'ADALAH
Buletin Hukum & Keadilan

ISSN: 2338 4638

Volume 7 Nomor 7 (2023)

Kejahatan Siber (Cybercrime) dan Tantangan Penegakan Hukum di Era Digital

ISSN: 2338 4638

Volume 7 Nomor 7 (2023)

'ADALAH

Buletin Hukum & Keadilan

Tipologi Kejahatan Siber dan Penanggulangannya di Indonesia: Klasifikasi, Modus Operandi, dan Evaluasi Kerangka Hukum dalam Menghadapi Ancaman Digital Kontemporer

Gilang Rizki Aji Putra[*]

Universitas Islam Negeri Syarif Hidayatullah Jakarta

10.15408/adalah.v7i7.51838

Abstract:

Cybercrime has evolved from simple hacking into a multidimensional, organized criminal industry operating across jurisdictions. This article aims to classify the typology of cybercrime in Indonesia, analyze emerging modus operandi, and evaluate the effectiveness of existing legal and institutional frameworks in addressing these threats. Using a normative legal research method with typological, statutory, and case study approaches, the study identifies seven major categories of cybercrime in Indonesia, each with distinct technical characteristics and social impacts. The findings reveal that the national regulatory framework remains sectoral and reactive, failing to anticipate crime hybridization and the use of anonymization technologies such as cryptocurrency and the dark web. Case analyses of online fraud, ransomware, and online child sexual exploitation demonstrate a gap between law enforcement capacity and offender sophistication. The study concludes that combating cybercrime requires multidimensional strategies integrating digital forensics, international cooperation, and platform regulation.

Keywords: Cybercrime, Typology, Electronic Information and Transactions Law (ITE Law), Law Enforcement, 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

Perkembangan teknologi informasi dan komunikasi telah melahirkan dimensi kriminalitas baru yang tidak lagi terbatas oleh ruang dan waktu. Kejahatan siber, yang pada awalnya dipandang sebagai anomali, kini telah menjadi ancaman serius bagi keamanan nasional, stabilitas ekonomi, dan perlindungan warga negara. Indonesia, dengan lebih dari 200 juta pengguna internet, merupakan salah satu pasar digital terbesar sekaligus target paling rentan bagi pelaku kejahatan siber. Data dari Kepolisian Republik Indonesia mencatat peningkatan signifikan laporan kejahatan siber setiap tahunnya, dengan kerugian finansial yang mencapai triliunan rupiah (Bareskrim Polri, 2023).

Kejahatan siber memiliki karakteristik yang membedakannya dari kejahatan konvensional. Ia bersifat borderless, anonim, dan dapat dilakukan secara otomatis dalam skala masif. Pelaku tidak perlu hadir secara fisik di lokasi korban, cukup dengan koneksi internet dan perangkat lunak berbahaya. Lebih dari itu, lanskap kejahatan siber terus bermutasi seiring dengan inovasi teknologi. Jika satu dekade lalu ancaman utama adalah *virus* dan *worm*, kini ancaman telah berkembang menjadi *ransomware*, serangan terhadap rantai pasok (*supply chain attack*), penyalahgunaan kecerdasan buatan untuk *deepfake*, hingga kejahatan berbasis kriptografi. Kompleksitas ini menuntut adanya pemahaman

taksonomi yang jelas untuk merumuskan strategi penanggulangan yang efektif (Brenner, 2022).

Sayangnya, kerangka hukum dan kelembagaan penanggulangan kejahatan siber di Indonesia belum sepenuhnya adaptif. Regulasi seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan perubahannya memang menyediakan dasar pemidanaan, tetapi cakupannya masih terbatas pada delik-delik tertentu dan belum mengantisipasi modus-modus baru secara komprehensif. Di sisi lain, kapasitas teknis aparat penegak hukum masih belum merata, sementara koordinasi antarlembaga masih terfragmentasi. Rumusan masalah artikel ini adalah: Pertama, bagaimana tipologi kejahatan siber yang berkembang di Indonesia berdasarkan karakteristik dan modus operandinya? Kedua, bagaimana efektivitas kerangka penanggulangan yang ada saat ini dan apa langkah strategis yang diperlukan? Tujuannya untuk menyusun klasifikasi yang koheren sebagai dasar evaluasi kebijakan dan perumusan strategi penanggulangan yang lebih komprehensif.

B. KLASIFIKASI KEJAHATAN SIBER DAN PENDEKATAN PENANGGULANGAN

Untuk memetakan kejahatan siber secara sistematis, literatur internasional menawarkan beberapa skema klasifikasi. Salah satu yang paling berpengaruh adalah kerangka yang dikembangkan

oleh David Wall (2007) yang membagi kejahatan siber menjadi empat kategori: (1) cyber-trespass, yaitu pelanggaran terhadap sistem atau jaringan seperti peretasan; (2) *cyber-deception and theft*, yaitu penipuan dan pencurian daring termasuk pencurian identitas; (3) *cyber-pornography and obscenity*, mencakup konten ilegal dan eksploitasi seksual; serta (4) *cyber-violence*, yaitu tindakan yang menimbulkan kerugian psikologis seperti perundungan dan ujaran kebencian.

Klasifikasi lain yang lebih teknis diajukan oleh Konvensi Budapest tentang Kejahatan Siber (2001), yang membagi kejahatan siber ke dalam empat kelompok besar: (a) tindak pidana terhadap kerahasiaan, integritas, dan ketersediaan data dan sistem komputer; (b) tindak pidana yang berkaitan dengan komputer; (c) tindak pidana yang berkaitan dengan konten; dan (d) tindak pidana yang berkaitan dengan pelanggaran hak cipta dan hak terkait. Klasifikasi ini menjadi rujukan bagi banyak negara, termasuk Indonesia yang saat ini masih berstatus sebagai observer dalam *Convention Committee on Cybercrime.*

Dari perspektif penanggulangan, literatur membedakan antara pendekatan represif (penegakan hukum pidana), pendekatan preventif (keamanan sistem dan edukasi), dan pendekatan kolaboratif (kemitraan publik-swasta dan kerjasama internasional). Teori nodal governance menekankan bahwa keamanan siber tidak dapat diwujudkan oleh

negara sendirian; ia memerlukan jaringan kolaborasi antara pemerintah, industri, akademisi, dan masyarakat sipil (Shearing & Wood, 2003). Kerangka ini akan digunakan untuk mengevaluasi sejauh mana penanggulangan kejahatan siber di Indonesia bersifat multi-dimensi atau masih terpaku pada logika represif semata.

