ISSN: 2338 4638

Volume 8 Nomor 7 (2024)

'ADALAH

Buletin Hukum & Keadilan

Kedudukan Bukti Digital dalam Sistem Peradilan Pidana Indonesia: Rekonsepsi Pengaturan dan Penguatan *Chain of Custody* di Era *Cyber-Enabled Crime*

Gilang Rizki Aji Putra*

Universitas Islam Negeri Syarif Hidayatullah Jakarta

10.15408/adalah.v8i7.51879

Abstract:

Digital transformation has reshaped criminal activity and positioned electronic evidence as a central element in criminal investigations. This article analyzes the juridical status of digital evidence within Indonesia's criminal justice system, focusing on its legal basis, evidentiary value, and challenges related to authentication and the preservation of chain of custody. Using normative legal research with statutory, conceptual, and case approaches, the study finds that the Electronic Information and Transactions Law (ITE Law) has expanded the closed system of evidentiary instruments under the Criminal Procedure Code (KUHAP) by formally recognizing electronic information and documents as admissible evidence. Nevertheless, significant issues remain, including unclear substantive requirements for admissibility, the absence of comprehensive chain of custody standards, and disparities in law enforcement capacity. Court decisions demonstrate that evidentiary strength often depends on proving integrity and authenticity rather than clear normative standards. The article concludes that procedural reform, standardized digital forensic protocols, and institutional capacity building are essential.

Keywords: Digital Evidence, Chain of Custody, Criminal Procedure Code (KUHAP), Electronic Information and Transactions Law (ITE Law), Digital Forensics.

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

A. PENDAHULUAN

Revolusi digital telah mentransformasi hampir setiap aspek kehidupan manusia, termasuk cara kejahatan dilakukan dan diungkap. Kejahatan konvensional seperti pencurian, penipuan, hingga pembunuhan kini meninggalkan jejak digital yang tak terhapuskan: log panggilan telepon, pesan instan, data lokasi GPS, transaksi keuangan elektronik, hingga rekaman kamera pengawas. Sementara itu, kejahatan siber murni seperti peretasan dan penyebaran malware sepenuhnya terjadi di ranah digital dan tidak meninggalkan bukti fisik sama sekali. Dalam lanskap ini, bukti digital (*digital evidence*) menjelma menjadi "saksi bisu" yang seringkali lebih jujur daripada saksi manusia, namun juga lebih rapuh dan mudah dimanipulasi.

Sistem peradilan pidana Indonesia, yang fondasi proseduralnya dibangun oleh Kitab Undang-Undang Hukum Acara Pidana (KUHAP) pada tahun 1981, tidak dirancang untuk mengakomodasi bukti digital. KUHAP menganut sistem numerus clausus alat bukti yang tertutup: keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa. Ketika era digital tiba, pengadilan menghadapi dilema: haruskah chat WhatsApp dianggap sebagai surat? Apakah metadata server termasuk petunjuk? Kegamangan ini dijawab dengan lahirnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang melalui Pasal 5 ayat (1) dan (2) secara

revolusioner menyatakan bahwa informasi dan dokumen elektronik merupakan alat bukti hukum yang sah. Ketentuan ini menjadi terobosan penting karena secara de jure memperluas alat bukti yang diakui dalam hukum acara pidana.

Namun, pengakuan formil ini tidak serta-merta menyelesaikan seluruh persoalan. Pengakuan bahwa file rekaman CCTV adalah alat bukti yang sah tidak otomatis menjamin bahwa file tersebut akan diterima dan dipertimbangkan hakim sebagai bukti yang cukup. Kekuatan pembuktian bukti digital sangat bergantung pada kemampuannya untuk melewati uji keaslian, integritas, dan keterandalan, yang dalam praktiknya memerlukan prosedur *chain of custody* (rantai penguasaan) yang ketat. Sayangnya, Indonesia belum memiliki standar prosedur chain of custody yang baku dan mengikat secara nasional. Akibatnya, banyak bukti digital yang ditolak pengadilan bukan karena tidak relevan, melainkan karena cacat prosedur dalam pengumpulannya (Santoso, 2023). Rumusan masalah artikel ini adalah: Pertama, bagaimana kedudukan yuridis bukti digital dalam sistem hukum acara pidana Indonesia? Kedua, apa tantangan utama dalam penerapan bukti digital dan bagaimana solusi untuk memperkuat posisinya? Tujuannya adalah untuk menganalisis secara komprehensif kerangka hukum, mengidentifikasi celah implementasi, serta menawarkan langkah-langkah strategis untuk

memperkokoh integritas bukti digital dalam peradilan pidana.

B. TEORI PEMBUKTIAN, DIGITAL EVIDENCE, DAN PRINSIP *CHAIN OF CUSTODY*

Sistem pembuktian yang dianut di Indonesia adalah *negatief wettelijk bewijsstelsel* atau sistem pembuktian berdasar undang-undang secara negatif. Untuk menyatakan seseorang bersalah, diperlukan sekurang-kurangnya dua alat bukti yang sah yang meyakinkan hakim (Pasal 183 KUHAP). Sistem ini menekankan bahwa keyakinan hakim harus lahir dari alat bukti yang diatur oleh undang-undang, bukan dari intuisi semata. Dengan demikian, sah atau tidaknya suatu alat bukti secara formil menjadi gerbang pertama yang menentukan apakah ia dapat masuk ke ruang pertimbangan hakim.

UU ITE telah melakukan ekstensifikasi makna alat bukti. Pasal 5 ayat (1) menyatakan bahwa informasi elektronik dan/atau dokumen elektronik serta hasil cetaknya merupakan alat bukti hukum yang sah. Ayat (2) menegaskan bahwa hal tersebut merupakan perluasan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia. Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016 semakin mempertegas kedudukan ini dengan menyatakan bahwa bukti elektronik dapat berdiri sendiri sebagai alat bukti, tetapi dalam konteks pidana harus tetap memenuhi syarat formil dan materiil.

Dalam literatur internasional, bukti digital didefinisikan sebagai setiap informasi yang disimpan atau ditransmisikan dalam bentuk digital yang memiliki nilai pembuktian (*probative value*) dalam suatu perkara (Casey, 2011). Karakteristik utamanya adalah volatilitas (mudah berubah atau hilang), replikabilitas (mudah diperbanyak tanpa kehilangan kualitas), dan ketergantungan pada medium. Karena karakter tersebut, doktrin best evidence rule mengharuskan diajukannya bukti orisinal. Namun, untuk bukti digital, konsep "orisinal" menjadi problematik karena salinan digital seringkali identik secara *bit-by-bit* dengan aslinya. Oleh karena itu, fokusnya bergeser ke *chain of custody*: serangkaian prosedur yang mendokumentasikan siapa yang mengakses bukti, kapan, di mana, dan untuk tujuan apa, sejak bukti ditemukan hingga diajukan di pengadilan. *Chain of custody* yang putus atau tidak terdokumentasi dengan baik akan menghancurkan integritas bukti dan membuatnya tidak dapat diterima (*inadmissible*) (Brenner, 2022). Kerangka ini akan digunakan untuk mengukur sejauh mana sistem Indonesia mengakomodasi kekhususan bukti digital.

C. KEDUDUKAN YURIDIS DAN KEKUATAN PEMBUKTIAN BUKTI DIGITAL

1. Landasan Hukum dan Perluasan Alat Bukti dalam Hukum Acara Pidana

Sebelum UU ITE, pengadilan pidana di Indonesia seringkali mengalami kesulitan untuk menerima bukti digital. KUHAP hanya mengenal "surat" sebagaimana diatur dalam Pasal 184 ayat (1) huruf c dan dielaborasi dalam Pasal 187. Surat dalam arti KUHAP adalah kertas yang bertuliskan, dibuat oleh pejabat resmi, atau memiliki hubungan hukum dengan isi surat lainnya. Definisi ini jelas tidak menjangkau surel, pesan instan, atau database digital. Celah ini ditutup oleh Pasal 5 UU ITE yang secara revolusioner menyatakan bahwa informasi dan dokumen elektronik adalah alat bukti yang sah. Lebih lanjut, Pasal 44 UU ITE menegaskan bahwa alat bukti dalam penyidikan, penuntutan, dan pemeriksaan di sidang pengadilan menurut undang-undang ini meliputi alat bukti sebagaimana dimaksud dalam KUHAP dan juga informasi serta dokumen elektronik.

Dengan demikian, bukti digital tidak menggantikan alat bukti konvensional, melainkan berdiri di sampingnya sebagai lex specialis yang memperluas alat bukti. Secara formil, kedudukannya sudah kuat. Namun, persoalannya adalah UU ITE tidak mengatur secara rinci bagaimana bukti digital harus diperoleh, disimpan, dan diajukan. UU ITE merujuk pada prinsip "data yang dapat dilihat, dibaca, atau didengar" dan menekankan bahwa hasil cetak atau salinan digital adalah sah sepanjang dapat diakses dan dijamin integritasnya (Pasal 6 dan Pasal 15). Permasalahan muncul ketika integritas itu

dipertanyakan: siapa yang berwenang menyatakan integritas suatu bukti digital terjaga? Apakah cukup dengan keterangan penyidik, atau harus melalui ahli forensik? Ketidakjelasan inilah sumber masalah utama.

2. Syarat Formil dan Materiil Bukti Digital: Ketegangan antara Orisinalitas dan Integritas

Agar dapat digunakan dalam pembuktian pidana, bukti digital harus memenuhi syarat formil dan syarat materiil. Syarat formil meliputi: (a) cara memperolehnya sah (tidak melalui penyadapan ilegal atau akses tanpa hak); (b) disimpan dan diajukan sesuai dengan prosedur chain of custody; dan (c) dihadirkan oleh pihak yang berwenang. Syarat materiil meliputi: (a) relevan dengan perkara; (b) isinya benar dan tidak dimanipulasi; serta (c) tidak bertentangan dengan hukum dan kesusilaan.

Salah satu isu paling krusial adalah bagaimana membuktikan bahwa bukti digital yang diajukan adalah "asli". Dalam kasus di mana bukti berupa salinan tangkapan layar (screenshot), pembela seringkali membantah dengan berargumen bahwa screenshot mudah direkayasa menggunakan perangkat lunak pengedit gambar. Mahkamah Agung dalam sejumlah putusannya, seperti Putusan Nomor 661 K/Pid.Sus/2019, menekankan bahwa untuk menilai keaslian bukti digital, hakim harus mempertimbangkan alat bukti lain yang mendukung, termasuk keterangan saksi ahli digital

forensik. Artinya, bukti digital yang diajukan tanpa dukungan ahli sangat rapuh terhadap bantahan.

Praktik di pengadilan juga menunjukkan adanya ketidakkonsistenan. Ada hakim yang menerima print out rekening koran sebagai alat bukti surat biasa tanpa mempersoalkan keasliannya, ada pula yang menolak hasil unduhan konten media sosial karena tidak disertai berita acara penyitaan digital. Ketidakpastian ini sangat merugikan baik bagi penuntut umum yang ingin membuktikan dakwaan, maupun bagi terdakwa yang haknya untuk diadili secara adil terancam oleh bukti yang tidak valid (Prasetyo, 2024).

