Rewang Rencang : Jurnal Hukum Lex Generalis. Vol. 5. No.7 (2024)
Tema/Edisi : Hukum Pidana (Bulan Ketujuh)
https://jhlg.rewangrencang.com/

KENDALA TEKNIS DAN HUKUM DALAM PROSES PENYIDIKAN TINDAK PIDANA SIBER DI INDONESIA

TECHNICAL AND LEGAL OBSTACLES IN THE INVESTIGATION PROCESS OF CYBER CRIMES IN INDONESIA

Muhammad Singgih Imam Wibowo, Akhmad Munawar dan Hidayatullah
Universitas Islam Kalimantan Muhammad Arsyad Al-Banjari Banjarmasin
Korespondensi: sisimbobo@gmail.com

Citation Structure Recommendation :
Wibowo, Muhammad Singgih Imam, Akhmad Munawar dan Hidayatullah. *Kendala Teknis dan Hukum dalam Proses Penyidikan Tindak Pidana Siber di Indonesia*. Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.5. No.7 (2024).

ABSTRAK

Penelitian ini bertujuan untuk menganalisis kendala teknis dan hukum yang dihadapi dalam proses penyidikan tindak pidana siber di Indonesia. Seiring dengan pesatnya perkembangan teknologi informasi, kejahatan siber menjadi salah satu tantangan terbesar dalam sistem peradilan pidana di Indonesia. Penelitian ini mengidentifikasi berbagai hambatan teknis, seperti keterbatasan alat forensik digital dan kesulitan dalam pengumpulan bukti yang terdistribusi di berbagai platform. Selain itu, aspek hukum, termasuk ketidaksesuaian antara regulasi nasional dan standar internasional, serta tantangan dalam kerjasama lintas yurisdiksi, turut mempengaruhi efektivitas penyidikan. Berdasarkan hasil analisis, penelitian ini menyarankan beberapa langkah strategis, termasuk pembaruan regulasi, peningkatan kapasitas sumber daya manusia, dan penguatan koordinasi antar lembaga penegak hukum baik di tingkat nasional maupun internasional. Penelitian ini diharapkan dapat memberikan kontribusi untuk memperbaiki sistem penyidikan tindak pidana siber di Indonesia dan mendukung upaya pemberantasan kejahatan siber secara lebih efektif.

Kata Kunci: Perbedaan Makna, Restorative Justice, Perma No.1 Tahun 2024, Sistem Hukum Pidana di Indonesia

ABSTRACT

This research aims to analyze the technical and legal obstacles faced in the process of investigating cybercrimes in Indonesia. Along with the rapid development of information technology, cybercrime has become one of the biggest challenges in the criminal justice system in Indonesia. This research identified various technical barriers, such as limitations of digital forensic tools and difficulties in collecting distributed evidence across multiple platforms. In addition, legal aspects, including inconsistencies between national regulations and international standards, as well as challenges in cross-jurisdictional cooperation, also influence the effectiveness of investigations. Based on the results of the analysis, this research suggests several strategic steps, including updating regulations, increasing human resource capacity, and strengthening coordination between law enforcement agencies at both the national and international levels. It is hoped that this research can contribute to improving the cybercrime investigation system in Indonesia and support efforts to eradicate cybercrime more effectively.

Keywords: Law; Obstacles; Investigation; Cyber; Crime

A. PENDAHULUAN

Tindak pidana siber telah menjadi salah satu bentuk kejahatan yang paling kompleks dan dinamis di Indonesia, terutama di era digital saat ini. Secara filosofis, tindak pidana siber menguji prinsip keadilan substantif dalam hukum, menuntut sistem hukum untuk melindungi hak individu sambil memastikan stabilitas masyarakat dalam tatanan digital yang terus berkembang. Kejahatan ini juga menimbulkan pertanyaan mendasar tentang penerapan nilai keadilan dalam konteks teknologi modern, termasuk perlunya memastikan transparansi dan akuntabilitas dalam proses hukum, terutama ketika bukti digital sering kali sulit diverifikasi. Dalam hal ini, hukum harus mampu beradaptasi tanpa kehilangan prinsip dasarnya, sehingga tidak hanya menghukum pelaku tetapi juga melindungi korban dan meminimalkan dampak sosial yang ditimbulkan.[1]

Dari sisi sosial, tindak pidana siber berdampak luas, tidak hanya pada individu tetapi juga pada sektor ekonomi, keamanan nasional, dan stabilitas sosial. Kejahatan seperti penipuan daring, pencurian data, dan peretasan sistem merugikan masyarakat, terutama kelompok rentan seperti pengguna internet pemula atau individu dengan literasi digital rendah. Selain itu, serangan terhadap infrastruktur strategis negara semakin memperbesar risiko yang dihadapi Indonesia di era digital. Peningkatan literasi digital menjadi langkah penting untuk mencegah kejahatan siber, diikuti oleh kolaborasi antara pemerintah, sektor swasta, dan masyarakat untuk membangun ekosistem digital yang aman. Sinergi ini juga mendukung penguatan kesadaran kolektif dalam menghadapi ancaman siber yang terus berkembang.