C. TIPOLOGI KEJAHATAN SIBER DI INDONESIA DAN MODUS OPERANDINYA

Berdasarkan analisis terhadap data kepolisian, putusan pengadilan, dan laporan lembaga riset keamanan siber, kejahatan siber di Indonesia dapat diklasifikasikan ke dalam tujuh tipologi utama:

1. Peretasan dan Akses Ilegal (*Hacking and Unauthorized Access*)

Ini adalah bentuk paling klasik dari kejahatan siber yang diatur dalam Pasal 30 UU ITE. Pelaku melakukan akses tanpa hak ke sistem komputer atau jaringan. Motivasinya bervariasi, mulai dari sekadar pembuktian kemampuan (*bragging rights*), pencurian data (*data breach*), hingga sabotase politik (hacktivism). Kasus peretasan terhadap situs-situs pemerintah dan lembaga pendidikan oleh kelompok seperti "Bjorka" dan "Anonymous Indonesia" menunjukkan bahwa sektor publik masih memiliki kerentanan tinggi. Modus yang sering digunakan termasuk SQL *injection*, *cross-site scripting*, dan eksploitasi kerentanan perangkat lunak yang belum

ditambal. Ironisnya, banyak serangan yang berhasil disebabkan oleh kelalaian mendasar seperti penggunaan kata sandi default atau absennya pembaruan keamanan (ID-SIRTII, 2023).

2. Penipuan Daring (*Online Fraud*)

Penipuan daring merupakan salah satu kejahatan siber dengan volume tertinggi di Indonesia. Tipologi ini mencakup *phishing*, *social engineering*, penipuan investasi bodong, undian palsu, dan *romance scam*. Pelaku menggunakan manipulasi psikologis untuk memperoleh data pribadi atau uang. Modus *phishing* mengalami evolusi dari sekadar email palsu menjadi *smishing* (SMS *phishing*) dan *vishing* (*voice phishing*). Penipuan berkedok investasi menggunakan trading *binary option* dan robot trading ilegal juga telah merugikan ratusan ribu korban. Keberadaan *platform* media sosial dan pesan instan mempermudah pelaku menjangkau korban secara masif. Pasal 28 ayat (1) UU ITE yang mengatur berita bohong dan penyesatan seringkali digunakan sebagai dasar penindakan, namun karakter transnasional dari sindikat penipuan daring menyulitkan pelacakan dan penangkapan (Mulyadi, 2023).

3. Kejahatan Konten Ilegal (*Illicit Content Offenses*)

Kejahatan ini meliputi penyebaran konten pornografi, khususnya pornografi anak, konten bermuatan SARA, dan ujaran kebencian. Indonesia

memiliki kerangka hukum ganda melalui UU ITE, UU Pornografi, dan UU Perlindungan Anak. Eksploitasi seksual anak daring merupakan sub-tipologi yang sangat memprihatinkan. Pelaku menggunakan media sosial, game daring, dan platform komunikasi terenkripsi untuk merekrut korban dan mendistribusikan materi pelecehan. Laporan dari *National Center for Missing and Exploited Children* (NCMEC) menempatkan Indonesia sebagai salah satu negara dengan volume pelaporan konten kekerasan seksual anak daring tertinggi di Asia Tenggara (ECPAT Indonesia, 2022). Tantangan utama dalam penanggulangan tipologi ini adalah penggunaan *enkripsi end-to-end* yang menyulitkan intersepsi, serta lambatnya proses takedown konten oleh platform global.

4. Pencurian Data dan Perdagangan Data Ilegal (*Data Theft and Trafficking*)

Dengan berlakunya UU PDP, pencurian dan perdagangan data pribadi kini memiliki rezim hukum yang lebih spesifik. Namun, praktik ini sudah lama menjadi sub-ekonomi gelap (*dark economy)* di Indonesia. Data pelanggan, nomor telepon, hingga data kependudukan diperjualbelikan secara bebas di forum-forum gelap dan grup pesan instan. Modusnya meliputi scraping otomatis terhadap basis data yang rentan, *insider threat* (karyawan yang mencuri data), dan pembelian data dari sesama pelaku kejahatan. Data yang dicuri kemudian digunakan untuk penipuan, pembobolan

rekening, hingga pemerasan. Meskipun secara normatif melanggar UU ITE dan UU PDP, penegakan hukum terhadap pencurian data masih sangat minim karena sulitnya melacak asal-usul data di pasar gelap dan rendahnya pelaporan dari korporasi yang enggan mengakui kebocoran (Pratiwi & Nugroho, 2023).

5. Serangan Ransomware dan Pemerasan Digital (*Ransomware and Digital Extortion*)

Ransomware adalah jenis *malware* yang mengenkripsi data korban dan menuntut tebusan agar data dipulihkan. Di Indonesia, serangan ini tidak hanya menargetkan korporasi besar, tetapi juga instansi pemerintahan dan fasilitas kesehatan. Pusat Data Nasional (PDN) sempat menjadi target serangan siber, yang meskipun detailnya tidak diungkapkan sepenuhnya, menandakan ancaman serius terhadap kedaulatan data. Modus terbaru adalah *double extortion*, di mana pelaku tidak hanya mengenkripsi data tetapi juga mencuri dan mengancam akan mempublikasikannya jika tebusan tidak dibayar. Pembayaran tebusan umumnya diminta dalam bentuk mata uang kripto yang sulit dilacak. Tantangan dalam penanggulangan ransomware adalah penggunaan infrastruktur anonim seperti TOR dan jaringan botnet yang tersebar di berbagai negara, sehingga memerlukan kerjasama internasional yang intensif (Siregar, 2024).

