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik

Undang-Undang Nomor 19 Tahun 2011 tentang Perubahan atas Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Werner, Jon M., and Randy L. DeSimone. (2012). *Human Resource Development 6th Edition.South Western Cengage Learning Mason*.