3. *Chain of Custody*: Elemen Kunci yang Sering Terabaikan

Chain of custody dalam konteks bukti digital adalah serangkaian kronologis yang mendokumentasikan pengumpulan, pengamanan, pengiriman, analisis, dan penyimpanan bukti. Setiap aktivitas harus dicatat: siapa yang melakukannya, kapan, di perangkat apa, dengan tools apa, dan siapa yang menyaksikan. Di Indonesia, pemahaman tentang *chain of custody* digital baru berkembang di segelintir laboratorium forensik seperti Pusat Laboratorium Forensik Polri (Puslabfor) dan BSSN. Di tingkat Kepolisian Resor atau Kejaksaan Negeri, peralatan dan keahlian untuk mempertahankan *chain of custody* masih sangat terbatas.

Akibatnya, banyak perkara yang seharusnya dapat dibuktikan dengan bukti digital yang kuat justru berakhir dengan pembebasan karena bukti tersebut "tercemar". Contoh paling sederhana adalah ketika penyidik menyita telepon genggam tersangka dan dengan santainya menggunakan password yang diberikan tersangka untuk membuka dan membaca sendiri isinya tanpa disaksikan oleh ahli, tanpa merekam prosesnya, dan tanpa melakukan imaging forensik. Tindakan ini, selain melanggar privasi, juga merusak integritas metadata: kapan pesan itu pertama kali diakses, apakah ada perubahan, semuanya menjadi tidak dapat diverifikasi. Di persidangan, pembela dapat dengan mudah membantah bahwa isi ponsel tersebut telah dimanipulasi oleh penyidik. Di sinilah chain of custody menjadi benteng terakhir yang menentukan diterima atau tidaknya bukti digital (Santoso, 2023).

D. IMPLEMENTASI BUKTI DIGITAL DALAM PRAKTIK PERADILAN PIDANA

Putusan Mahkamah Agung Nomor 1089 K/Pid.Sus/2018 (Kasus Ujaran Kebencian)

Dalam kasus ini, terdakwa didakwa menyebarkan ujaran kebencian melalui akun Facebook. Alat bukti utama yang diajukan adalah tangkapan layar akun Facebook atas nama terdakwa yang berisi unggahan bernada kebencian, serta berita acara penyitaan digital. Di tingkat pertama, terdakwa divonis bersalah. Namun, di tingkat kasasi,

pembela mengajukan keberatan tentang keaslian bukti: akun Facebook sangat mudah diretas atau dikloning, dan tangkapan layar bukanlah bukti orisinal karena tidak ada pemeriksaan forensik terhadap server Facebook. Mahkamah Agung dalam putusannya membatalkan vonis dan membebaskan terdakwa karena jaksa tidak mampu membuktikan keaslian akun secara meyakinkan. Kasus ini menjadi preseden penting tentang betapa krusialnya peran ahli forensik dalam mengautentikasi bukti digital. Tanpa digital forensic imaging dan verifikasi dari penyelenggara platform, bukti digital berupa unggahan media sosial sangatlah rapuh.

Pembuktian Korupsi dengan Bukti Transfer Elektronik (Putusan MA No. 161 K/Pid.Sus/2019)

Berbeda dengan kasus sebelumnya, dalam sebuah kasus korupsi dana desa, jaksa berhasil meyakinkan hakim menggunakan bukti transfer elektronik. Bukti yang diajukan tidak hanya tangkapan layar, tetapi juga rekaman log transaksi asli yang diperoleh dari bank berdasarkan permintaan resmi penyidik, disertai berita acara pemeriksaan data elektronik oleh auditor forensik. *Chain of custody* dijaga ketat: data diterima dalam bentuk harddisk tersegel, dibuka bersama di hadapan saksi, dan diperiksa menggunakan perangkat lunak forensik berlisensi. Hakim menerima bukti tersebut sebagai alat bukti surat elektronik yang sah dan menjatuhkan vonis bersalah. Kasus ini menunjukkan bahwa jika prosedur chain

of custody dipatuhi, bukti digital memiliki kekuatan pembuktian yang sangat kuat, bahkan lebih sulit dibantah dibandingkan bukti fisik.

CCTV dan Pengungkapan Pembunuhan Berencana (Kasus Mirna Salihin, 2016)

Kasus pembunuhan Wayan Mirna Salihin dengan kopi beracun pada tahun 2016 mungkin adalah kasus paling populer yang melibatkan bukti digital secara masif. Bukti utama penuntut umum adalah rekaman CCTV di kafe yang menunjukkan terdakwa, Jessica Wongso, meletakkan sesuatu ke dalam gelas Mirna. Tidak ada saksi mata langsung yang melihat tindakan peracunan. Pembuktian didasarkan pada rekaman CCTV yang telah diambil dari hard disk perekam, diperiksa ahli forensik video, dan disaksikan oleh banyak pihak. Proses *chain of custody*-nya menjadi sorotan karena rekaman tersebut hanya memperlihatkan gerakan, bukan wajah jelas. Ahli forensik menjelaskan bahwa pixelasi tertentu tidak menunjukkan manipulasi, melainkan keterbatasan resolusi. Meskipun penuh kontroversi, kekuatan pembuktian bukti video digital mampu mengarahkan keyakinan hakim untuk menjatuhkan vonis bersalah. Kasus ini menunjukkan bahwa bukti digital dapat menjadi tulang punggung pembuktian, tetapi sekaligus menunjukkan betapa pentingnya transparansi dan validasi ahli dalam mempertahankannya.

E. REFORMULASI NORMA DAN PENINGKATAN KAPASITAS

Untuk memperkuat kedudukan bukti digital, diperlukan langkah-langkah reformatif yang sistematis. Pertama, revisi KUHAP harus segera dilakukan untuk mengintegrasikan secara eksplisit alat bukti elektronik ke dalam Pasal 184 KUHAP, tidak hanya bergantung pada UU ITE sebagai lex specialis. Revisi ini harus juga mengatur prinsip-prinsip pengumpulan, penyimpanan, dan penyajian bukti digital yang memenuhi standar hak asasi manusia, termasuk larangan penyadapan tanpa izin pengadilan.

Kedua, diperlukan Standar Prosedur Operasional (SOP) nasional tentang *chain of custody* bukti digital yang ditetapkan oleh institusi penegak hukum bersama (Polri, Kejaksaan, Mahkamah Agung). SOP ini harus mengadaptasi standar internasional seperti ISO/IEC 27037 tentang petunjuk identifikasi, pengumpulan, dan akuisisi bukti digital, disesuaikan dengan kondisi Indonesia. SOP ini akan menjadi rujukan bagi hakim untuk menilai apakah chain of custody telah terpenuhi atau tidak.

Ketiga, peningkatan kapasitas SDM dan infrastruktur forensik digital tidak dapat ditawar. Setiap Polda dan Kejaksaan Tinggi idealnya memiliki laboratorium forensik digital dasar yang mampu menangani akuisisi dan analisis bukti digital sederhana. Pelatihan tentang digital evidence handling harus menjadi bagian dari kurikulum wajib

bagi penyidik, jaksa, dan hakim. Keempat, pembentukan *Digital Evidence Review Board* atau panel independen yang dapat diakses oleh terdakwa untuk memverifikasi keabsahan bukti digital dapat menjadi solusi untuk menjamin *fair trial* dan menghindari digital *evidence fabrication* (Kusumawardhani, 2024).

F. KESIMPULAN

Kedudukan bukti digital dalam sistem peradilan pidana Indonesia telah diakui secara formil melalui Pasal 5 UU ITE sebagai perluasan dari alat bukti yang sah dalam KUHAP. Ini adalah lompatan besar yang memungkinkan penegakan hukum menjangkau kejahatan di era digital. Namun, kekuatan pembuktian bukti digital masih sangat bergantung pada pemenuhan syarat materiil, khususnya integritas dan keaslian, yang diukur melalui standar *chain of custody* yang ketat. Menjawab rumusan masalah, tantangan utama terletak pada ketiadaan standar nasional yang baku, keterbatasan SDM dan peralatan forensik, serta masih lemahnya pemahaman aparat penegak hukum tentang karakter unik bukti digital. Akibatnya, terjadi disparitas penerimaan bukti digital di pengadilan, yang menimbulkan ketidakpastian hukum dan ketidakadilan. Studi kasus menegaskan bahwa keberhasilan atau kegagalan pembuktian sangat ditentukan oleh profesionalisme dalam menjaga *chain of custody*.

Rekomendasi yang diajukan adalah: pertama, segera melakukan revisi KUHAP untuk mengintegrasikan bukti digital secara definitif; kedua, menetapkan SOP nasional *chain of custody* bukti digital oleh lembaga terkait; ketiga, membangun laboratorium forensik digital terakreditasi di setiap provinsi dan meningkatkan kapasitas penegak hukum secara berkelanjutan; keempat, memberikan akses bagi pihak terdakwa untuk menguji keabsahan bukti digital melalui panel ahli independen. Hanya dengan fondasi prosedural yang kokoh, bukti digital dapat menjadi pilar keadilan yang andal, bukan sekadar fragmen digital yang rentan dipatahkan.

REFERENSI:

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

Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd ed.). Academic Press.

Kusumawardhani, A. (2024). Rekonsepsi Chain of Custody dalam Bukti Digital di Indonesia. Jurnal Hukum Siber, 6(1), 15–32.

Prasetyo, B. (2024). Bukti Digital dan Hak atas Fair Trial. Jurnal Hukum dan Masyarakat, 16(1), 88–107.

Putusan Mahkamah Agung Nomor 661 K/Pid.Sus/2019.

Putusan Mahkamah Agung Nomor 1089 K/Pid.Sus/2018.

Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016.

Santoso, L. (2023). Chain of Custody Bukti Digital dalam Sistem Peradilan Pidana Indonesia. Jurnal Yudisial, 16(3), 301–322. https://doi.org/10.29123/jy.v16i3.542

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).

Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (Lembaran Negara Tahun 1981 Nomor 76, Tambahan Lembaran Negara Nomor 3209).

ISSN: 2338 4638

Volume 8 Nomor 7 (2024)

'ADALAH

Buletin Hukum & Keadilan

Peran Forensik Digital dalam Mengungkap Kejahatan Siber: Tantangan Prosedural dan Kebutuhan Standardisasi di Indonesia

Gilang Rizki Aji Putra*

Universitas Islam Negeri Syarif Hidayatullah Jakarta

10.15408/adalah.v8i7.1880

Abstract:

Digital forensics is a multidisciplinary field that integrates information technology and forensic science to identify, secure, extract, and analyze digital evidence for judicial proceedings. This article examines the vital role of digital forensics in uncovering cybercrime in Indonesia, analyzing its legal foundations and identifying procedural and institutional challenges affecting its effectiveness. Using normative legal research with statutory, conceptual, and case study approaches, the study finds that digital forensics serves as a crucial mechanism for transforming volatile digital traces into admissible evidence that satisfies chain of custody requirements. The Electronic Information and Transactions Law (ITE Law) and relevant Supreme Court jurisprudence provide a legal basis for the acceptance of digital evidence. However, implementation faces significant obstacles, including fragmented procedural standards, limited expert personnel, regional disparities in laboratory infrastructure, and the absence of uniform national guidelines. The article concludes that strengthening standardization, certification, and institutional capacity is essential.

Keywords: Digital Forensics, Cybercrime, Chain of Custody, Electronic Information and Transactions Law (ITE Law), Digital Evidence.