6. Serangan terhadap Infrastruktur Kritis (*Critical Infrastructure Attacks*)

Tipologi ini menyasar sistem yang vital bagi keberlangsungan negara, seperti jaringan listrik, transportasi, perbankan, dan telekomunikasi. Meskipun belum terjadi insiden katastrofik di Indonesia, beberapa serangan terhadap perbankan dan lembaga keuangan menunjukkan potensi eskalasi. Serangan *Distributed Denial of Service* (DDoS) yang melumpuhkan layanan perbankan daring, serta upaya peretasan terhadap sistem pembayaran, merupakan contoh konkret. Ancaman ini semakin nyata dengan meningkatnya konektivitas IoT di sektor industri (Industrial IoT). Pengaturan mengenai perlindungan infrastruktur informasi vital telah diatur dalam Peraturan Pemerintah dan Peraturan BSSN, namun pengawasan dan standar keamanan yang ketat masih dalam tahap pengembangan (BSSN, 2023).

7. Kejahatan Siber Baru Berbasis AI dan *Deepfake*

Tipologi termutakhir yang mulai terdeteksi adalah penggunaan kecerdasan buatan untuk kejahatan. *Deepfake*, yaitu teknologi yang dapat memanipulasi video dan suara sehingga tampak asli, mulai digunakan untuk penipuan dan disinformasi. Kasus penipuan dengan menyamar sebagai eksekutif perusahaan menggunakan suara tiruan hasil AI

sudah terjadi secara global dan diperkirakan akan segera merambah Indonesia. Selain itu, penyalahgunaan AI generatif untuk menciptakan konten pelecehan seksual non-konsensual juga menjadi ancaman baru. Regulasi di Indonesia belum secara spesifik mengatur pertanggungjawaban pidana terhadap konten yang dihasilkan oleh AI, sehingga terdapat celah hukum yang serius (Kusumawardhani, 2024).

D. ANTARA REGULASI DAN REALITAS

Penanggulangan kejahatan siber di Indonesia bertumpu pada beberapa pilar: regulasi, kelembagaan, kapasitas teknis, dan kerjasama internasional. Pada aspek regulasi, UU ITE telah beberapa kali direvisi, tetapi cakupannya masih terasa kurang adaptif. Beberapa ketentuan seperti Pasal 30 (akses ilegal) dan Pasal 32 (manipulasi data) sudah cukup memadai untuk kejahatan tradisional, tetapi belum mengantisipasi ransomware sebagai delik yang spesifik atau penyalahgunaan AI. UU PDP dan UU Terorisme menambahkan lapisan norma, tetapi fragmentasi ini justru menciptakan kebingungan yurisdiksi. Ratifikasi Konvensi Budapest yang telah lama didiskusikan belum juga terealisasi, sehingga kerjasama internasional dalam penanganan kejahatan siber masih bersifat ad hoc.

Dari segi kelembagaan, terdapat tumpang tindih kewenangan antara Bareskrim Polri (Dittipidsiber), BSSN, Kominfo, dan lembaga

lainnya. Masing-masing memiliki mandat yang berbeda, tetapi koordinasi di lapangan seringkali tidak mulus. Keberadaan BSSN sebagai otoritas keamanan siber nasional merupakan langkah maju, namun fungsi penegakan hukum tetap berada di kepolisian, sementara BSSN lebih fokus pada respons insiden dan audit. Kapasitas penyidik siber juga masih terbatas secara kuantitas dan kualitas. Menurut data Mabes Polri, jumlah penyidik siber yang memiliki sertifikasi forensik digital internasional masih sangat minim dibandingkan dengan beban kasus yang masuk (Santoso, 2023).

Satu persoalan krusial adalah kesenjangan kecepatan antara aksi kejahatan dan respons penegakan hukum. Ketika pelaku dapat mentransfer aset kripto dalam hitungan detik, aparat masih bergulat dengan birokrasi pembekuan rekening yang memakan waktu berhari-hari. Ketika konten pelecehan seksual anak tersebar luas dalam hitungan jam, mekanisme takedown masih bergantung pada itikad baik platform asing. Hal ini menegaskan bahwa penanggulangan yang hanya bersifat reaktif dan bertumpu pada pidana tidak akan mencukupi.

E. TIGA WAJAH KEJAHATAN SIBER DI INDONESIA

Sindikat *Scamming* Lintas Negara "Kampung Soetta"

Pada tahun 2022, Polri membongkar sindikat penipuan daring yang beroperasi dari kawasan Kampung Melayu, Jakarta Timur, yang menargetkan

warga negara asing. Modusnya adalah romance scam dan penipuan investasi menggunakan platform digital. Sindikat ini dikelola secara hierarkis dengan pembagian peran yang rapi: operator, penerjemah, dan penarik dana. Kasus ini menunjukkan bahwa Indonesia tidak hanya menjadi korban, tetapi juga menjadi basis operasi bagi sindikat kejahatan siber internasional. Penanganannya memerlukan kerjasama dengan kepolisian negara korban, namun ekstradisi dan pertukaran informasi masih terkendala birokrasi.

Serangan *Ransomware* terhadap Pusat Data Nasional (2024)

Serangan terhadap Pusat Data Nasional Sementara (PDNS) yang terjadi pada Juni 2024 menjadi *wake-up call* bagi keamanan siber nasional. Pelaku menggunakan varian *ransomware* yang dikenal sebagai *Brain Cipher*, yang tidak hanya mengenkripsi data tetapi juga menuntut tebusan. Insiden ini melumpuhkan sejumlah layanan publik dan menunjukkan kerentanan infrastruktur digital pemerintah. Respons pemerintah adalah menolak membayar tebusan dan berupaya memulihkan data dari cadangan, namun sebagian data dinyatakan tidak dapat dipulihkan. Kasus ini mengekspos kelemahan dalam manajemen keamanan siber, termasuk tata kelola pencadangan data dan protokol respons insiden. Dari perspektif hukum, tantangannya adalah mengidentifikasi pelaku yang menggunakan teknik anonimisasi canggih, serta

pertanyaan tentang akuntabilitas pengelola sistem yang lalai (Nugroho, 2024).