Dari perspektif yuridis, meskipun Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) telah memberikan dasar hukum untuk menangani kejahatan siber, regulasi ini dianggap belum cukup memadai untuk mengatasi kompleksitas kejahatan modern, seperti *ransomware*, *deepfake*, kejahatan yang melibatkan teknologi *blockchain* & kecerdasan buatan.[2]

---

[1] Adami Chazawi, *Tindak Pidana Informasi & Transaksi Elektronik*, Bayumedia Publishing, Malang, 2011, p.1.

[2] Ramadhani Fariza, *Dinamika UU ITE Sebagai Hukum Positif di Indonesia Guna Meminimalisir Kejahatan Siber*, Kultura: Jurnal Ilmu Hukum, Sosial, dan Humaniora, Vol.1, No.1 (September 2023), p.92.

Proses pembuktian di pengadilan juga menjadi tantangan besar karena karakteristik bukti digital yang berbeda dari bukti konvensional, membutuhkan mekanisme validasi khusus. Selain itu, sifat lintas batas dari kejahatan siber memperumit penyidikan, terutama ketika pelaku berada di negara tanpa perjanjian ekstradisi atau mekanisme kerjasama internasional. Di tingkat nasional, koordinasi antar lembaga sering kali terhambat oleh tumpang tindih kewenangan, sehingga memperlambat efektivitas penyelesaian kasus.

Penelitian ini memiliki urgensi tinggi mengingat peningkatan signifikan dalam jumlah tindak pidana siber di Indonesia setiap tahunnya.[3] Tanpa langkah serius untuk mengatasi kendala teknis, seperti kurangnya sumber daya manusia di bidang forensik digital dan keterbatasan teknologi, serta hambatan hukum yang mencakup kebutuhan reformasi regulasi, kejahatan siber dapat berkembang menjadi ancaman sistemik yang sulit dikendalikan. Indonesia juga membutuhkan kerangka hukum dan mekanisme penyidikan yang selaras dengan standar internasional, seperti *Budapest Convention on Cybercrime*, untuk mencegah negara ini menjadi titik lemah dalam jaringan keamanan global. Adapun penelitian dalam tulisan ini bertujuan untuk memberikan rekomendasi secara praktis dan implementatif guna meningkatkan efektivitas proses penyidikan, mendukung regulasi yang lebih adaptif, dan memperkuat kapasitas aparat penegak hukum agar mampu melindungi masyarakat sekaligus mengikuti perkembangan teknologi di era digital.

Berdasarkan paparan di atas, terlihat jelas bahwa tindak pidana siber menghadirkan berbagai tantangan, baik secara teknis maupun hukum, yang memengaruhi efektivitas proses penyidikan di Indonesia. Oleh karena itu penelitian ini akan berfokus pada masalah tentang Bagaimana kendala teknis dan Hukum dalam proses penyidikan tindak pidana siber di Indonesia?

[3] Alifya Putri Azahra, dkk., *Analisa kepada Para Oknum yang Tidak Bijak dalam Menggunakan Media Sosial atau Cyberspace*, Civilia: Jurnal Kajian Hukum dan Pendidikan Kewarganegaraan, Vol.3, No.1 (Januari 2024), p.43.

B. PEMBAHASAN

Penyidikan tindak pidana siber di Indonesia menghadapi beragam tantangan yang bersifat teknis maupun hukum. Kejahatan siber yang berkembang pesat memerlukan pendekatan yang tidak hanya adaptif terhadap kemajuan teknologi, tetapi juga memperhatikan aspek legalitas yang sesuai dengan regulasi yang ada. Dalam bab ini, akan dibahas secara mendalam mengenai kendala teknis yang dihadapi oleh penyidik, peraturan hukum yang mendukung atau membatasi efektivitas penyidikan, koordinasi antar lembaga penegak hukum, serta tantangan lintas yurisdiksi yang memengaruhi proses penyidikan tindak pidana siber di Indonesia. Melalui analisis yang mendalam, diharapkan dapat ditemukan solusi strategis yang dapat meningkatkan efektivitas sistem penyidikan tindak pidana siber di Indonesia, serta memperkuat koordinasi nasional dan internasional dalam pemberantasan kejahatan siber.

1. Kendala Teknis dalam Proses Penyidikan Tindak Pidana Siber

Penyidikan tindak pidana siber di Indonesia menghadapi berbagai kendala teknis yang menghambat efektivitas proses penegakan hukum. Kendala teknis tersebut antara lain:

a. Keterbatasan sumber daya manusia.
b. Keterbatasan peralatan teknis dan infrastruktur.
c. Kompleksitas bukti digital.
d. Keterbatasan kerjasama internasional.