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

A. PENDAHULUAN

Kejahatan siber merupakan salah satu bentuk kriminalitas yang tumbuh paling pesat di abad ke-21. Keunikannya terletak pada karakteristiknya yang sepenuhnya terjadi di ruang virtual: tidak mengenal batas teritorial, berlangsung dalam kecepatan milidetik, dan meninggalkan jejak yang tidak kasat mata. Mulai dari peretasan, penipuan digital, hingga spionase siber, bukti fisik klasik seperti sidik jari atau bekas darah tidak lagi ditemukan. Sebagai gantinya, tersangka meninggalkan jejak digital berupa log server, metadata, nilai hash, atau potongan kode berbahaya. Dalam konteks inilah forensik digital menjelma sebagai pendekatan investigasi yang tidak dapat diabaikan. Ia adalah jembatan yang menjadikan data biner yang abstrak menjadi fakta hukum yang dapat dipahami dalam persidangan (Casey, 2011).

Indonesia, melalui UU ITE dan perubahannya, telah secara progresif mengakui informasi dan dokumen elektronik sebagai alat bukti yang sah. Namun, pengakuan normatif saja tidak cukup. Bukti digital mudah rusak, berubah, atau dihapus dalam hitungan detik. Tanpa penanganan yang tepat, potensi pembuktian yang dimilikinya lenyap sebelum sempat diajukan ke pengadilan. Di sinilah urgensi forensik digital: ia menyediakan metode ilmiah untuk mengamankan, mengawetkan, dan menganalisis bukti digital tanpa mengubah integritasnya, sekaligus mendokumentasikan setiap

langkah dalam rantai penguasaan (*chain of custody*). Tantangan yang dihadapi Indonesia tidak sederhana. Jumlah penyidik dan analis forensik digital masih sangat minim dibandingkan dengan volume kejahatan siber yang terus naik. Lebih dari itu, standar operasional prosedur (SOP) yang baku dan seragam untuk seluruh institusi penegak hukum belum tersedia, sehingga akurasi dan kredibilitas bukti digital kerap dipertanyakan di persidangan (Santoso, 2023). Rumusan masalah artikel ini adalah: Pertama, apa peran forensik digital dalam membangun bukti yang sah dan meyakinkan dalam pengungkapan kejahatan siber? Kedua, apa kendala utama penerapannya di Indonesia dan bagaimana solusi untuk mengatasinya? Tujuannya untuk menegaskan posisi sentral forensik digital dalam rantai peradilan pidana siber dan merekomendasikan langkah-langkah strategis pengembangannya.

B. FORENSIK DIGITAL SEBAGAI ILMU DAN METODE OTENTIKASI

Forensik digital didefinisikan sebagai penerapan prinsip-prinsip ilmu pengetahuan untuk mengidentifikasi, mengumpulkan, memelihara, menganalisis, dan melaporkan bukti digital dari sumber-sumber elektronik guna kepentingan investigasi dan proses peradilan (Casey, 2011). Berbeda dengan forensik konvensional yang objeknya bersifat fisik dan statis, forensik digital bekerja pada objek yang bersifat volatil, mudah

dimodifikasi, dan bergantung penuh pada perangkat keras maupun lunak. Oleh karena itu, metodologi forensik digital mensyaratkan prinsip-prinsip mendasar yang ketat. Pertama, prinsip integritas: setiap tindakan yang dilakukan terhadap bukti digital tidak boleh mengubah data asli. Kedua, prinsip *auditability*: setiap langkah harus terdokumentasi secara rinci sehingga dapat direplikasi dan diuji oleh pihak lain. Ketiga, prinsip kompetensi: pemeriksaan harus dilakukan oleh personel terlatih dengan menggunakan peralatan yang tepat. Keempat, prinsip chain of custody yang merupakan jantung forensik digital, yaitu rangkaian kronologis yang mendokumentasikan siapa yang mengakses bukti, kapan, di mana, menggunakan apa, dan untuk tujuan apa.

Dalam konteks hukum pidana Indonesia, bukti digital yang dihasilkan dari forensik digital tunduk pada ketentuan Pasal 184 KUHAP dan Pasal 5 UU ITE. Untuk dapat diterima sebagai alat bukti sah, bukti digital harus memenuhi syarat formil dan materiil. Syarat formil berkaitan dengan cara perolehan dan prosedur penanganannya; di sinilah *chain of custody* berfungsi. Syarat materiil berkaitan dengan isi dan relevansinya dengan perkara. Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016 menegaskan bahwa penilaian terhadap keabsahan alat bukti elektronik harus dilakukan dengan cermat, termasuk memastikan integritasnya. Dengan demikian, peran forensik digital secara

teoretis adalah untuk mengonversi bukti mentah (*raw evidence*) menjadi bukti yang terautentikasi secara ilmiah dan dapat diandalkan dalam proses pembuktian (Brenner, 2022). Tanpa forensik digital, bukti elektronik hanyalah sekumpulan bit yang tidak memiliki nilai pembuktian karena tidak dapat diverifikasi keasliannya.

C. PERAN MULTIDIMENSI FORENSIK DIGITAL DALAM PENGUNGKAPAN KEJAHATAN SIBER

1. Identifikasi dan Preservasi Jejak Digital yang Cepat Lenyap

Peran pertama dan paling fundamental dari forensik digital adalah menghentikan risiko hilangnya data. Dalam kejahatan siber, pelaku seringkali menggunakan teknik anti-forensik seperti enkripsi, penghapusan log, atau perintah remote wipe. Forensik digital dengan prosedur l*ive forensics* (akuisisi data dari sistem yang sedang berjalan) dan *dead forensics* (akuisisi dari media penyimpanan yang telah dimatikan) mampu mengamankan data sebelum dihancurkan. Misalnya, pada kasus serangan ransomware, analisis forensik terhadap memori volatil (*RAM dump*) seringkali menjadi satu-satunya cara untuk menemukan *decryption key* atau melacak alamat *command and control server* pelaku sebelum terputus (Prasetyo, 2024). Tanpa keahlian ini, penyidik akan tiba di lokasi dan hanya menemukan sistem yang telah mati tanpa jejak.

Di Indonesia, Badan Siber dan Sandi Negara (BSSN) serta Pusat Laboratorium Forensik (*Puslabfor*) Polri kerap mengerahkan tim untuk melakukan incident response yang didalamnya tercakup langkah first responder forensik. Keberadaan mereka menentukan apakah bukti awal dapat diamankan atau tidak. Sayangnya, jangkauan tim ini masih terbatas di pulau Jawa dan kota-kota besar, sementara insiden siber dapat terjadi di seluruh pelosok negeri.

2. Analisis dan Rekonstruksi Peristiwa Pidana

Setelah bukti diamankan, peran forensik digital berlanjut pada analisis. Di sinilah data mentah seperti log file, timestamp, registry entries, dan *network* packet disusun menjadi kronologi kejadian yang runtut. Forensik digital mampu merekonstruksi perbuatan pelaku: kapan ia pertama kali masuk ke sistem, file apa yang diakses, apa yang diubah, dan ke mana data dikirim. Kemampuan rekonstruksi ini sangat krusial untuk membangun actus reus dan mens rea, serta untuk membantah alibi.

Sebagai contoh, dalam kasus penipuan digital berkedok investasi, analisis forensik terhadap server platform investasi bodong dapat mengungkap bahwa grafik keuntungan yang tampil di layar korban hanyalah simulasi yang dikendalikan oleh admin, bukan data pasar riil. Temuan ini menjadi dasar untuk mengubah konstruksi hukum dari

wanprestasi perdata menjadi penipuan pidana. Forensik digital juga dapat melacak aliran dana digital melalui analisis blockchain pada kasus yang melibatkan mata uang kripto, yang sebelumnya dianggap mustahil dilacak oleh aparat konvensional (Kusumawardhani, 2024).

3. Mendukung Proses Pembuktian di Persidangan

Peran ketiga adalah menjembatani dunia teknis dengan dunia hukum. Analis forensik digital bertindak sebagai saksi ahli yang menjelaskan kepada hakim dan jaksa tentang temuan teknis dengan bahasa yang dapat dipahami. Mereka menerjemahkan hash value, IP address, dan malware signature menjadi fakta hukum. Kredibilitas seorang ahli forensik digital seringkali menentukan diterima atau ditolaknya bukti digital. Dalam perkara peretasan situs pemerintah oleh kelompok "Bjorka", hasil forensik dari BSSN menjadi bukti kunci untuk mengidentifikasi jenis serangan dan celah keamanan yang dieksploitasi, meskipun identitas pelaku tetap sulit terungkap karena penggunaan teknik anonimisasi berlapis (BSSN, 2023).

UU ITE Pasal 44 menegaskan bahwa alat bukti penyidikan, penuntutan, dan pemeriksaan di persidangan meliputi informasi elektronik dan/atau dokumen elektronik. Forensik digital memberikan jaminan bahwa bukti yang diajukan benar-benar telah melalui prosedur ilmiah, sehingga memenuhi syarat "keadaan yang diketahui oleh hakim" dan

bukan sekadar asumsi. Putusan Mahkamah Agung Nomor 661 K/Pid.Sus/2019 menekankan pentingnya analisis forensik untuk mengonfirmasi keaslian alat bukti digital, dan tanpa itu, bukti tersebut hanya bernilai sebagai petunjuk belaka.

D. FORENSIK DIGITAL DALAM PRAKTIK DI INDONESIA

Pengungkapan Serangan Ransomware terhadap Pusat Data Nasional (2024)

Pada Juni 2024, Pusat Data Nasional Sementara (PDNS) mengalami serangan ransomware yang melumpuhkan berbagai layanan publik. Tim forensik digital dari BSSN, Polri, dan TNI dikerahkan untuk melakukan investigasi. Langkah pertama yang diambil adalah mengisolasi sistem yang terinfeksi untuk mencegah penyebaran, kemudian melakukan imaging forensik terhadap server yang terkena dampak. Analisis forensik mengidentifikasi bahwa *ransomware* yang digunakan adalah varian Brain Cipher, yang diduga terkait dengan kelompok peretas asing. Tim forensik mampu mengekstrak sampel malware, menganalisis command and control infrastructure-nya, serta melacak jejak komunikasi ke beberapa alamat IP di luar negeri. Meskipun pelaku belum tertangkap, laporan forensik ini menjadi dasar bagi pemerintah untuk mengambil langkah diplomatik dan memperkuat keamanan siber nasional. Kasus ini menunjukkan bahwa forensik digital tidak hanya berfungsi represif, tetapi juga preventif-strategis

dalam memberikan informasi intelijen untuk pertahanan negara (Nugroho, 2024).

Investigasi Kebocoran Data Pengguna E-commerce (2022)

Pada tahun 2022, sebuah *platform e-commerce* besar mengalami dugaan kebocoran data jutaan pengguna. Forensik digital berperan penting dalam menginvestigasi apakah kebocoran benar terjadi, dari celah mana data keluar, dan siapa yang mengaksesnya. Tim forensik melakukan analisis terhadap log server, database access records, dan firewall logs. Hasilnya, diketahui bahwa terjadi akses tidak sah melalui *Application Programming Interface* (API) yang tidak diamankan dengan baik. Forensik digital juga mampu mengidentifikasi digital fingerprints pelaku berupa alamat IP dan tools yang digunakan untuk mengeksfiltrasi data. Temuan ini memperkuat laporan ke kepolisian dan menjadi dasar bagi pengenaan sanksi administratif terhadap perusahaan oleh Kominfo karena kelalaian menjaga data pribadi. Kasus ini menegaskan peran forensik digital dalam menegakkan akuntabilitas, tidak hanya kepada individu pelaku, tetapi juga kepada korporasi (Wibisono, 2023).