Eksploitasi Seksual Anak Daring melalui Game Online

Sepanjang tahun 2023, KPAI dan ECPAT mencatat peningkatan kasus grooming dan eksploitasi seksual anak melalui *platform game* daring yang memiliki fitur obrolan. Pelaku dewasa mendekati anak dengan menyamar sebagai teman sebaya, kemudian secara bertahap meminta konten eksplisit. *Platform game* seringkali tidak memiliki sistem verifikasi usia yang ketat dan responsif terhadap pelaporan. Meskipun terdapat UU Perlindungan Anak dan UU Pornografi, penegakannya terhadap *platform* yang servernya berada di luar negeri sangat sulit. Kasus ini menegaskan bahwa keamanan anak di ruang digital memerlukan kerjasama lintas sektor dan kewajiban hukum yang lebih keras bagi penyelenggara platform (ECPAT Indonesia, 2023).

F. DARI REPRESI MENUJU KETAHANAN SIBER

Menghadapi kompleksitas kejahatan siber, Indonesia perlu mengadopsi strategi penanggulangan yang bergeser dari dominasi pendekatan represif menuju model ketahanan siber yang holistik. Pertama, pembentukan Satuan Tugas Siber Nasional yang berada langsung di bawah Presiden dapat menjadi solusi untuk mengatasi

fragmentasi kelembagaan. Satgas ini bertugas mengkoordinasikan aspek pencegahan, deteksi dini, respons insiden, dan penegakan hukum, dengan melibatkan BSSN, Polri, Kominfo, Kejaksaan, serta unsur swasta dan akademisi.

Kedua, pengembangan kapasitas forensik digital harus dipercepat. Laboratorium forensik digital di tingkat daerah perlu diperbanyak dan dilengkapi dengan perangkat analisis terkini. Pelatihan berkelanjutan bagi penyidik siber mengenai investigasi mata uang kripto, analisis *dark web*, dan penanganan bukti digital harus menjadi prioritas. Ketiga, ratifikasi Konvensi *Budapest* tidak bisa ditunda lebih lama lagi. Aksesi terhadap konvensi ini akan memberikan kerangka hukum untuk kerjasama internasional, termasuk ekstradisi, bantuan hukum timbal balik, dan akses terhadap infrastruktur 24/7 *network* untuk kontak darurat siber.

Keempat, regulasi *platform* harus diperketat. *Platform digital* yang menyediakan layanan di Indonesia harus diwajibkan memiliki perwakilan hukum dan mematuhi batas waktu takedown konten ilegal yang tegas. Kelima, edukasi dan literasi digital harus menjadi gerakan nasional yang berkelanjutan, menanamkan kesadaran akan modus kejahatan dan cara perlindungannya sejak usia dini. Pendekatan pencegahan yang melibatkan komunitas dan institusi pendidikan akan mengurangi jumlah

korban secara signifikan dalam jangka panjang (Simanjuntak, 2024).

G. KESIMPULAN

Kejahatan siber di Indonesia telah berkembang menjadi fenomena multi-wajah dengan tujuh tipologi utama yang mencakup peretasan, penipuan, konten ilegal, pencurian data, *ransomware*, serangan infrastruktur kritis, dan kejahatan berbasis AI. Masing-masing tipologi menunjukkan karakteristik dan tantangan penanggulangan yang berbeda, namun semuanya menuntut respons yang lebih canggih dan terintegrasi daripada yang saat ini tersedia. Menjawab rumusan masalah, kerangka penanggulangan yang ada masih bersifat parsial, sektoral, dan didominasi oleh pendekatan represif yang lamban terhadap dinamika kejahatan. Lemahnya koordinasi antarlembaga, kapasitas teknis yang tidak merata, serta belum diratifikasinya Konvensi Budapest adalah titik-titik lemah yang harus segera dibenahi.

Rekomendasi yang diajukan meliputi: pertama, pembentukan Satgas Siber Nasional yang terintegrasi; kedua, percepatan ratifikasi Konvensi Budapest dan penyelarasan legislasi nasional; ketiga, investasi besar-besaran pada infrastruktur forensik digital dan pelatihan aparat; keempat, pengenaan kewajiban hukum yang lebih ketat pada penyelenggara platform digital; dan kelima, pengarusutamaan literasi keamanan digital dalam

kurikulum nasional. Hanya dengan strategi multi-dimensi yang menyeimbangkan represi, pencegahan, dan kolaborasi, Indonesia dapat membangun ketahanan terhadap ancaman kejahatan siber yang terus bermetamorfosis.

REFERENSI:

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

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

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

ECPAT Indonesia. (2022). Laporan Situasi Eksploitasi Seksual Anak Daring di Indonesia. ECPAT Indonesia.

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

Kusumawardhani, A. (2024). Kecerdasan Buatan dan Kekosongan Hukum Pidana di Indonesia. Jurnal Hukum Siber, 6(1), 15–32.

Mulyadi, L. (2023). Phising dan Social Engineering dalam Hukum Pidana Indonesia. 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.

Pratiwi, N., & Nugroho, S. (2023). Pasar Gelap Data Pribadi dan Penegakan Hukum di Indonesia. Jurnal Hukum dan Teknologi, 5(1), 45–63.

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

Shearing, C., & Wood, J. (2003). Nodal Governance, Democracy, and the New 'Denizens'. Journal of Law and Society, 30(3), 400–419. https://doi.org/10.1111/1467-6478.00263

Simanjuntak, K. (2024). Literasi Keamanan Digital sebagai Pilar Ketahanan Siber Nasional. Jurnal Komunikasi dan Keamanan, 3(1), 40–58.