Salah satu kendala utama adalah keterbatasan sumber daya manusia (SDM) yang memiliki keahlian khusus di bidang forensik digital. Penyidik sering kali tidak dibekali dengan pengetahuan atau pelatihan yang cukup untuk menangani bukti digital, seperti analisis log aktivitas, pelacakan alamat IP, atau penguraian data terenkripsi. Dalam banyak kasus, penegak hukum membutuhkan keahlian tingkat lanjut untuk membongkar sistem kompleks yang digunakan oleh pelaku, seperti penggunaan jaringan anonim (dark web) atau transaksi *cryptocurrency* yang sulit dilacak. Selain keterbatasan SDM, peralatan teknis dan infrastruktur pendukung penyidikan juga sering kali tidak memadai. Alat analisis forensik digital yang mutakhir, seperti perangkat lunak pelacak data atau alat pemulihan data yang terhapus, masih langka atau tidak tersedia di banyak wilayah.

Hal ini membuat proses penyelidikan menjadi lambat dan kurang akurat, terutama ketika bukti digital memerlukan penanganan segera untuk mencegah kehilangan data akibat manipulasi atau batas waktu penyimpanan. Kendala teknis lainnya adalah kompleksitas bukti digital yang sering kali tersebar di berbagai platform global. Penyidik harus berhadapan dengan sistem keamanan tinggi yang diterapkan oleh layanan cloud atau platform media sosial, yang sering kali berbasis di luar negeri. Situasi ini menuntut kerjasama internasional, yang tidak selalu mudah diperoleh, terutama jika platform itu ada di negara tanpa perjanjian kerjasama hukum dengan Indonesia. Selain itu, bukti digital bersifat mudah dimanipulasi atau dihapus, sehingga memerlukan tindakan cepat dan akurat, yang sering kali menjadi tantangan teknis tersendiri bagi aparat penegak hukum.

Menurut teori penyidikan pidana, keberhasilan penyidikan sangat bergantung pada tiga elemen utama: kapasitas penyidik, ketersediaan alat dan teknologi, serta kerangka kerja hukum dan prosedural yang mendukung[4]a. Dalam konteks tindak pidana siber, kapasitas penyidik menjadi aspek yang paling krusial karena sifat kejahatan ini membutuhkan keterampilan teknis khusus. Berdasarkan hal ini, penyidikan yang efektif juga mensyaratkan integrasi teknologi sebagai alat bantu untuk mengumpulkan, memproses, dan menganalisis bukti. Namun, dalam praktiknya, keterbatasan infrastruktur dan teknologi menjadi penghambat utama, sehingga teori ini belum sepenuhnya diterapkan di Indonesia.

Kerangka penyidikan pidana juga menekankan pentingnya kerjasama lintas batas dalam kejahatan yang bersifat global. Hal ini terkait doktrin "*universal jurisdiction*," yang menyatakan negara-negara perlu bekerja sama untuk menindak kejahatan lintas yurisdiksi. Namun, kendala teknis seperti perlambatan akses ke data dari server internasional menunjukkan adanya kesenjangan antara teori dan praktik di Indonesia. Untuk mengatasi kendala teknis itu, teori penyidikan pidana menyarankan perlunya peningkatan kapasitas SDM melalui pelatihan khusus, pengadaan alat forensik yang mutakhir, dan pembentukan kerjasama internasional yang lebih erat. Dengan demikian, penyidikan tindak pidana siber dapat berjalan lebih efektif, selaras dengan dinamika teknologi yang terus berkembang.

[4] Febiana R. dan Agussalim Burhanuddin, *Implementasi Kebijakan Sekuritisasi Maritim Presiden Jokowi dalam Menghadapi Aktivitas Ilegal di Perairan Indonesia*, Jurnal Studi Diplomasi dan Keamanan, Vol.16, No.1 (Januari 2024), p.45.

2. Kendala Hukum dalam Proses Penyidikan Tindak Pidana Siber

Tindak pidana siber merupakan salah satu bentuk kejahatan yang paling kompleks dan menantang dalam sistem hukum modern, terutama karena sifatnya yang lintas batas dan berbasis teknologi. Di Indonesia, penyidikan tindak pidana siber menghadapi berbagai kendala hukum yang menghambat efektivitas penegakan hukum. Kendala tersebut antara lain:

a. Keterbatasan Regulasi Terhadap Efektivitas Penyidikan Tindak Pidana Siber

Peraturan hukum yang berlaku di Indonesia, terutama Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), beserta perubahannya melalui UU Nomor 19 Tahun 2016, memberikan kerangka legal dalam menangani tindak pidana siber[5]. UU ITE mendukung penyidikan melalui pengaturan mengenai jenis-jenis tindak pidana siber, seperti pencemaran nama baik, akses ilegal, manipulasi data, hingga penipuan berbasis elektronik. UU ini juga memberikan dasar hukum bagi penyidik untuk melakukan tindakan-tindakan seperti pemblokiran akses, penyitaan perangkat digital, dan permintaan data elektronik dari penyedia layanan. Selain itu, UU ITE juga diintegrasikan dengan Kitab Undang-Undang Hukum Acara Pidana (KUHAP), yang menjadi pedoman umum dalam penyidikan[6]. Namun, di balik kontribusi positifnya, UU ITE juga menghadapi sejumlah keterbatasan yang membatasi efektivitas penyidikan tindak pidana siber. Salah satu batasan utama adalah kurangnya detail dalam mengatur prosedur teknis penanganan bukti elektronik.