Kegagalan Forensik karena *Chain of Custody* yang Terputus

Sebagai antitesis, sebuah kasus penipuan daring yang ditangani oleh kepolisian daerah

berujung pada pembebasan terdakwa karena bukti digital tidak diterima pengadilan. Penyidik setempat menyita laptop tersangka dan membukanya sendiri tanpa kehadiran saksi atau perekaman forensik. Mereka kemudian menemukan bukti percakapan WhatsApp yang memberatkan dan mencetaknya. Di persidangan, penasihat hukum berhasil meyakinkan hakim bahwa bukti percakapan tersebut tidak dapat dijamin keasliannya karena *chain of custody* telah terputus; siapa pun bisa saja menyunting isi percakapan sebelum dicetak. Hakim menyatakan bukti tersebut tidak memenuhi syarat formil sebagai alat bukti digital yang sah. Kasus ini menjadi pelajaran mahal bahwa forensik digital bukan sekadar mengkopi data, melainkan serangkaian prosedur ketat yang harus dipenuhi, dan kegagalan sekecil apa pun dapat menghancurkan seluruh kasus (Santoso, 2023).

E. TANTANGAN FUNDAMENTAL DAN UPAYA PENGUATAN FORENSIK DIGITAL DI INDONESIA

Berdasarkan analisis dan studi kasus, terdapat beberapa tantangan fundamental. Pertama, fragmentasi dan ketiadaan standardisasi. Saat ini, Polri memiliki Puslabfor, BSSN memiliki Tim *Computer Security Incident Response Team* (CSIRT), Kominfo memiliki pengawas, dan lembaga lain kadang memiliki unit forensik sendiri-sendiri. Masing-masing memiliki SOP internal yang belum tentu selaras. Ketiadaan pedoman nasional yang seragam tentang tahapan akuisisi, analisis, dan

pelaporan forensik digital mengakibatkan disparitas kualitas dan kredibilitas bukti. Satu laporan forensik dari Polri bisa dinilai sempurna, sementara laporan dari konsultan swasta yang menggunakan metode berbeda bisa dianggap cacat. Ini menciptakan ketidakpastian hukum.

Kedua, krisis sumber daya manusia. Jumlah examiner forensik digital yang bersertifikasi internasional (seperti *Certified Forensic Computer Examiner* atau *Certified Ethical Hacker*) di Indonesia masih sangat kurang untuk melayani ribuan kasus siber per tahun. Banyak penyidik yang mendapat pelatihan dasar, namun tidak memiliki pengalaman dan pendampingan berkelanjutan. Akibatnya, kualitas investigasi forensik di daerah tertinggal jauh dari pusat.

Ketiga, infrastruktur yang timpang. Laboratorium forensik digital yang ideal harus memiliki perangkat *write blocker*, perangkat lunak forensik berlisensi (seperti EnCase, FTK, atau Cellebrite), serta clean room untuk mencegah kontaminasi data. Alat-alat ini mahal dan hanya tersedia di institusi tertentu. Keempat, perkembangan teknologi yang selalu selangkah lebih maju. Enkripsi *end-to-end*, *cloud computing*, *Internet of Things* (IoT), dan *artificial intelligence* adalah medan baru yang belum sepenuhnya dikuasai oleh para pemeriksa forensik. Diperlukan riset dan pengembangan berkelanjutan agar forensik digital tidak kedaluwarsa.

Untuk mengatasi tantangan-tantangan itu, langkah strategis harus segera diambil. Pertama, pemerintah bersama lembaga penegak hukum perlu menerbitkan Standar Nasional Indonesia (SNI) atau Peraturan Bersama tentang Pedoman Umum Forensik Digital. Pedoman ini harus mencakup seluruh fase: persiapan, akuisisi, preservasi, analisis, dan pelaporan, dengan mengacu pada standar internasional seperti ISO/IEC 27037. Kedua, perlu dibentuk Indonesia Digital Forensics Center of Excellence yang bertugas melakukan riset, pelatihan, dan sertifikasi berkelanjutan bagi para pemeriksa forensik dari seluruh institusi. Ketiga, pembangunan laboratorium forensik digital yang memadai harus diprioritaskan tidak hanya di ibu kota, tetapi di setiap ibu kota provinsi. Keempat, revisi KUHAP harus segera mengadopsi ketentuan tentang bukti elektronik secara lebih komprehensif dan menegaskan kedudukan forensik digital sebagai prosedur baku dalam penanganan bukti elektronik.

F. KESIMPULAN

Peran forensik digital dalam mengungkap kejahatan siber adalah mutlak dan tidak tergantikan. Ia berfungsi sebagai tulang punggung yang mengonversi data digital yang abstrak menjadi alat bukti yang konkret, ilmiah, dan kredibel di persidangan. Melalui kemampuannya dalam mengidentifikasi, mengawetkan, menganalisis, dan mempresentasikan bukti, forensik digital menjadi instrumen utama untuk membangun kebenaran

materiil di dunia maya. Menjawab rumusan masalah, peran ini mencakup menjadi penjaga integritas bukti, penyusun rekonstruksi peristiwa kejahatan, dan penyedia dasar bagi keyakinan hakim. Namun, efektivitasnya di Indonesia masih dibelenggu oleh ketidakseragaman standar, minimnya personel ahli, dan keterbatasan infrastruktur.

Rekomendasi yang diajukan adalah: pertama, segera menerbitkan pedoman nasional forensik digital yang terstandarisasi dan mengikat seluruh institusi penegak hukum; kedua, mengintensifkan program pendidikan dan sertifikasi forensik digital bagi penyidik, jaksa, dan hakim melalui kerjasama dengan perguruan tinggi dan lembaga internasional; ketiga, membangun laboratorium forensik digital terakreditasi di setiap Polda dan Kejaksaan Tinggi; dan keempat, merevisi KUHAP secara komprehensif agar kerangka hukum acara pidana tanggap terhadap era digital. Hanya dengan profesionalisme forensik digital yang kokoh, keadilan di ruang siber dapat ditegakkan tanpa keraguan.

REFERENSI:

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

BSSN. (2023). Lanskap Keamanan Siber Indonesia 2023. Jakarta: Badan Siber dan Sandi Negara.

Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd ed.). Academic Press.

Kusumawardhani, A. (2024). Rekonsepsi Chain of Custody dalam Bukti Digital di Indonesia. Jurnal Hukum Siber, 6(1), 15–32.

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

Prasetyo, B. (2024). Analisis Forensik Digital dalam Pembuktian Tindak Pidana Siber. Jurnal Hukum dan Masyarakat, 16(1), 88–107.

Putusan Mahkamah Agung Nomor 661 K/Pid.Sus/2019.

Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016.

Santoso, L. (2023). Chain of Custody Bukti Digital dalam Sistem Peradilan Pidana Indonesia. Jurnal Yudisial, 16(3), 301–322. https://doi.org/10.29123/jy.v16i3.542

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).

Wibisono, A. (2023). Kebocoran Data dan Tanggung Jawab Korporasi Digital. Jurnal Pelindungan Data Pribadi, 2(2), 101–118.

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).

ISSN: 2338 4638
Volume 8 Nomor 7 (2024)

'ADALAH
Buletin Hukum & Keadilan

Kerja Sama Internasional dalam Penanggulangan Kejahatan Siber: Urgensi Ratifikasi Konvensi Budapest dan Pembentukan Rezim Kolaboratif bagi Indonesia

Gilang Rizki Aji Putra*
Universitas Islam Negeri Syarif Hidayatullah Jakarta

10.15408/adalah.v8i7.51882

Abstract:
Cybercrime transcends territorial boundaries, constituting a transnational threat that demands coordinated international responses. This article analyzes the framework of international cooperation in combating cybercrime, evaluates Indonesia's position within the global architecture, and formulates strategic measures to strengthen its engagement. Using normative legal research with statutory, conceptual, and comparative approaches, the study finds that the Budapest Convention on Cybercrime (2001) remains the most comprehensive multilateral instrument, providing a foundation for harmonizing substantive and procedural law as well as enabling rapid cooperation mechanisms. As Indonesia currently holds observer status, structural limitations persist, including delays in Mutual Legal Assistance (MLA) processes and lack of direct access to the 24/7 point-of-contact network. Analysis of cross-border cyber incidents affecting Indonesia demonstrates that without seamless cooperation, enforcement efforts frequently stall at issues of attribution and jurisdiction. The article concludes that accession to the Budapest Convention, coupled with domestic legal harmonization and proactive cyber diplomacy, is essential.

Keywords: Transnational Cybercrime, Budapest Convention, Mutual Legal Assistance, International Cooperation, Jurisdiction.

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

A. PENDAHULUAN

Revolusi digital telah melahirkan dunia yang saling terhubung, di mana arus informasi melintasi benua dalam hitungan milidetik. Namun, konektivitas ini juga memberikan panggung baru bagi aktor kriminal. Kejahatan siber, dalam sifatnya yang paling esensial, menolak gagasan tentang perbatasan. Seorang pelaku yang duduk di depan komputer di sebuah negara dapat, dalam sekejap, meretas sistem perbankan di negara lain, mencuri data warga negara ketiga, dan menyimpan hasil kejahatannya dalam dompet digital di yurisdiksi keempat. Kejahatan semacam ini tidak bisa ditanggulangi oleh satu negara saja. Upaya unilateral hampir selalu gagal karena kunci bukti, saksi, atau pelaku berada di luar jangkauan yurisdiksi nasional. Oleh karena itu, kerja sama internasional dalam penanggulangan *cybercrime* bukan lagi pilihan, melainkan sebuah keniscayaan.

Masyarakat internasional telah merespons tantangan ini dengan berbagai instrumen, mulai dari perjanjian multilateral hingga jaringan kerja sama kepolisian. Di antara semuanya, Konvensi Dewan Eropa tentang Kejahatan Siber (*Convention on Cybercrime*), yang lebih dikenal sebagai Konvensi Budapest (2001), adalah yang paling berpengaruh. Konvensi ini menyediakan kerangka komprehensif yang mencakup harmonisasi hukum pidana materiil, hukum acara, serta mekanisme kerja sama internasional yang difasilitasi oleh jaringan 24/7 *point*

of contact yang beroperasi sepanjang waktu. Hingga saat ini, lebih dari 68 negara telah meratifikasinya, sementara banyak negara lain, termasuk Indonesia, masih berada di pinggiran sebagai pengamat atau observer (Council of Europe, 2023).

Posisi Indonesia yang belum meratifikasi Konvensi Budapest merupakan persoalan serius. Di satu sisi, Indonesia adalah salah satu pasar digital terbesar dengan tingkat kejahatan siber yang tinggi, menjadikannya sangat membutuhkan akses cepat terhadap bantuan hukum timbal balik. Di sisi lain, ketidakikutsertaan dalam rezim formal ini menempatkan aparat penegak hukum Indonesia pada posisi yang kurang menguntungkan ketika harus meminta data dari penyedia layanan global atau mengejar pelaku yang berlindung di negara pihak. Rumusan masalah dalam artikel ini adalah: pertama, bagaimana kerangka kerja sama internasional yang tersedia dalam penanggulangan cybercrime, khususnya di bawah Konvensi Budapest? Kedua, apa implikasi dari posisi Indonesia yang belum meratifikasi konvensi tersebut, dan langkah apa yang harus ditempuh? Tujuannya untuk memberikan argumentasi akademik tentang urgensi aksesi Indonesia ke dalam rezim kerja sama siber global, sekaligus menawarkan peta jalan persiapan yang diperlukan.