Siregar, L. (2024). Investigasi Mata Uang Kripto dalam Kejahatan Ransomware. Jurnal Yudisial, 17(1), 88–105.

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,

ISSN: 2338 4638

Volume 7 Nomor 7 (2023)

'ADALAH

Buletin Hukum & Keadilan

Anatomi Penipuan Digital dan Tantangan Penegakan Hukumnya di Indonesia: Dari *Social Engineering* hingga *Deepfake*, serta Problematika Rezim Pembuktian

Gilang Rizki Aji Putra*

Universitas Islam Negeri Syarif Hidayatullah Jakarta

10.15408/adalah.v7i7.51839

Abstract:

Digital fraud has become the most pervasive criminal modality in the digital economy, transcending territorial boundaries and systematically exploiting human psychological vulnerabilities. This article analyzes the anatomy and evolving modus operandi of digital fraud in Indonesia and identifies the multidimensional challenges in its enforcement. Using normative legal research with case, statutory, and comparative approaches, the study finds that digital fraud has evolved from conventional phishing into complex psychological manipulation schemes enhanced by deepfake technology and automated systems. The analysis reveals that Indonesia's criminal law framework, including the Penal Code and the Electronic Information and Transactions Law, still contains fundamental weaknesses in jurisdiction, evidentiary standards, and digital asset tracing. Major cases, such as binary options scams and banking social engineering schemes, confirm that law enforcement agencies often struggle to match the speed and sophistication of offenders. The article concludes that effective enforcement requires jurisdictional reform, strengthened digital forensic capacity, and enhanced international cooperation mechanisms.

Keywords: Digital Fraud, Social Engineering, Deepfake, 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

Penipuan adalah bentuk kejahatan tertua dalam peradaban manusia. Namun, digitalisasi telah memberinya sayap baru yang membuatnya terbang lebih cepat, lebih jauh, dan lebih mematikan. Jika dulu penipu harus bertatap muka dengan korbannya, kini mereka cukup duduk di depan layar, menebar ribuan kail secara otomatis menggunakan bot, menunggu satu-dua korban yang lengah. Penipuan digital bukan lagi kejahatan sederhana; ia telah menjadi industri terorganisasi yang dijalankan oleh sindikat lintas negara, dilengkapi dengan perangkat lunak canggih, pusat panggilan palsu, dan jaringan pencucian uang digital yang rumit.

Di Indonesia, data dari Kepolisian Republik Indonesia dan Otoritas Jasa Keuangan menunjukkan bahwa penipuan digital adalah jenis kejahatan siber dengan volume laporan tertinggi. Kerugian finansial yang ditimbulkan mencapai triliunan rupiah setiap tahunnya, dan angka tersebut kemungkinan besar hanyalah puncak gunung es karena banyak korban yang enggan melapor (Bareskrim Polri, 2023). Modus yang awalnya hanya berupa *surel phishing* kini telah berevolusi menjadi *smishing*, *vishing*, *social engineering* terstruktur, hingga penggunaan deepfake untuk meniru wajah dan suara orang yang dipercaya korban.

Paradoksnya, di saat modus penipuan semakin kompleks, kerangka hukum pidana di Indonesia masih bertumpu pada instrumen yang dirancang untuk era pra-digital. Pasal 378 KUHP tentang penipuan memerlukan adanya "tipu muslihat" yang menggerakkan korban untuk menyerahkan sesuatu secara sukarela. Ketentuan ini, jika diterapkan pada penipuan digital yang serba otomatis dan melibatkan artificial intelligence, menimbulkan persoalan yuridis yang serius: apakah algoritma yang menipu memenuhi unsur "tipu muslihat"? Bagaimana membuktikan "kesukarelaan" penyerahan dalam transaksi elektronik yang terjadi dalam hitungan detik? UU ITE memang menyediakan beberapa pasal yang dapat digunakan, seperti Pasal 28 ayat (1) tentang berita bohong dan Pasal 35 tentang manipulasi data, tetapi konstruksi deliknya tidak secara spesifik dirancang untuk mengkriminalisasi penipuan digital secara komprehensif (Nugroho, 2024). Rumusan masalah dalam artikel ini adalah: Pertama, bagaimana karakteristik dan modus operandi penipuan digital yang berkembang di Indonesia? Kedua, apa tantangan utama dalam penegakan hukum terhadap penipuan digital dan bagaimana strategi mengatasinya? Tujuannya untuk memetakan pola kejahatan dan mengevaluasi kapasitas sistem hukum pidana dalam meresponsnya.

B. DOKTRIN PENIPUAN DAN REZIM PEMBUKTIAN DI ERA DIGITAL

Secara doktrinal, penipuan dalam hukum pidana dibangun di atas tiga elemen utama: (1) adanya tipu muslihat atau rangkaian kebohongan, (2) adanya penyerahan barang atau uang oleh korban, dan (3) adanya hubungan kausal antara tipu muslihat dengan penyerahan tersebut (Moeljatno, 2021). Dalam konteks digital, ketiga elemen ini mengalami distorsi. Tipu muslihat tidak lagi dilakukan oleh manusia secara personal, tetapi dapat diprogram dalam bentuk algoritma, *chatbot*, atau pesan otomatis. Penyerahan tidak lagi berupa penyerahan fisik, melainkan transfer dana digital yang dapat dipicu oleh satu kali klik. Sementara kausalitas menjadi semakin kabur karena intervensi teknologi otomatis di antara pelaku dan korban.

Persoalan ini bersinggungan dengan teori pembuktian dalam hukum acara pidana. Indonesia menganut sistem pembuktian negatif berdasarkan undang-undang (*negatief wettelijk bewijsstelsel*), yang mensyaratkan sekurang-kurangnya dua alat bukti sah ditambah keyakinan hakim. Dalam penipuan digital, alat bukti elektronik yang diakui dalam Pasal 5 UU ITE menjadi kunci. Namun, bukti elektronik bersifat volatil, mudah dihapus, dan rentan terhadap manipulasi. Prinsip *chain of custody* menjadi sangat krusial, tetapi implementasinya di lapangan masih lemah karena keterbatasan kapasitas forensik digital (Santoso, 2023).