Misalnya, regulasi ini tidak secara spesifik mengatur standar pengumpulan, penyimpanan, dan analisis bukti digital, yang dapat menyebabkan bukti menjadi tidak sah atau sulit digunakan di pengadilan. Selain itu, UU ITE sering kali dianggap belum cukup adaptif terhadap perkembangan teknologi, seperti penggunaan kecerdasan buatan atau teknologi blockchain dalam kejahatan siber, sehingga penyidik sering kali harus berinovasi di luar kerangka hukum yang ada.

---

[5] Rizka Alifia Zahra, dkk., *Catfishing dan Implikasinya terhadap Romance Scam oleh Simon Leviev dalam Dokumenter Netflix 'Tinder Swindler' Menurut Perspektif Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Kitab Undang-Undang Hukum Pidana*, Padjadjaran Law Review, Vol.10, No.1 (Juli 2022), p.15.

[6] Cokorda Istri Ratih Utami Dewi, dkk., *Peran Kejaksaan dalam Tahap Penuntutan Terhadap Anak yang Melakukan Tindak Pidana Pornografi*, Jurnal Analogi Hukum, Vol.1, No.3 (Juni 2020), p.282.

Kendala lain adalah kerumitan dalam memperoleh data dari platform teknologi global. Meskipun UU ITE mengamanatkan kerja sama dengan penyedia layanan, realisasi di lapangan sering kali terkendala oleh perbedaan yurisdiksi hukum internasional. Sebagai contoh, penyedia platform global yang berbasis di luar negeri tidak selalu mematuhi permintaan data dari aparat penegak hukum Indonesia, terutama jika tidak ada perjanjian bilateral atau multilateral yang relevan. Hal ini memperlambat proses penyidikan dan mengurangi peluang untuk mengungkap pelaku kejahatan.

Kerangka teori penyidikan pidana menekankan pentingnya regulasi hukum yang jelas, adaptif, dan implementatif untuk mendukung proses penyidikan. Dalam konteks ini, UU ITE dikategorikan sebagai regulasi yang memberikan fondasi dasar, namun memerlukan pengembangan untuk mengikuti dinamika kejahatan siber yang terus berkembang. Menurut teori penyidikan, hukum pidana yang efektif harus mencakup aturan substansial (materi tindak pidana) dan aturan prosedural (cara penanganan perkara).[7] Dalam kasus UU ITE, meskipun aturan substansial sudah memadai, aturan prosedural masih kurang mendalam, khususnya dalam pengelolaan bukti digital. Hal ini kemudian menyatakan bahwa penyidikan tindak pidana lintas batas membutuhkan kolaborasi internasional yang kuat. Dalam hal ini, UU ITE belum sepenuhnya memfasilitasi kerja sama global yang efektif, karena ketergantungannya pada mekanisme tradisional seperti Mutual Legal Assistance (MLA), yang cenderung lamban. Sebagai perbandingan, beberapa negara maju telah mengadopsi perjanjian internasional, seperti *Budapest Convention on Cybercrime*, yang dapat mempercepat proses investigasi[8]. Untuk memperkuat efektivitas UU ITE, reformasi hukum yang mengadopsi standar internasional dan pengaturan prosedural yang lebih teknis diperlukan. Dengan demikian, kerangka hukum Indonesia dapat menjadi lebih responsif terhadap tantangan kejahatan siber modern dan mendukung aparat penegak hukum dalam menjalankan tugasnya secara efisien.

---

[7] Eko Nurisman, *Risalah Tantangan Penegakan Hukum Tindak Pidana Kekerasan Seksual Pasca Lahirnya Undang-Undang Nomor 12 Tahun 2022*, Jurnal Pembangunan Hukum Indonesia, Vol.4, No.2 (Mei 2022), p.173.