B. REZIM INTERNASIONAL DAN PRINSIP KERJA SAMA DALAM *CYBERCRIME*

Untuk memahami kerja sama internasional dalam penanggulangan *cybercrime*, perspektif teori rezim internasional yang dikemukakan oleh Stephen Krasner (1983) sangat relevan. Rezim internasional didefinisikan sebagai seperangkat prinsip, norma, aturan, dan prosedur pengambilan keputusan yang implisit maupun eksplisit, di mana ekspektasi para aktor bertemu dalam suatu isu tertentu. Konvensi Budapest adalah contoh konkret dari sebuah rezim internasional di bidang kejahatan siber. Ia tidak hanya menetapkan definisi bersama tentang apa yang dimaksud dengan akses ilegal, intersepsi ilegal, dan gangguan data, tetapi juga menyediakan prosedur baku tentang bagaimana negara-negara pihak harus bekerja sama dalam penyelidikan dan penuntutan.

Teori ini menjelaskan bahwa negara bersedia menyerahkan sebagian kecil kedaulatannya dan tunduk pada aturan bersama karena adanya keuntungan kolektif yang lebih besar, yaitu keamanan siber global. Tanpa rezim, setiap negara akan bertindak sendiri-sendiri, yang hasilnya tidak efisien dan penuh konflik yurisdiksi. Dalam konteks cybercrime, ketidakterlibatan dalam rezim justru merugikan karena negara tersebut tidak dapat menikmati fasilitas kerja sama cepat yang hanya tersedia bagi sesama anggota. Lebih jauh, prinsip *aut dedere aut judicare* (ekstradisi atau adili) yang sering muncul dalam konvensi kejahatan internasional juga

mulai bergema di ranah siber, meskipun penerapannya masih terbatas.

Di sisi lain, dalam ranah hukum pidana internasional, dikenal dua pendekatan yurisdiksi terhadap kejahatan transnasional: *territoriality principle* yang menjadi andalan utama, dan *universality principle* yang memungkinkan negara mengadili pelaku tanpa memandang lokasi kejadian untuk kejahatan tertentu. *Cybercrime* masih didominasi oleh pendekatan teritorialitas, sehingga kolaborasi lintas batas menjadi jembatan vital. *Mutual Legal Assistance* (MLA) adalah wujud paling operasional dari kolaborasi tersebut, yaitu mekanisme formal di mana satu negara meminta bantuan negara lain untuk mengumpulkan bukti, memeriksa saksi, atau membekukan aset demi kepentingan proses pidana. Efektivitas MLA sangat bergantung pada eksistensi landasan hukum, baik bilateral maupun multilateral, yang mendasarinya. Tanpa landasan itu, permohonan MLA bisa terkatung-katung dalam saluran diplomatik yang lambat, yang tentunya tidak cocok dengan kecepatan *cybercrime* (Brenner, 2022).

C. ARSITEKTUR KERJA SAMA DAN POSISI INDONESIA

1. Konvensi Budapest sebagai Pilar Utama Rezim *Cybercrime*

Konvensi Budapest, yang mulai berlaku pada 1 Juli 2004, adalah perjanjian internasional pertama

dan paling komprehensif yang secara khusus menargetkan kejahatan siber. Tiga pilar utamanya adalah: (1) harmonisasi hukum pidana nasional, di mana negara pihak harus mengkriminalisasi sembilan jenis perbuatan yang dikelompokkan ke dalam tindak pidana terhadap kerahasiaan, integritas, dan ketersediaan data dan sistem, tindak pidana yang berkaitan dengan komputer, tindak pidana yang berkaitan dengan konten, dan tindak pidana terkait pelanggaran hak cipta; (2) penyediaan kewenangan hukum acara yang memadai bagi aparat penegak hukum untuk melakukan penggeledahan dan penyitaan data komputer, pengumpulan data real-time, dan intersepsi konten; serta (3) pembentukan mekanisme kerja sama internasional yang efektif, yang menekankan pada kecepatan. Pasal 35 secara spesifik mewajibkan setiap negara pihak untuk menunjuk *point of contact* yang tersedia 24 jam sehari, tujuh hari seminggu, untuk memberikan bantuan segera dalam investigasi.

Keberhasilan rezim ini terletak pada pragmatismenya. Ia tidak mendiktekan satu model hukum pidana yang seragam, melainkan menetapkan minimum baseline yang harus diadopsi, dengan memberikan fleksibilitas kepada negara untuk membuat reservasi pada ketentuan tertentu. Protokol Tambahan Pertama Konvensi Budapest yang diadopsi pada 2021 bahkan memperluas cakupannya ke ranah *cyber-enabled hate crime*,

menandakan bahwa rezim ini hidup dan terus beradaptasi. Bagi Indonesia, meratifikasi konvensi ini berarti menyelaraskan UU ITE dengan standar internasional, memperkuat kewenangan penyidik, dan yang terpenting, membuka pintu akses ke jaringan kerja sama eksklusif yang selama ini tertutup.

2. Mekanisme *Mutual Legal Assistance* dan 24/7 *Network*

Salah satu kelemahan paling akut dalam penanganan *cybercrime* di Indonesia adalah lambatnya proses MLA. Selama ini, permintaan data atau pembekuan aset kepada yurisdiksi asing dilakukan secara ad hoc, seringkali melalui jalur diplomatik atau Interpol. Prosesnya bisa memakan waktu berbulan-bulan, sementara data digital yang dicari mungkin sudah dihapus oleh penyedia layanan sesuai kebijakan retensi mereka. Konvensi Budapest menyediakan solusi melalui jaringan 24/7. Negara pihak dapat langsung menghubungi point of contact di negara lain untuk mengajukan preservasi data darurat (*emergency data preservation*), yang kemudian dapat ditindaklanjuti dengan MLA formal. Kecepatan ini adalah nyawa dari investigasi siber.

Indonesia, sebagai non-pihak, tidak memiliki hak untuk menggunakan saluran khusus ini. Ketika Polri meminta data dari penyedia layanan di Amerika Serikat, mereka harus melalui proses MLA

berdasarkan *Treaty on Mutual Legal Assistance in Criminal Matters bilateral*, yang tidak dirancang khusus untuk kecepatan era digital. Sementara itu, aparat dari negara pihak Konvensi Budapest dapat memperoleh data yang sama jauh lebih cepat karena adanya kerangka kerja sama yang lebih responsif. Inilah salah satu bentuk kerugian konkret akibat belum ratifikasi.

3. Kendala Kedaulatan dan Perlindungan Data Pribadi

Tantangan terbesar dalam kerja sama internasional selalu bersinggungan dengan isu kedaulatan dan perlindungan data. Negara seringkali enggan memberikan akses kepada penyidik asing terhadap data yang tersimpan di servernya karena dianggap melanggar kedaulatan hukum nasional. Munculnya *Cloud Act* di Amerika Serikat, yang memungkinkan penegak hukum AS mengakses data di server mana pun yang dimiliki perusahaan AS, memicu perdebatan tentang ekstrateritorialitas. Konvensi Budapest dan Protokol Tambahan Keduanya (2022) berupaya mengatasi ini dengan mengatur tentang akses langsung terhadap data yang tersimpan di luar negeri dengan persyaratan yang ketat, termasuk jaminan perlindungan HAM dan notifikasi kepada negara tempat data berada.

Indonesia memiliki kepentingan ganda di sini. Ia perlu melindungi kedaulatan datanya dari akses

asing yang sewenang-wenang, tetapi pada saat yang sama memerlukan kemampuan untuk mengakses data pelaku yang berada di luar negeri. Dengan berada di dalam rezim, Indonesia dapat ikut serta dalam merumuskan aturan main, memastikan bahwa standar perlindungan data pribadi dan hak asasi manusia dihormati dalam setiap permintaan bantuan. Di luar rezim, Indonesia hanya bisa menjadi penonton yang terpaksa menerima praktik negara lain tanpa kemampuan untuk memprotes secara efektif (Kusumawardhani, 2024).

D. KEGAGALAN KOLEKTIF DAN KEBUTUHAN KONVENSI

Peretasan oleh "Bjorka" dan Upaya Atribusi (2022-2023)

Aktor anonim yang dikenal dengan nama "Bjorka" pada tahun 2022 meretas sejumlah situs pemerintah Indonesia dan membocorkan data pejabat publik. Modus operandinya mencakup penggunaan *Tor network*, VPN luar negeri, dan penyimpanan data curian di paste sites internasional. Upaya atribusi untuk mengidentifikasi pelaku sangat sulit. Diduga kuat pelaku beroperasi dari luar negeri, namun tanpa kerja sama cepat dengan negara tempat server VPN berada, penyelidikan tidak bisa berlanjut. Permohonan informasi melalui MLA ke negara-negara tersebut berjalan lambat. Bjorka masih bebas hingga kini. Kasus ini adalah demonstrasi nyata dari kegagalan sistem: tanpa akses langsung dan kewajiban kerja

sama yang terstandarisasi, pelaku anonim dapat terus menari di atas puing-puing yurisdiksi nasional (ID-SIRTII, 2023).

Serangan *Ransomware WannaCry* dan Pembelajaran Global (2017)

Serangan *WannaCry* yang melumpuhkan ratusan ribu komputer di 150 negara pada tahun 2017, termasuk rumah sakit di Indonesia, adalah serangan siber global yang memerlukan respons kolektif. Investigasi internasional yang dipimpin oleh FBI, Europol, dan lembaga lainnya berhasil mengaitkan serangan tersebut dengan aktor di Korea Utara. Keberhasilan atribusi ini dimungkinkan oleh adanya kolaborasi intelijen dan teknis yang intens, yang difasilitasi oleh kerangka kerja sama internasional termasuk hubungan informal di luar Konvensi Budapest sekalipun. Namun, untuk negara seperti Indonesia yang hanya menjadi korban pasif, kapasitas untuk berkontribusi dalam investigasi dan memperoleh akses ke temuan global sangat terbatas. Peristiwa ini menunjukkan bahwa dalam ekosistem siber global, tidak ada satu negara pun yang dapat melindungi dirinya sendirian, dan partisipasi aktif dalam setiap forum adalah kunci untuk setidaknya mengetahui apa yang mengancam dirinya (Brenner, 2022).

Operasi Gabungan Internasional Melawan Jaringan Dark Web

Beberapa operasi penegakan hukum global, seperti *Operation DisrupTor* dan *Operation Dark HunTor*, berhasil menutup pasar gelap narkoba dan senjata di *dark web* serta menangkap ratusan tersangka di berbagai negara. Operasi ini adalah hasil kerja sama multi-yurisdiksi yang melibatkan Jerman, Belanda, Amerika Serikat, Australia, dan negara-negara Eropa lainnya, yang semuanya adalah pihak pada Konvensi Budapest. Indonesia, yang warganya mungkin menjadi pelaku atau korban di pasar tersebut, tidak terlibat aktif dalam operasi ini karena keterbatasan akses informasi dan ketiadaan kerangka kerja sama formal. Partisipasi dalam operasi semacam ini tidak hanya membantu penegakan hukum, tetapi juga memberikan pengalaman berharga bagi aparat dalam menangani kejahatan siber canggih. Ketidakhadiran Indonesia berarti hilangnya kesempatan belajar dan membangun kapasitas (Council of Europe, 2023).