Selain itu, penipuan digital seringkali bersifat transnasional. Pelaku, server, korban, dan aliran dana berada di yurisdiksi yang berbeda. Hukum pidana tradisional dibangun di atas asas teritorialitas, yang berarti penerapannya terbatas pada wilayah negara. Keadaan ini menciptakan *jurisdictional* gap: pelaku yang berada di luar negeri sulit dijangkau, sementara ekstradisi dan bantuan hukum timbal balik seringkali berjalan lambat dan birokratis (Brenner, 2022). Kerangka teori ini akan digunakan untuk menganalisis kesenjangan antara realitas kriminal dan kapasitas sistem peradilan pidana Indonesia.

C. MODUS OPERANDI YANG TERUS BEREVOLUSI

1. *Phishing, Smishing,* dan *Vishing*: Fondasi *Social Engineering*

Phishing adalah teknik pengelabuan di mana pelaku mengirimkan tautan palsu yang menyerupai situs resmi untuk mencuri kredensial korban. Evolusinya melahirkan *smishing* (melalui SMS) dan *vishing* (melalui panggilan suara). Modus terbaru yang marak di Indonesia adalah penipuan berkedok perubahan tarif transfer bank atau undangan pernikahan digital dengan ekstensi APK. Korbannya tidak lagi hanya individu yang kurang melek teknologi, melainkan juga profesional dan pebisnis. APK yang diunduh tanpa sadar akan mencuri data SMS, termasuk *one time password* (OTP) perbankan, yang memungkinkan pelaku menguras rekening

korban dalam hitungan menit. Secara teknis, ini adalah kombinasi antara phishing dan trojan yang beroperasi secara otomatis.

2. *Social Engineering* Terstruktur: Manipulasi Psikologis Sistematis

Berbeda dengan *phishing* yang bersifat massal, *social engineering* terstruktur menargetkan korban tertentu (*spear phishing*). Pelaku melakukan riset mendalam tentang target, memetakan jejaring sosialnya, dan membangun skenario yang sangat personal sehingga korban tidak menyadari sedang dimanipulasi. Modus yang paling meresahkan adalah penipuan berkedok kurir palsu, di mana pelaku menyamar sebagai petugas bank atau kepolisian dan menggunakan data pribadi korban yang sudah dicuri sebelumnya untuk meyakinkan. Korban diinstruksikan untuk memindahkan dana ke "rekening aman" dengan dalih sedang terjadi transaksi mencurigakan. Modus ini sangat efektif karena menggabungkan data bocor, tekanan psikologis, dan otoritas palsu (Mulyadi, 2023).

3. Penipuan Investasi dan *Binary Option* Ilegal

Penipuan berkedok investasi adalah salah satu yang paling merugikan secara agregat. Platform trading ilegal seperti kasus Binomo dan Quotex yang melibatkan selebriti sebagai influencer berhasil mengumpulkan dana dari ratusan ribu korban dengan janji keuntungan fantastis. Padahal, platform

tersebut hanya menampilkan simulasi grafik, sementara uang korban dialirkan ke rekening pribadi afiliator. Di sini, pelaku tidak hanya terdiri dari operator platform, tetapi juga *influencer* yang mempromosikan tanpa verifikasi. Konstruksi pertanggungjawaban pidana terhadap influencer dalam kasus semacam ini masih menjadi perdebatan: apakah mereka termasuk pelaku penipuan bersama, atau hanya sebagai korban yang tidak tahu-menahu? Putusan pengadilan terhadap kasus-kasus ini menunjukkan variasi, menandakan ketidakpastian hukum (Wibisono, 2023).

4. Deepfake dan Penipuan Berbasis AI: Ancaman Masa Depan

Pada tahap paling mutakhir, teknologi deepfake mulai digunakan untuk penipuan. Pelaku dapat memalsukan video dan suara seseorang, misalnya seorang CEO untuk memerintahkan stafnya mentransfer dana. Kasus ini sudah terjadi di luar negeri dan potensial terjadi di Indonesia karena teknologi deepfake semakin mudah diakses. Masalahnya, hukum Indonesia belum mengatur tentang pertanggungjawaban pidana penggunaan AI untuk penipuan. Apakah AI dianggap sebagai alat yang netral, atau sebagai perpanjangan dari niat jahat pelaku? Ketiadaan kerangka hukum yang jelas ini meninggalkan kekosongan yang berbahaya (Kusumawardhani, 2024).

D. TIGA LAPIS HAMBATAN STRUKTURAL

1. Hambatan Yurisdiksi dan Anonimitas Pelaku

Sebagian besar sindikat penipuan digital besar beroperasi dari luar wilayah Indonesia. Mereka menggunakan VPN, server di negara ketiga, dan infrastruktur anonim untuk menyembunyikan jejak. Polri, dalam kapasitasnya, tidak dapat begitu saja menetapkan tersangka dan melakukan penangkapan di negara lain. Perjanjian ekstradisi dan *Mutual Legal Assistance* (MLA) ada, tetapi mekanismenya lamban. Sementara itu, Indonesia belum meratifikasi Konvensi Budapest tentang Kejahatan Siber, yang memungkinkan kerjasama lintas batas yang lebih cepat. Akibatnya, seringkali yang berhasil ditangkap hanyalah "kaki tangan" lokal, sementara otak sindikat tetap aman di luar jangkauan (ID-SIRTII, 2023).