[8] Chat Le Nguyen dan Golman Wilfred, *Diffusion of the Budapest Convention on Cybercrime and the Development of Cybercrime Legislation in Pacific Island Countries*: *'Law on the Books' vs 'Law in action'*, Computer Law & Security Review, Elsevier, Vol.40 (April 2021), p.105523.

b. Tumpang Tindih Kewenangan Antar Lembaga dalam Penyidikan Tindak Pidana Siber

Penyidikan tindak pidana siber di Indonesia melibatkan berbagai lembaga penegak hukum yang memiliki peran dan kewenangan berbeda. Proses koordinasi antar lembaga seperti Kepolisian Republik Indonesia (Polri), Kementerian Komunikasi dan Informatika (Kominfo), dan Badan Siber dan Sandi Negara (BSSN) sangat penting dalam menghadapi kejahatan siber yang kompleks. Polri bertindak sebagai ujung tombak dalam penyidikan melalui unit khusus, seperti Direktorat Tindak Pidana Siber (Dittipidsiber). Kominfo berperan dalam memblokir akses terhadap konten ilegal serta memfasilitasi komunikasi dengan penyedia layanan digital. Sementara itu, BSSN memberikan dukungan teknis melalui keamanan infrastruktur siber dan analisis data digital. Meskipun telah ada kerjasama antarlembaga, koordinasi ini masih menghadapi sejumlah tantangan. Salah satunya adalah tumpang tindih kewenangan yang sering kali menyebabkan inefisiensi dalam penyelidikan.

Sebagai contoh, dalam kasus tertentu, proses pelaporan dan tindak lanjutnya memerlukan konfirmasi dari beberapa lembaga, sehingga memperlambat tindakan yang seharusnya bersifat segera. Selain itu, kurangnya sistem pertukaran informasi yang terintegrasi juga menjadi hambatan. Data yang relevan dengan penyidikan sering kali tersebar di berbagai instansi, tanpa ada mekanisme berbagi informasi yang efektif. Tantangan lainnya adalah kurangnya protokol operasional standar yang mengatur bagaimana lembaga-lembaga ini bekerja sama secara optimal. Dalam banyak kasus, ketiadaan koordinasi yang kuat menyebabkan keterlambatan atau ketidaktepatan langkah penanganan kejahatan siber. Di sisi lain, perbedaan prioritas dan alokasi sumber daya di antara lembaga penegak hukum juga memengaruhi efektivitas proses penyidikan.

Berdasarkan teori penyidikan pidana, kerja sama antarlembaga merupakan elemen kunci dalam menangani kejahatan yang kompleks, termasuk tindak pidana siber. Teori ini menekankan pentingnya sinergi antar institusi melalui pembagian peran yang jelas, pertukaran informasi yang efisien, dan koordinasi strategis yang didukung oleh regulasi dan teknologi. Dalam kasus di Indonesia, meskipun lembaga seperti Polri, Kominfo serta BSSN memiliki mandat yang relevan,

belum ada kerangka kerja koordinasi yang sepenuhnya terintegrasi dan memadai. Hal ini juga menggarisbawahi pentingnya protokol operasional yang baku untuk mengatasi potensi konflik atau tumpang tindih kewenangan. Dalam konteks ini, Indonesia memerlukan aturan yang lebih spesifik terkait pembagian tugas, jalur komunikasi, dan prosedur tanggap darurat dalam kasus siber.

Sebagai contoh, protokol pertukaran data yang aman dan efisien di antara lembaga penegak hukum dapat mempercepat proses penyidikan dan meningkatkan akurasi hasil. Selain itu, teori penyidikan modern menggarisbawahi pentingnya platform teknologi terpadu untuk mendukung kerja sama lintas lembaga. Di negara-negara maju, sistem seperti cyber incident response platforms telah berhasil digunakan untuk mengoordinasikan tindakan berbagai institusi dalam menangani kejahatan siber.[9] Di Indonesia, pengembangan sistem serupa dapat menjadi solusi untuk memperbaiki koordinasi yang saat ini masih sporadis. Melalui teori-teori ini, koordinasi antar lembaga di Indonesia dapat ditingkatkan, sehingga penyidikan tindak pidana siber menjadi lebih efektif dan responsif terhadap perkembangan teknologi dan modus operandi pelaku kejahatan.

c. Perbedaan Yurisdiksi Hukum Antar Negara

Tindak pidana siber sering kali melibatkan pelaku, korban, dan infrastruktur yang berada di berbagai negara, menciptakan tantangan lintas yurisdiksi yang signifikan bagi penyidik di Indonesia. Salah satu tantangan utama adalah perbedaan regulasi hukum antara negara. Misalnya, tindakan yang dianggap sebagai tindak pidana di Indonesia, seperti akses ilegal ke data, mungkin tidak diatur atau bahkan dianggap legal di negara lain. Akibatnya, penyidik menghadapi kesulitan dalam memperoleh kerja sama dari otoritas asing, baik dalam bentuk penyerahan data maupun ekstradisi pelaku. Ketiadaan perjanjian kerja sama internasional yang memadai juga menjadi hambatan besar. Indonesia sendiri telah menjalin sejumlah perjanjian bilateral dan terlibat dalam mekanisme seperti MLA, namun prosesnya sering kali lambat dan tidak efisien.[10]

---

[9]Daniel Schlette, dkk., *A Comparative Study on Cyber Threat Intelligence: The Security Incident Response Perspective*, IEEE Communications Surveys & Tutorials, IEEE, Vol.23, No.4 (Oktober 2021), p.2553.