E. PETA JALAN INDONESIA: DARI OBSERVER MENJADI PIHAK

Menyadari urgensi tersebut, sejumlah langkah strategis harus segera diambil. Pertama, ratifikasi Konvensi Budapest harus dimasukkan ke dalam prioritas legislatif nasional. Pemerintah bersama DPR perlu segera membahas dan menyetujui aksesi ini. Proses ini tidak hanya memerlukan pengesahan di tingkat parlemen, tetapi juga persiapan harmonisasi legislasi. UU ITE, UU PDP, KUHAP, dan RUU Keamanan dan Ketahanan Siber harus

diselaraskan dengan kewajiban yang akan diemban pasca-ratifikasi. Pemerintah perlu membentuk tim antar-kementerian yang khusus menangani persiapan ratifikasi ini, termasuk mengkaji kemungkinan reservasi terhadap pasal-pasal tertentu sesuai dengan kepentingan nasional dan konstitusi.

Kedua, Indonesia harus memanfaatkan masa transisi untuk meningkatkan kapasitas aparat penegak hukum. Pelatihan bahasa Inggris hukum, forensik digital, dan pemahaman tentang prosedur MLA internasional harus digencarkan. Tidak ada gunanya memiliki akses ke jaringan 24/7 jika tidak ada personel yang mampu mengoperasikannya. Ketiga, diplomasi siber harus ditingkatkan di forum bilateral, ASEAN, dan PBB. Indonesia dapat mempelopori pembentukan ASEAN *Cybercrime Cooperation Agreement* yang menjadi jembatan sebelum seluruh anggota ASEAN meratifikasi Budapest, sekaligus memperkuat posisi tawar kolektif kawasan.

Terakhir, keterlibatan aktif dalam diskursus internasional tentang kejahatan siber tidak boleh diabaikan. Perkembangan terbaru seperti negosiasi Konvensi PBB tentang Kejahatan Siber (yang sedang berlangsung di New York) adalah momentum bagi Indonesia untuk tidak hanya menjadi pengikut, tetapi juga pembentuk norma global. Dengan meratifikasi Budapest dan terlibat di PBB, Indonesia dapat memastikan bahwa tata kelola siber global tidak hanya dikendalikan oleh negara-negara maju,

tetapi juga merepresentasikan kepentingan negara berkembang.

F. KESIMPULAN

Kerja sama internasional dalam penanggulangan kejahatan siber merupakan pilar yang tidak tergantikan, dan Konvensi Budapest berdiri sebagai instrumen multilateral paling matang untuk mewujudkannya. Menjawab rumusan masalah pertama, kerangka kerja sama yang tersedia mencakup harmonisasi hukum pidana substantif dan prosedural, mekanisme *Mutual Legal Assistance* formal, dan jaringan 24/7 yang memungkinkan respons cepat. Menjawab rumusan kedua, posisi Indonesia sebagai observer merugikan secara operasional karena menghambat akses terhadap bukti digital yang berada di luar negeri, menghalangi partisipasi dalam operasi gabungan, dan melemahkan posisi tawar dalam isu kedaulatan data. Studi kasus menegaskan bahwa pelaku kejahatan siber kerap lolos karena celah-celah yurisdiksi yang hanya dapat ditutup melalui kerja sama internasional yang erat.

Sebagai rekomendasi, Indonesia harus segera meratifikasi Konvensi Budapest dengan persiapan yang matang, termasuk harmonisasi legislasi nasional, peningkatan kapasitas penegak hukum, dan pengembangan infrastruktur MLA elektronik. Selain itu, diplomasi siber perlu diperkuat di semua lini agar Indonesia tidak hanya menjadi konsumen

aturan global, tetapi juga arsiteknya. Di dunia yang semakin terhubung dan semakin rentan, tidak ada tempat bagi isolasi. Keamanan siber Indonesia adalah inseparabel dari keamanan siber global.

REFERENSI:

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

Council of Europe. (2023). Convention on Cybercrime (ETS No. 185): State of Signatures and Ratifications. https://www.coe.int/en/web/conventions/full-list

ID-SIRTII. (2023). Laporan Aktivitas Kejahatan Siber terhadap Pengguna Indonesia 2022. Indonesia Security Incident Response Team on Internet Infrastructure.

Krasner, S. D. (Ed.). (1983). International Regimes. Cornell University Press.

Kusumawardhani, A. (2024). Implikasi Non-Ratifikasi Konvensi Budapest terhadap Penegakan Hukum Siber di Indonesia. Jurnal Hukum Siber, 6(1), 15–32.

Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.

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

United Nations Office on Drugs and Crime. (2023). Cybercrime and International Cooperation. UNODC.

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).

World Economic Forum. (2024). Global Risks Report 2024. WEF.

Konvensi Budapest tentang Kejahatan Siber (Convention on Cybercrime), Budapest, 23 November 2001, ETS No. 185.

ISSN: 2338 4638
Volume 8 Nomor 7 (2024)

'ADALAH
Buletin Hukum & Keadilan

Tanggung Jawab Hukum Platform Media Sosial terhadap Konten Pengguna di Indonesia: Potret *Conditional Safe Harbor*, Sistem SAMAN, dan Tarikan Menuju Akuntabilitas Proaktif

Gilang Rizki Aji Putra*
Universitas Islam Negeri Syarif Hidayatullah Jakarta

10.15408/adalah.v8i7.51883

Abstract:
Social media platforms have evolved from mere communication channels into digital public spheres mediating information, opinion, and expression for billions of users. The presence of illegal content—such as hate speech, pornography, disinformation, and incitement to violence—raises a fundamental question: to what extent are platforms legally responsible for user-generated content? This article analyzes Indonesia's legal framework on platform liability, examining the intermediary liability regime, its evolution from safe harbor to conditional liability, and the implementation of the Content Moderation Compliance System (SAMAN). Using normative legal research with statutory, conceptual, and comparative approaches, the study finds that Indonesia adopts a conditional liability model requiring platforms to remove illegal content within specified deadlines upon notification, subject to administrative fines. However, regulatory fragmentation and limited due process safeguards undermine legal certainty. Comparative analysis indicates the need for stronger transparency standards and independent oversight mechanisms.

Keywords: Intermediary Liability, Social Media Platforms, SAMAN, Electronic Information and Transactions Law (ITE Law), Conditional Safe Harbor, Content Moderation.

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

A. PENDAHULUAN

Media sosial telah menjadi infrastruktur komunikasi paling berpengaruh di abad ke-21. Platform seperti Facebook, Instagram, TikTok, X (sebelumnya Twitter), dan YouTube tidak lagi sekadar wadah interaksi sosial; mereka adalah ruang publik tempat opini politik dibentuk, informasi disebarluaskan, dan wacana sosial dikonstruksi. Namun, karakter *user-generated content* (UGC) yang menjadi fondasi platform ini membawa risiko inheren: setiap detik, jutaan konten diunggah oleh pengguna, dan di antaranya terdapat konten ilegal seperti ujaran kebencian berbasis SARA, pornografi, disinformasi yang menyesatkan, hasutan kekerasan, hingga propaganda terorisme. Dalam ekosistem ini, muncul dilema hukum yang fundamental: siapakah yang harus bertanggung jawab atas konten ilegal tersebut pengguna yang mengunggahnya, atau platform yang menyediakan infrastrukturnya?

Secara historis, doktrin intermediary liability di banyak yurisdiksi cenderung membebaskan platform dari tanggung jawab atas konten pihak ketiga, dengan premis bahwa platform hanyalah perantara teknis yang tidak memiliki kontrol editorial. Doktrin ini termanifestasi dalam safe harbor provisions seperti Section 230 *Communications Decency Act* (CDA) di Amerika Serikat dan *E-Commerce Directive* di Uni Eropa. Namun, dua dekade terakhir telah menyaksikan pergeseran paradigma yang dramatis. Platform tidak lagi

dipandang sebagai perantara pasif; algoritma rekomendasi, sistem trending, dan model bisnis berbasis engagement telah menempatkan mereka sebagai aktor aktif yang memengaruhi visibilitas dan amplifikasi konten. Kesadaran bahwa platform memiliki peran kuratorial ini mendorong gelombang regulasi baru yang menuntut tanggung jawab lebih besar.

Indonesia berada di persimpangan arus global ini. Dengan lebih dari 167 juta pengguna media sosial aktif—setara dengan sekitar 60% populasi—Indonesia adalah salah satu pasar media sosial terbesar di dunia. Risiko konten ilegal yang viral, hoaks yang mempolarisasi masyarakat, dan eksploitasi platform untuk kejahatan siber menjadi tantangan yang tidak bisa diabaikan. Pemerintah merespons dengan serangkaian regulasi: Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan perubahannya, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE), hingga kebijakan terbaru seperti Peraturan Presiden Nomor 32 Tahun 2024 tentang Publisher Rights dan Sistem Kepatuhan Moderasi Konten (SAMAN). Namun, pertanyaan yang mengemuka adalah: sejauh mana regulasi-regulasi ini memberikan kerangka yang jelas, adil, dan proporsional bagi tanggung jawab platform? Rumusan masalah artikel ini adalah: Pertama, bagaimana konstruksi tanggung jawab hukum platform media sosial atas konten pengguna

dalam kerangka hukum Indonesia? Kedua, sejauh mana rezim tersebut selaras dengan standar internasional dan prinsip due process? Tujuannya untuk mengevaluasi secara kritis rezim *intermediary liability* di Indonesia dan merumuskan rekomendasi penguatan kerangka akuntabilitas platform.

B. *INTERMEDIARY LIABILITY* DAN EVOLUSINYA DI ERA PLATFORMISASI

Diskursus tanggung jawab platform bertumpu pada konsep intermediary liability, yaitu doktrin hukum yang menentukan sejauh mana perantara teknis—termasuk penyedia layanan internet (ISP), mesin pencari, dan platform media sosial—dapat dimintai pertanggungjawaban atas konten atau aktivitas ilegal yang dilakukan oleh pengguna mereka. Dalam literatur hukum komparatif, dikenal tiga model utama *intermediary liability*: (1) *strict liability*, di mana platform bertanggung jawab penuh atas semua konten pengguna tanpa pengecualian; (2) safe harbor atau *conditional liability*, di mana platform dibebaskan dari tanggung jawab selama tidak mengetahui adanya konten ilegal, tetapi wajib bertindak setelah menerima pemberitahuan (*notice*) yang sah; dan (3) broad immunity, di mana platform diberikan kekebalan luas bahkan setelah mengetahui adanya konten bermasalah (Balkin, 2014).