2. Hambatan Pembuktian: *Chain of Custody* dan Bukti Digital

Pembuktian penipuan digital sangat bergantung pada bukti elektronik: *log server*, alamat IP, riwayat transaksi, dan komunikasi digital. Namun, bukti elektronik memiliki karakteristik yang rapuh. Ia mudah dihapus atau diubah jika tidak segera diamankan dengan prosedur forensik yang benar. Di Indonesia, laboratorium forensik digital masih terbatas dan terkonsentrasi di kota besar. Akibatnya, penyidik di daerah seringkali tidak

mampu memproses barang bukti digital dengan baik, sehingga perkara gagal di pengadilan karena cacat prosedural (Santoso, 2023). Selain itu, pelaku seringkali menggunakan akun fiktif yang sulit dilacak ke identitas asli. Ketiadaan regulasi yang mewajibkan registrasi identitas asli untuk nomor prabayar dan akun media sosial yang ketat membuat anonimitas menjadi tameng yang mudah bagi penipu.

3. Hambatan Pemulihan Aset: Kecepatan vs Birokrasi

Ketika korban menyadari telah ditipu dan melaporkan ke bank, dana biasanya sudah berpindah ke beberapa rekening lain dalam waktu kurang dari satu jam. Pelaku menggunakan jaringan rekening penampung (mule accounts) yang disewakan oleh pihak ketiga, yang kemudian langsung dicairkan atau dikonversi ke mata uang kripto. Kecepatan ini tidak dapat dilawan oleh mekanisme pembekuan rekening yang ada. Bank memerlukan surat resmi dari kepolisian, sementara penerbitan surat tersebut membutuhkan waktu. Belum ada mekanisme *real-time blocking* yang terintegrasi antara kepolisian, bank, dan penyedia dompet digital. Akibatnya, meskipun pelaku tertangkap, dana korban seringkali sudah tidak dapat dipulihkan (Prasetyo, 2024).

E. POTRET KEGAGALAN DAN KEBERHASILAN PENEGAKAN HUKUM

Sindikat Penipuan Berbasis APK dan Perjuangan Pembuktian

Pada tahun 2023, publik dihebohkan dengan modus penipuan baru berupa file APK undangan pernikahan. Ribuan korban kehilangan akses rekening karena secara tidak sadar mengunduh malware yang mencuri OTP SMS. Dalam kasus ini, Polri berhasil menangkap beberapa pelaku di dalam negeri. Namun, sidang pengadilan mengungkap betapa sulitnya membuktikan keterkaitan antara pelaku yang ditangkap dengan keseluruhan jaringan. Para pelaku mengaku hanya sebagai "penjual data" atau "operator teknis" tanpa mengetahui skema besar. Kelemahan dalam digital forensic chain membuat dakwaan terbatas pada akses ilegal, bukan pada kerugian finansial total yang diderita korban. Kasus ini menunjukkan bahwa keberhasilan penangkapan tidak selalu berbanding lurus dengan keadilan substantif bagi korban (Mulyadi, 2023).

Binary Option Binomo dan Pertanggungjawaban Influencer

Kasus Indra Kenz dan Doni Salmanan menjadi landmark dalam penegakan hukum penipuan digital. Keduanya adalah influencer yang mempromosikan platform binary option ilegal Binomo dan Quotex. Mereka divonis bersalah atas penipuan dan pencucian uang, dengan pidana penjara yang cukup berat. Keberhasilan ini

menunjukkan bahwa aparat mampu menjangkau aktor-aktor yang selama ini merasa kebal hukum. Namun, kasus ini juga menyisakan pertanyaan: para influencer lainnya yang mempromosikan platform serupa, namun belum diproses secara hukum, menunjukkan adanya inkonsistensi penegakan. Selain itu, ribuan korban belum memperoleh ganti rugi yang memadai karena aset para terpidana tidak mencukupi untuk mengganti total kerugian. Sekali lagi, persoalan pemulihan aset menjadi titik lemah yang belum terpecahkan (Wibisono, 2023).

Penipuan *Business Email Compromise* (BEC) terhadap Perusahaan Ekspor

Kasus BEC menargetkan perusahaan yang melakukan transaksi internasional. Pelaku meretas surel perusahaan atau membuat surel yang sangat mirip, lalu mengirimkan instruksi pembayaran palsu. Sebuah perusahaan ekspor di Jawa Timur pernah kehilangan miliaran rupiah karena mengirimkan dana ke rekening pelaku di luar negeri atas instruksi surel yang diyakini berasal dari mitra bisnisnya. Dalam kasus ini, kendala yurisdiksi sangat terasa karena rekening tujuan berada di Hong Kong dan Tiongkok. Proses MLA yang panjang membuat pelacakan aset nyaris mustahil. Kasus BEC adalah contoh sempurna dari kejahatan transnasional yang membutuhkan kerjasama internasional yang kuat dan respons cepat yang belum dimiliki Indonesia.

F. STRATEGI PENEGAKAN HUKUM YANG ADAPTIF DAN BERORIENTASI PEMULIHAN

Merespons tantangan-tantangan di atas, penegakan hukum penipuan digital harus mengalami transformasi fundamental. Pertama, dari sisi legislasi, perlu segera dilakukan revisi UU ITE atau pembentukan undang-undang khusus penipuan digital yang mengakomodasi perkembangan teknologi, termasuk memperjelas pertanggungjawaban penggunaan AI dan bot dalam penipuan. Unsur "tipu muslihat" dalam Pasal 378 KUHP juga perlu diinterpretasi secara lebih luas atau dilengkapi dengan delik baru yang tidak memerlukan interaksi manusia langsung.

Kedua, dari sisi kelembagaan, pembentukan direktori nasional nomor rekening penipuan yang terintegrasi secara real-time antara kepolisian, OJK, Bank Indonesia, dan seluruh penyedia jasa keuangan adalah kebutuhan yang mendesak. Direktori ini memungkinkan setiap laporan penipuan langsung memicu pembekuan dana otomatis di seluruh jaringan, sehingga memutus kecepatan pelaku. Ketiga, ratifikasi Konvensi Budapest berikut aksesi pada Protokol Tambahannya harus segera dilakukan agar Indonesia memiliki landasan hukum untuk kerjasama lintas batas yang lebih efektif, termasuk akses terhadap bukti digital yang disimpan oleh penyedia layanan di luar negeri.