[10]Muhammad Yudha Prawira dan Fatra Alamsyah, *The Implementation of Mutual Legal Assistance between Indonesia and Switzerland Regarding Asset Recovery*, Indonesian Comparative Law Review, Vol.5, No.2 (Desember 2023), p.70.

Hal ini menghambat pengumpulan bukti digital yang bersifat mudah berubah dan memiliki jangka waktu relevansi yang singkat. Penyedia layanan digital global berbasis luar negeri sering kali enggan mematuhi permintaan data dari otoritas Indonesia karena keterbatasan yuridis dan perlindungan privasi di negara asal mereka. Tantangan lain adalah penggunaan teknologi canggih oleh pelaku kejahatan siber, seperti anonimisasi melalui *Virtual Private Network* (VPN) atau enkripsi *end-to-end*, yang semakin mempersulit pelacakan. Di banyak kasus, penyidik Indonesia harus mengandalkan teknologi dan bantuan dari lembaga asing, yang sering kali terbatas oleh kebijakan dan prioritas negara mitra.

Menurut kerangka teoretik penyidikan pidana, pengungkapan tindak pidana lintas batas membutuhkan integrasi yang kuat antara hukum domestik dan mekanisme kerja sama internasional. Teori ini menekankan bahwa penyidikan lintas yurisdiksi memerlukan landasan hukum yang harmonis, alat investigasi yang canggih, serta protokol kolaborasi yang efektif. Dalam konteks Indonesia, UU ITE dan KUHAP memberi dasar hukum domestik, tetapi belum sepenuhnya mengakomodasi kebutuhan investigasi lintas negara[11]. Misalnya, Indonesia belum menjadi bagian dari Budapest Convention on Cybercrime[12] yang merupakan instrumen internasional utama untuk menangani kejahatan siber secara lintas batas. Juga perlu disorot pentingnya penguatan teknologi dan kapasitas penyidik.

Dalam menghadapi tantangan seperti anonimisasi dan enkripsi, penyidik harus memiliki akses ke alat analisis digital yang mutakhir serta pelatihan yang berkelanjutan. Kerangka teoretik menyarankan bahwa investasi dalam teknologi dan SDM memperkuat posisi Indonesia dalam menangani kejahatan siber lintas yurisdiksi. Teori juga menyarankan bahwa waktu adalah faktor kunci dalam penyidikan lintas batas. Bukti digital bersifat sementara, sehingga mekanisme kerja sama yang lambat dapat menyebabkan hilangnya data penting. Sehingga, diperlukan reformasi regulasi domestik yang mempercepat proses permintaan data lintas negara, misalnya melalui pengaturan langsung dengan penyedia layanan global atau adopsi protokol internasional yang lebih fleksibel.

---

[11] Rizki Setyobowo Sangalang dan Thea Farina, *Hukum Pidana Cyber*, PT. Media Penerbit Indonesia, Medan, 2024, p.57.

[12] Dirga Agung, *The Role of Interpol in the Settlement of Cybercrime Cases Under the Budapest Convention on Cybercrimes*, International Journal of Global Community, Vol.5, No.1 (Maret 2022), p.51.

3. Langkah Strategis untuk Mengatasi Kendala Teknis dan Hukum dalam Penyidikan Tindak Pidana Siber di Indonesia

Untuk mengatasi kendala teknis dan hukum dalam penyidikan tindak pidana siber di Indonesia, beberapa langkah strategis dapat dilakukan, baik dari sisi penguatan hukum, pengembangan kapasitas penyidik, maupun pembaruan teknologi. Pertama, perbaikan dan harmonisasi regulasi sangat diperlukan agar lebih sesuai dengan tantangan kejahatan siber yang terus berkembang. Indonesia perlu memperbarui dan menyesuaikan UU ITE dengan perkembangan teknologi terkini, serta memperjelas kewenangan otoritas dalam penyidikan kasus siber, khususnya dalam hal pengumpulan data dan penegakan hukum lintas yurisdiksi. Harmonisasi dengan konvensi internasional, seperti Budapest Convention on Cybercrime, juga menjadi langkah penting untuk memperkuat kerjasama antarnegara dalam penanganan kejahatan siber lintas batas[13].

Kedua, penguatan kapasitas sumber daya manusia (SDM) melalui pelatihan berkelanjutan bagi penyidik siber sangat penting. Penyidik harus dibekali dengan keterampilan dan pemahaman teknis tentang bagaimana mengidentifikasi, mengumpulkan, dan menganalisis bukti digital. Pelatihan ini perlu mencakup aspek teknis seperti penggunaan alat forensik digital, analisis data yang kompleks, serta pemahaman mengenai teknik pemulihan data yang hilang atau rusak. Selain itu, penyidik harus mendapatkan pemahaman tentang hukum internasional yang mengatur penyidikan lintas yurisdiksi, agar lebih siap dalam menghadapi kasus yang melibatkan pihak asing atau data yang disimpan di luar negeri.