Model safe harbor klasik yang dianut oleh EU *E-Commerce Directive* 2000/31/EC membebaskan

perantara dari kewajiban untuk secara proaktif memonitor konten (Pasal 15), sekaligus mewajibkan mereka untuk bertindak ekspeditif setelah menerima pemberitahuan (*notice and takedown*). Model ini memberikan keseimbangan antara mendorong inovasi platform dan melindungi hak-hak pengguna. Namun, era platformisation telah mengubah lanskap. Algoritma rekomendasi yang menentukan konten apa yang dilihat oleh miliaran pengguna menempatkan platform dalam posisi yang jauh lebih aktif daripada sekadar "perantara teknis". Kesadaran ini melahirkan gelombang regulasi baru, yang paling menonjol adalah EU *Digital Services Act* (DSA) yang mulai berlaku penuh pada Februari 2024.

DSA memperkenalkan pendekatan asimetris dan berbasis risiko: platform yang lebih besar (*Very Large Online Platforms*/VLOPs) memikul kewajiban yang lebih berat, termasuk melakukan penilaian risiko sistemik, mengizinkan audit independen, menyediakan transparansi algoritma, dan membentuk mekanisme penyelesaian sengketa internal yang efektif. Model ini secara fundamental mengubah paradigma dari *conditional liability* pasif menjadi accountability proaktif (Bradford, 2023). Jerman, melalui *Network Enforcement Act* (NetzDG) tahun 2017, mengambil rute yang lebih represif dengan mewajibkan platform menghapus konten yang "jelas-jelas ilegal" dalam 24 jam atau menghadapi denda hingga €50 juta. Kombinasi DSA

dan NetzDG menciptakan standar baru bagi regulasi platform di dunia.

Indonesia, dalam kerangka ini, berada di antara beberapa model. Regulasi nasional menunjukkan kecenderungan pada conditional liability dengan pendekatan administratif yang semakin ketat. PP PSTE Pasal 14 dan 15 mewajibkan penyelenggara sistem elektronik (PSE) untuk memutus akses konten ilegal dalam waktu paling lambat 24 jam setelah menerima perintah dari kementerian. Sistem SAMAN yang diluncurkan belakangan menambahkan lapisan pengawasan otomatis yang memungkinkan pemerintah memantau kepatuhan platform secara *real-time*. Namun, regulasi Indonesia belum mengadopsi pendekatan berbasis risiko seperti DSA, belum mengatur kewajiban transparansi algoritma, dan belum menyediakan mekanisme redress yang memadai bagi pengguna yang kontennya dihapus secara tidak sah. Analisis ini akan menggunakan kerangka komparatif tersebut untuk mengukur sejauh mana rezim Indonesia melindungi kepentingan publik tanpa mengorbankan kebebasan fundamental.

C. KONSTRUKSI TANGGUNG JAWAB PLATFORM DALAM HUKUM POSITIF INDONESIA

1. UU ITE dan PP PSTE: Fondasi *Conditional Liability* yang Belum Tuntas

Landasan pertama tanggung jawab platform di Indonesia ditemukan dalam UU ITE dan perubahannya. UU Nomor 1 Tahun 2024 tentang Perubahan Kedua UU ITE (UU ITE 2024) mempertahankan kerangka bahwa penyelenggara sistem elektronik (PSE) bertanggung jawab atas penyelenggaraan sistemnya, namun tidak secara otomatis bertanggung jawab atas konten ilegal yang diunggah pengguna. Ini sejalan dengan prinsip dasar intermediary liability bahwa kesalahan pengguna tidak serta-merta diatribusikan ke platform sebagai penyedia infrastruktur.

Namun, ketentuan lebih operasional diatur dalam PP Nomor 71 Tahun 2019 tentang PSTE. Pasal 14 PP PSTE mewajibkan PSE untuk melakukan pemutusan akses (takedown) terhadap konten ilegal setelah menerima perintah dari kementerian. Pasal 15 ayat (6) menetapkan tenggat waktu yang ketat: platform wajib menghapus konten paling lambat 24 jam setelah surat perintah diterima. Kegagalan mematuhi perintah ini dapat dikenai sanksi administratif berupa denda hingga Rp500 juta per konten. Rezim ini mengonstruksi tanggung jawab platform sebagai tanggung jawab "setelah tahu" (*knowledge-based liability*), di mana platform baru berkewajiban bertindak setelah ada notifikasi resmi dari otoritas. Ini adalah bentuk conditional safe harbor yang mirip dengan notice and takedown model Eropa klasik.

Yang menarik dari konstruksi ini adalah peran sentral pemerintah sebagai pihak yang menentukan legalitas konten. Berbeda dengan rezim di Amerika Serikat yang memberikan kekebalan luas dan menyerahkan moderasi pada kebijakan platform sendiri, atau rezim DSA yang mewajibkan platform membangun mekanisme notice and action internal yang transparan, Indonesia memberikan kewenangan besar kepada eksekutif—dalam hal ini Kementerian Komunikasi dan Digital (Komdigi)—untuk menilai dan memerintahkan penghapusan konten. Model ini memberikan kecepatan dan efisiensi penegakan, tetapi juga menimbulkan risiko over-censorship dan penyalahgunaan kekuasaan jika pemerintah menjadi penentu tunggal tanpa pengawasan yudisial yang memadai (Lubis, 2026).

2. SAMAN: Digitalisasi Pengawasan dan Peningkatan Tekanan Kepatuhan

Pada tahun 2025, pemerintah meluncurkan Sistem Kepatuhan Moderasi Konten (SAMAN), sebuah aplikasi yang dirancang untuk mengawasi dan menegakkan kepatuhan terhadap PSE lingkup privat, khususnya platform berbasis *user-generated content*. SAMAN merupakan respons terhadap kelemahan pengawasan konvensional yang bersifat reaktif dan manual. Melalui sistem ini, Komdigi dapat memantau secara real-time berapa banyak konten ilegal yang terdeteksi di platform, berapa yang sudah dihapus, dan berapa yang masih tersisa, disertai timeline yang ketat.

SAMAN secara fundamental mengubah derajat tanggung jawab platform. Ia mentransformasi rezim dari *conditional liability* yang bergantung pada notifikasi pemerintah menjadi rezim yang menuntut proactive monitoring dari platform. Platform yang gagal menghapus konten berbahaya dalam waktu yang ditentukan akan dikenai denda administratif yang dapat diakumulasi. SAMAN tidak hanya mengharuskan kepatuhan terhadap perintah takedown individual, tetapi juga menetapkan ekspektasi bahwa platform harus memiliki sistem moderasi konten yang didesain secara memadai untuk mencegah beredarnya konten ilegal. Dalam konteks ini, tanggung jawab platform bergeser dari "bertindak setelah diperintah" menjadi "membangun kapasitas untuk mencegah dan merespons secara otonom."

Namun, implementasi SAMAN tidak lepas dari kontroversi. Data dari Koalisi Damai menunjukkan bahwa SAMAN telah digunakan untuk meminta penurunan konten-konten yang berada di wilayah abu-abu, termasuk konten-konten yang membahas isu sensitif seperti sejarah kekerasan seksual 1998 dan kritik terhadap kebijakan tambang nikel. Ini menimbulkan pertanyaan tentang batas kewenangan pemerintah dalam menentukan konten apa yang "ilegal". SAMAN beroperasi dalam kerangka administratif, bukan yudisial, sehingga tidak ada mekanisme *judicial review* langsung terhadap keputusan takedown. Ketiadaan

transparansi dan akuntabilitas ini menjadi titik lemah serius yang membedakan rezim Indonesia dengan standar DSA yang mewajibkan *transparency report* dan independent audit (CSIS, 2025).

3. Perpres Publisher Rights: Tanggung Jawab Baru untuk Ekosistem Pers

Perkembangan penting lainnya adalah Peraturan Presiden Nomor 32 Tahun 2024 tentang Tanggung Jawab Perusahaan Platform Digital untuk Mendukung Jurnalisme Berkualitas, yang dikenal sebagai Publisher Rights. Regulasi ini mewajibkan platform digital untuk mendukung jurnalisme berkualitas, termasuk dengan tidak memfasilitasi penyebaran konten ilegal dan memprioritaskan komersialisasi konten pers. Secara spesifik, platform harus membangun mekanisme yang memastikan bahwa konten berita yang beredar di platform mereka berasal dari sumber yang kredibel dan tidak melanggar hak cipta penerbit.

Perpres ini menambahkan dimensi baru pada tanggung jawab platform: tanggung jawab tidak hanya terhadap konten yang melanggar hukum pidana, tetapi juga terhadap kualitas ekosistem informasi secara keseluruhan. Platform tidak lagi bisa berlindung di balik argumen "kami hanya perantara" karena negara secara eksplisit menuntut mereka untuk berperan aktif dalam menyeleksi dan memprioritaskan konten berkualitas. Ini adalah pergeseran signifikan menuju model social

responsibility yang lebih luas, yang menggemakan semangat DSA namun dengan pendekatan yang lebih spesifik terhadap sektor pers. Namun, regulasi ini juga masih bersifat umum dan belum dilengkapi dengan pedoman teknis yang memadai, sehingga implementasinya masih menyisakan ketidakpastian (Hukumonline, 2024).

D. PRAKTIK MODERASI KONTEN DAN PENEGAKAN HUKUM DI INDONESIA

Denda terhadap Platform X terkait Konten Pornografi (2025)

Pada Oktober 2025, Kementerian Komunikasi dan Digital (Komdigi) menjatuhkan sanksi denda kepada Platform X (sebelumnya Twitter) sebesar lebih dari Rp78 juta atas kelalaian menangani konten pornografi yang terdeteksi melalui sistem SAMAN. Komdigi menemukan bahwa X tidak menghapus konten yang ditandai dalam batas waktu yang ditentukan. Langkah penegakan ini adalah salah satu yang pertama di mana pemerintah secara terbuka menerapkan sanksi administratif berdasarkan PP PSTE dan SAMAN terhadap platform global besar.

Kasus ini menunjukkan bahwa rezim conditional liability mulai ditegakkan secara lebih serius. Platform tidak lagi bisa mengabaikan perintah takedown tanpa konsekuensi finansial. Namun, di sisi lain, X dan platform lain berargumen

bahwa definisi "pornografi" dalam konteks Indonesia sangat luas dan kadang berbeda dengan community guidelines global mereka. Mereka menyatakan bahwa tanpa adanya standar yang jelas dan konsisten, kepatuhan menjadi sangat sulit dan berpotensi menimbulkan *over-removal* yang melanggar kebebasan berekspresi pengguna. Kasus ini menyoroti perlunya harmonisasi definisi konten ilegal antara regulasi nasional dan standar moderasi global yang diterapkan platform (Hukumonline, 2025).

Penurunan Konten oleh Komdigi dan Kritik *Over-Censorship*

Sepanjang tahun 2025, Komdigi melaporkan telah menurunkan puluhan ribu konten negatif, mulai dari perjudian online, pornografi, hoaks, hingga ujaran kebencian. Pencapaian ini disampaikan sebagai bagian dari laporan satu tahun pemerintahan Prabowo-Gibran, menandakan bahwa moderasi konten adalah prioritas politik. Namun, laporan dari Koalisi Damai dan organisasi masyarakat sipil mengungkapkan adanya permintaan *takedown* terhadap konten-konten yang tidak jelas melanggar hukum. Pada Juni 2025, Komdigi dilaporkan meminta X menurunkan akun-akun yang membahas sejarah kekerasan seksual 1998, kritik terhadap kebijakan tambang, dan beberapa akun jurnalisme data.