Ketiga, peningkatan infrastruktur teknologi dan fasilitas penyidikan digital juga sangat diperlukan. Penyidik perlu dilengkapi perangkat teknologi terbaru yang memungkinkan untuk melakukan penyidikan secara lebih cepat dan akurat. Ini termasuk perangkat lunak forensik digital yang mutakhir, sistem pengolahan data yang aman, dan jaringan komunikasi yang dapat mendukung pertukaran informasi antar lembaga secara efisien. Infrastruktur ini juga harus didukung oleh sistem yang dapat mendeteksi dan melawan teknik anonimasi yang sering digunakan oleh pelaku kejahatan siber, seperti VPN dan enkripsi *end-to-end*.

[13]Ana Campina dan Carlos Rodrigues, *Cybercrime and The Council of Europe Budapest Convention: Prevention, Criminalization, and International Cooperation*, The Book of Full Papers-7th International Zeugma Conference on Scientific Researches (2022), p.122.

Keempat, peningkatan koordinasi antar lembaga penegak hukum, baik di tingkat nasional maupun internasional, menjadi hal yang tidak kalah penting. Indonesia perlu memperkuat mekanisme kerja sama antara Polri, Kominfo, BSSN, dan lembaga penegak hukum lainnya, baik dalam konteks pertukaran data maupun prosedur penyidikan yang terintegrasi. Penyidikan tindak pidana siber yang melibatkan banyak lembaga perlu dilaksanakan dengan pembagian tugas yang jelas, komunikasi yang efisien, dan protokol yang disepakati bersama. Indonesia juga harus lebih aktif dalam menjalin kerjasama internasional untuk mempercepat permintaan data lintas negara dan melibatkan penyedia layanan digital global dalam upaya pemberantasan kejahatan siber.

Menurut kerangka teoretik penyidikan pidana, langkah-langkah strategis ini sejalan dengan prinsip dasar dalam penyidikan yaitu efektivitas, efisiensi, dan keterpaduan. Dalam konteks kejahatan siber, efektivitas penyidikan bergantung pada kemampuan penyidik untuk mengidentifikasi dan mengumpulkan bukti digital yang relevan[14], yang sering kali berupa data yang terdistribusi di berbagai platform dan lokasi. Oleh karena itu, perbaikan regulasi dan peningkatan infrastruktur teknologi adalah langkah krusial untuk memastikan bahwa bukti-bukti ini dapat diperoleh secara sah dan valid. Teori penyidikan pidana juga menekankan pentingnya koordinasi lintas lembaga. Kerja sama yang baik antara lembaga penegak hukum di Indonesia dan di luar negeri memungkinkan penyidik untuk mengatasi batasan yuridiksi dan memperoleh akses ke data yang relevan dengan cepat.

Dalam hal ini, Indonesia perlu mengadopsi prinsip kolaborasi yang lebih fleksibel dan responsif terhadap perkembangan teknologi siber, sebagaimana tercermin dalam kerangka hukum internasional yang ada. Selain itu, teori penyidikan menyarankan penguatan kapasitas SDM dan penggunaan teknologi yang tepat dapat mempercepat proses penyidikan. Dalam hal ini, alat dan teknologi forensik digital yang canggih mendukung penyidik untuk melakukan analisis yang lebih mendalam dan akurat. Peningkatan kapasitas SDM, khususnya dalam hal keterampilan teknis dan pengetahuan hukum, juga memastikan bahwa penyidik dapat menyelesaikan kasus dengan lebih efektif dan efisien.

[14] Ganro Algino, *Fungsi Digital Forensik bagi Satreskrim Polres Agam dalam Penyidikan Tindak Pidana Judi Online*, UNES Law Review, Vol.3, No.2 (Desember 2020), p.196.

C. PENUTUP

1. Penyidikan tindak pidana siber di Indonesia menghadapi berbagai kendala teknis yang signifikan. Kendala utama meliputi keterbatasan sumber daya manusia yang memiliki keahlian khusus di bidang forensik digital, kurangnya infrastruktur teknologi dan alat forensik mutakhir, kompleksitas bukti digital yang tersebar di berbagai platform global, serta keterbatasan kerjasama internasional. Tantangan ini menghambat efektivitas proses penyidikan, terutama dalam pengumpulan, pengolahan, dan validasi bukti digital yang sering kali bersifat sementara dan mudah dimanipulasi.
2. Kendala hukum yang dihadapi dalam penyidikan tindak pidana siber di Indonesia meliputi keterbatasan regulasi dalam mengatur pengelolaan bukti digital dan adaptasi terhadap perkembangan teknologi. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) meskipun memberikan kerangka dasar, belum sepenuhnya memadai untuk menangani kejahatan modern seperti *ransomware*, *blockchain*, dan *deepfake*. Selain itu, tumpang tindih kewenangan antar lembaga penegak hukum dan kurangnya protokol operasional standar memperburuk koordinasi nasional. Di tingkat internasional, perbedaan yurisdiksi hukum antar negara dan ketergantungan pada mekanisme *Mutual Legal Assistance* (MLA) yang lamban memperumit penyidikan lintas batas.

Sebagai langkah strategis untuk mengatasi kendala ini, Indonesia perlu melakukan perbaikan dalam regulasi, memperkuat kapasitas sumber daya manusia melalui pelatihan teknis, serta meningkatkan koordinasi antar lembaga penegak hukum, baik di tingkat nasional maupun internasional. Selain itu, penting bagi Indonesia untuk memperbarui regulasi yang ada, seperti UU ITE, agar lebih sesuai dengan perkembangan teknologi dan tantangan kejahatan siber yang semakin kompleks. Melalui langkah-langkah strategis yang terintegrasi ini, diharapkan proses penyidikan tindak pidana siber di Indonesia dapat berjalan lebih efektif, efisien, dan sesuai dengan standar hukum internasional yang berlaku.

DAFTAR PUSTAKA

Buku

Chazawi, Adami. 2011. *Tindak Pidana Informasi & Transaksi Elektronik*. (Malang: Bayumedia Publishing).

Sangalang, Rizki Setyobowo dan Farina, Thea. 2024. *Hukum Pidana Cyber*. (Medan: PT. Media Penerbit Indonesia).

Publikasi

Agung, Dirga. *The Role of Interpol in the Settlement of Cybercrime Cases Under the Budapest Convention on Cybercrimes.* International Journal of Global Community. Vol.5. No.1 (Maret 2022).

Algino, Ganaro. *Fungsi Digital Forensik bagi Satreskrim Polres Agam dalam Penyidikan Tindak Pidana Judi Online*. UNES Law Review. Vol.3. No.2 (Desember 2020).

Azahra, Alifya Putri, dkk. *Analisa kepada Para Oknum yang Tidak Bijak dalam Menggunakan Media Sosial atau Cyberspace*. Civilia: Jurnal Kajian Hukum dan Pendidikan Kewarganegaraan. Vol.3. No.1 (Januari 2024).

Campina, Ana dan Rodrigues, Carlos. *Cybercrime and The Council of Europe Budapest Convention: Prevention, Criminalization, and International Cooperation*. The Book of Full Papers-7th International Zeugma Conference on Scientific Researches (2022). (ISBN: 978-625-7464-72-7).

Dewi, Cokorda Istri Ratih Utami, dkk. *Peran Kejaksaan dalam Tahap Penuntutan Terhadap Anak yang Melakukan Tindak Pidana Pornografi*. Jurnal Analogi Hukum. Vol.1. No.3 (Juni 2020).

Fariza, Ramadhani. *Dinamika UU ITE Sebagai Hukum Positif di Indonesia Guna Meminimalisir Kejahatan Siber*. Kultura: Jurnal Ilmu Hukum, Sosial, Dan Humaniora. Vol.1. No.1 (September 2023).

Febiana, R. dan Burhanuddin, Agussalim. *Implementasi Kebijakan Sekuritisasi Maritim Presiden Jokowi dalam Menghadapi Aktivitas Ilegal di Perairan Indonesia*. Jurnal Studi Diplomasi dan Keamanan. Vol.16. No.1 (Januari 2024).

Nguyen, Chat Le dan Wilfred, Golman. *Diffusion of the Budapest Convention on Cybercrime and the Development of Cybercrime Legislation in Pacific Island Countries*: *'Law on the books' vs 'law in action'*. Computer Law & Security Review, Elsevier. Vol.40 (April 2021).

Nurisman, Eko. *Risalah Tantangan Penegakan Hukum Tindak Pidana Kekerasan Seksual Pasca Lahirnya Undang-Undang Nomor 12 Tahun 2022*. Jurnal Pembangunan Hukum Indonesia. Vol.4. No.2 (Mei 2022).

Prawira, Muhammad Yudha dan Alamsyah, Fatra. *The Implementation of Mutual Legal Assistance between Indonesia and Switzerland Regarding Asset Recovery*. Indonesian Comparative Law Review. Vol.5. No.2 (Desember 2023).

Schlette, Daniel, dkk. *A comparative Study on Cyber Threat Intelligence: The Security Incident Response Perspective*. IEEE Communications Surveys & Tutorials, IEEE. Vol.23. No.4 (Oktober 2021).

Zahra, Rizka Alifia dkk. *Catfishing dan Implikasinya terhadap Romance Scam oleh Simon Leviev dalam Dokumenter Netflix 'Tinder Swindler' Menurut Perspektif Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Kitab Undang-Undang Hukum Pidana*. Padjadjaran Law Review. Vol.10. No.1 (Juli 2022).

Sumber Hukum

Kitab Undang-Undang Hukum Pidana.

Undang-Undang Nomor 1 Tahun 1946 tentang Peraturan Hukum Pidana.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58. Tambahan Lembaran Negara Republik Indonesia Nomor 4843.