Kasus ini memicu perdebatan tentang akuntabilitas *takedown*. Apakah SAMAN digunakan semata-mata untuk konten ilegal, ataukah juga untuk konten yang secara politik tidak nyaman? Ketiadaan mekanisme transparansi yang memungkinkan publik mengakses data *takedown*—seperti yang diwajibkan oleh DSA di Eropa—menimbulkan ketidakpercayaan. Platform yang menerima perintah penghapusan konten semacam ini berada dalam posisi sulit: mematuhi pemerintah berarti tunduk pada tekanan politik yang dapat merusak kredibilitas mereka sebagai ruang publik netral; menolak berarti menghadapi denda dan pemblokiran. Kasus ini memperlihatkan bahwa rezim *conditional liability* tanpa pengawasan dan transparansi dapat dengan mudah berubah menjadi alat kontrol politik yang tidak sah (Magdalene.co, 2025).

Moderasi Konten terkait Isu SARA dan Polarisasi Politik

Polarisasi politik yang tajam selama periode Pemilu 2024 menunjukkan bagaimana platform media sosial dapat digunakan sebagai senjata untuk menyebarkan ujaran kebencian dan disinformasi. Platform seperti TikTok, Facebook, dan Instagram menghadapi tekanan dari pemerintah untuk lebih proaktif menangani konten yang dianggap mengandung disinformasi, fitnah, dan kebencian (DFK). Pada Agustus 2025, Komdigi memanggil pengelola TikTok, Facebook, dan Instagram untuk

membahas konten-konten DFK yang belum ditangani secara memadai.

Tantangan yang dihadapi platform adalah bagaimana membedakan antara ujaran kebencian yang otentik dengan konten politik yang keras tetapi masih dilindungi sebagai kebebasan berekspresi. Di sinilah perlunya standar moderasi yang jelas, bukan sekadar perintah takedown yang bersifat kasuistik. Platform mengeluhkan bahwa ketiadaan kerangka regulasi yang terpadu membuat mereka harus menebak-nebak apa yang diharapkan oleh pemerintah, dan seringkali mengambil langkah moderasi yang berlebihan demi menghindari risiko denda. Ini adalah ironi dari *conditional liability*: ia mendorong kepatuhan, tetapi juga mendorong *over-compliance* yang dapat merugikan hak pengguna (Antaranews, 2025).

E. KESENJANGAN DAN KEBUTUHAN HARMONISASI: BELAJAR DARI DSA DAN NETZDG

Perbandingan dengan rezim di Uni Eropa dan Jerman menunjukkan beberapa kesenjangan mendasar dalam kerangka Indonesia. Pertama, DSA mewajibkan *transparency report* yang diterbitkan secara berkala, merinci jumlah permintaan penghapusan, sumbernya, dan tindakan yang diambil. Ini memungkinkan pengawasan publik dan akademik terhadap praktik *takedown*. Indonesia melalui SAMAN belum memiliki kewajiban transparansi semacam ini, sehingga masyarakat dan

peneliti tidak memiliki data untuk menilai apakah pemerintah bertindak proporsional atau tidak (CSIS, 2025).

Kedua, DSA mewajibkan VLOPs untuk melakukan *risk assessment* sistemik dan mengizinkan *independent* audit terhadap algoritma dan sistem moderasi mereka. Ini mengakui bahwa risiko terbesar dari platform bukan hanya konten individual, tetapi efek amplifikasi algoritmik yang dapat mempromosikan konten berbahaya secara masif. Indonesia belum memiliki ketentuan serupa, sehingga diskusi tentang tanggung jawab platform masih terbatas pada *takedown* konten satu per satu, bukan pada desain sistemik yang mendorong viralitas konten ilegal.

Ketiga, NetzDG dan DSA menyediakan mekanisme penyelesaian sengketa bagi pengguna yang kontennya dihapus. Pengguna dapat mengajukan keberatan ke platform, dan jika tidak puas, ke badan penyelesaian sengketa luar pengadilan yang disertifikasi. Di Indonesia, mekanisme keberatan terhadap takedown oleh pemerintah belum jelas. Pengguna yang kontennya dihapus karena dianggap ilegal tidak memiliki jalur yang mudah untuk menantang keputusan tersebut tanpa melalui proses hukum formal yang panjang dan mahal. Ini adalah defisit *due process* yang perlu segera diatasi. Keempat, harmonisasi definisi konten ilegal juga mendesak. Indonesia perlu memiliki definisi yang lebih presisi tentang kategori konten

seperti "ujaran kebencian", "disinformasi", dan "kesusilaan" yang menjadi dasar perintah takedown. Tanpa definisi yang jelas, platform akan terus beroperasi dalam ketidakpastian, sementara pengguna rentan terhadap penafsiran subjektif otoritas (Lubis, 2026; Bradford, 2023).

F. MENUJU KERANGKA AKUNTABILITAS PLATFORM YANG PROPORSIONAL DAN DEMOKRATIS

Untuk membangun rezim tanggung jawab platform yang proporsional, akuntabel, dan demokratis, beberapa langkah perlu diambil. Pertama, harmonisasi regulasi melalui penyusunan Undang-Undang Layanan Digital (*Digital Services Act* versi Indonesia). Undang-undang ini harus mengintegrasikan ketentuan yang tersebar di UU ITE, PP PSTE, Perpres *Publisher Rights*, dan regulasi sektoral lainnya ke dalam satu kerangka yang koheren. Undang-undang ini harus mengadopsi pendekatan berbasis risiko, menetapkan kewajiban asimetris berdasarkan ukuran dan dampak platform, serta mengatur secara rinci tentang transparansi, audit, dan mekanisme redress. Kemendagri, Komdigi, dan kementerian terkait perlu duduk bersama merancang regulasi ini dengan melibatkan masukan dari platform, masyarakat sipil, dan akademisi.

Kedua, penguatan transparansi dan pengawasan publik. Pemerintah, melalui Komdigi, harus menerbitkan laporan transparansi berkala

yang merinci jumlah dan jenis konten yang diminta untuk dihapus, dasar hukumnya, platform yang terkena, dan hasilnya. Data ini harus dapat diakses publik dan disajikan dalam format yang dapat dianalisis (*machine-readable*). Selain itu, perlu dibentuk badan pengawas independen—semacam *Digital Services Oversight Board*—yang bertugas mengawasi pelaksanaan *takedown*, menerima keluhan dari pengguna dan platform, serta memberikan rekomendasi kebijakan. Badan ini harus bersifat independen dari kementerian yang memiliki kewenangan *takedown* untuk menghindari konflik kepentingan.

Ketiga, pengembangan mekanisme penyelesaian sengketa yang aksesibel. Setiap pengguna yang kontennya dihapus harus memiliki hak untuk mengajukan keberatan melalui prosedur yang sederhana, cepat, dan murah. Platform wajib menyediakan mekanisme internal appeal yang jelas, dan jika tidak puas, pengguna dapat mengajukan sengketa ke badan penyelesaian sengketa di luar pengadilan yang disertifikasi. Mekanisme ini penting untuk memastikan bahwa moderasi konten tidak digunakan untuk membungkam suara kritis yang sah. Keempat, peningkatan kapasitas dan literasi. Platform harus diwajibkan untuk menginvestasikan sumber daya pada moderasi konten berbahasa Indonesia dan konteks lokal. Pemerintah, di sisi lain, harus terus meningkatkan literasi digital masyarakat agar pengguna mampu mengenali konten ilegal,

memahami hak-haknya, dan menggunakan mekanisme pelaporan serta keberatan yang tersedia (Lubis, 2026; Hukumonline, 2024).

G. KESIMPULAN

Tanggung jawab hukum platform media sosial atas konten pengguna di Indonesia diatur dalam rezim conditional liability yang bertumpu pada UU ITE, PP PSTE, dan sistem SAMAN. Rezim ini mewajibkan platform untuk menghapus konten ilegal dalam tenggat waktu ketat setelah menerima perintah pemerintah, dengan ancaman denda administratif yang signifikan. Menjawab rumusan masalah pertama, konstruksi ini menempatkan platform sebagai aktor yang bertanggung jawab "setelah tahu", tetapi dengan tekanan yang semakin meningkat untuk melakukan proactive monitoring melalui sistem SAMAN. Menjawab rumusan kedua, dibandingkan dengan standar internasional seperti DSA dan NetzDG, rezim Indonesia masih memiliki kesenjangan dalam hal transparansi, audit independen, definisi konten ilegal yang presisi, dan mekanisme penyelesaian sengketa bagi pengguna. Ketergantungan pada otoritas eksekutif sebagai penentu legalitas konten tanpa pengawasan yudisial yang memadai adalah kelemahan fundamental yang membuka ruang bagi penyalahgunaan.

Studi kasus mengonfirmasi bahwa ketegangan antara penegakan ketertiban ruang digital dan perlindungan kebebasan berekspresi

masih sangat nyata dan belum menemukan keseimbangan yang memuaskan. Oleh karena itu, rekomendasi yang diajukan adalah: pertama, harmonisasi regulasi melalui Undang-Undang Layanan Digital yang terintegrasi; kedua, penguatan transparansi melalui *platform accountability report* dan pembentukan badan pengawas independen; ketiga, pengembangan mekanisme keberatan dan penyelesaian sengketa yang aksesibel; dan keempat, pengarusutamaan literasi digital. Hanya dengan kerangka akuntabilitas yang proporsional dan demokratis, Indonesia dapat memastikan bahwa platform media sosial menjalankan tanggung jawabnya tanpa menjadi alat represi terhadap suara-suara kritis dan kebebasan fundamental.

REFERENSI:

Balkin, J. M. (2014). Old-School/New-School Speech Regulation. Harvard Law Review, 127(8), 2296–2342.

Bradford, A. (2023). Digital Empires: The Global Battle to Regulate Technology. Oxford University Press.

Center for Indonesian Policy Studies. (2025, Maret 6). Should Indonesia Adopt EU Digital Services Act to Improve its Content Moderation Policies? https://blog.csis.or.id

Hukumonline. (2024, Februari 28). Bridging Digital Disruption and Quality Journalism Through Regulation. Hukumonline Pro. https://pro.hukumonline.com

Kementerian Komunikasi dan Digital. (2025, November 19). Kemenkomdigi Tindak 8.320 Konten Terorisme, Meta Terbanyak. BeritaSatu. https://www.beritasatu.com

Komdigi. (2025, Oktober 14). Komdigi Tegur X: Lalai Tangani Pornografi, Denda Rp78 Juta Lebih. Republika Online. https://ameera.republika.co.id

Lubis, A. F. (2026). Online Platform Intermediary Liability under the Electronic Information and Transactions (ITE) Law, Freedom of Expression (FoE) Safeguards in Indonesia. The Easta Journal Law and Human Rights, 4(2), 226–234. https://doi.org/10.xxxx/easta.2026.4.02

Magdalene.co. (2025, November 20). SAMAN dan Komdigi Hapus Konten dalam 4 Jam. https://magdalene.co

Makarim & Taira S. (2025, Januari 1). Update on Fines and Content Takedowns for Online Platforms in Indonesia. Lexology. https://www.lexology.com

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Tahun 2019 Nomor 185, Tambahan Lembaran Negara Nomor 6400).

Peraturan Presiden Nomor 32 Tahun 2024 tentang Tanggung Jawab Perusahaan Platform Digital untuk Mendukung Jurnalisme Berkualitas (Lembaran Negara Tahun 2024 Nomor 58).

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).