Keempat, investasi besar pada forensik digital di seluruh kepolisian daerah tidak bisa ditunda. Setiap Polda harus memiliki laboratorium forensik digital yang memadai, dengan sumber daya manusia yang tersertifikasi secara internasional. Kelima, edukasi publik harus menjadi gerakan yang berkelanjutan. Kampanye "Cek Fakta, Jangan Klik" saja tidak cukup; masyarakat perlu diedukasi tentang cara melaporkan, cara mengamankan bukti, dan hak-hak mereka sebagai korban (Simanjuntak, 2024). Hanya dengan kombinasi antara represi yang cepat, pencegahan yang masif, dan pemulihan yang berorientasi korban, penipuan digital dapat ditekan ke tingkat yang terkendali.

G. KESIMPULAN

Penipuan digital di Indonesia telah mencapai tingkat kompleksitas yang mengkhawatirkan, dengan modus operandi yang menggabungkan social engineering, otomatisasi, dan teknologi deepfake. Kerangka hukum pidana yang ada masih memiliki kelemahan fundamental pada aspek yurisdiksi, pembuktian, dan kecepatan pemulihan aset. Menjawab rumusan masalah, tantangan utama penegakan hukum terletak pada tiga lapis hambatan: yurisdiksi transnasional yang dimanfaatkan pelaku, lemahnya kapasitas forensik digital yang menggerogoti *chain of custody*, serta kecepatan aliran dana digital yang tidak dapat ditandingi oleh prosedur birokratis konvensional. Studi kasus mengkonfirmasi bahwa keberhasilan penangkapan

tidak selalu berarti keadilan bagi korban, karena pemulihan aset masih menjadi mata rantai terlemah.

Rekomendasi yang diajukan mencakup: pembentukan direktori nasional rekening penipuan dengan kemampuan pembekuan real-time, percepatan ratifikasi Konvensi Budapest, pengembangan laboratorium forensik digital di setiap Polda, revisi legislasi untuk mengakomodasi penipuan berbasis AI, serta pengarusutamaan pendidikan keamanan digital. Tanpa terobosan di bidang-bidang ini, penipuan digital akan terus menjadi *silent epidemic* yang menguras sumber daya ekonomi dan kepercayaan masyarakat terhadap ekosistem digital nasional.

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). Kecerdasan Buatan dan Kekosongan Hukum Pidana di Indonesia. Jurnal Hukum Siber, 6(1), 15–32.

Moeljatno. (2021). Asas-Asas Hukum Pidana (Edisi Revisi). Rineka Cipta.

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

Nugroho, A. (2024). Anatomi Kejahatan Penipuan Berbasis Teknologi Digital. Jurnal Hukum Pidana dan Kriminologi, 15(1), 41–60.

Prasetyo, B. (2024). Pemulihan Aset Korban Penipuan Digital: Tantangan dan Solusi. 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. https://doi.org/10.29123/jy.v16i3.542

Simanjuntak, K. (2024). Literasi Keamanan Digital sebagai Pilar Ketahanan Siber Nasional. Jurnal Komunikasi dan Keamanan, 3(1), 40–58.

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).

Wibisono, A. (2023). Pertanggungjawaban Pidana Influencer dalam Penipuan Investasi Ilegal.

Jurnal Pelindungan Data Pribadi dan Kejahatan Ekonomi, 2(2), 101–118.

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

Shearing, C., & Wood, J. (2003). Nodal Governance, Democracy, and the New 'Denizens'. Journal of Law and Society, 30(3), 400–419. https://doi.org/10.1111/1467-6478.00263

Simanjuntak, K. (2024). Literasi Keamanan Digital sebagai Pilar Ketahanan Siber Nasional. Jurnal Komunikasi dan Keamanan, 3(1), 40–58.

Siregar, L. (2024). Investigasi Mata Uang Kripto dalam Kejahatan Ransomware. Jurnal Yudisial, 17(1), 88–105.

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,

ISSN: 2338 4638

Volume 7 Nomor 7 (2023)

'ADALAH

Buletin Hukum & Keadilan

Peretasan dan Akses Ilegal dalam Perspektif Hukum Pidana Indonesia: Menimbang Ulang Konsep "Tanpa Hak" dan "Niat Baik" di Era *Ethical Hacking*

Gilang Rizki Aji Putra*

Universitas Islam Negeri Syarif Hidayatullah Jakarta

10.15408/adalah.v7i7.51840

Abstract:

Hacking and unauthorized access to electronic systems constitute one of the most fundamental forms of cybercrime, threatening the confidentiality, integrity, and availability of data. This article examines the legal construction of hacking and illegal access under Indonesian criminal law, particularly the Electronic Information and Transactions Law (ITE Law) and the Penal Code, and evaluates whether these provisions adequately distinguish malicious actors (black hat hackers) from ethical hackers. Using normative legal research with statutory, conceptual, and comparative approaches, the study finds that the key phrase "without right or unlawfully" under Article 30 of the ITE Law generates interpretative uncertainty and risks criminalizing legitimate cybersecurity research. The absence of regulations on bug bounty programs and the doctrine of implied consent further places security researchers in a vulnerable legal position. The article concludes that Indonesian criminal law should adopt a differentiated approach recognizing ethical hacking through explicit safe harbor provisions and clearer enforcement guidelines.

Keywords: Hacking, Illegal Access, Ethical Hacking, Electronic Information and Transactions Law (ITE Law), Bug Bounty..

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

A. PENDAHULUAN

Peretasan (*hacking*) adalah fenomena yang lahir bersamaan dengan perkembangan internet itu sendiri. Istilah ini pada mulanya merujuk pada aktivitas pemrograman yang cerdas dan eksploratif, namun seiring waktu mengalami stigmatisasi menjadi tindakan kriminal yang merugikan. Dalam hukum pidana Indonesia, peretasan diartikan sebagai akses tidak sah atau tanpa hak terhadap sistem komputer atau jaringan elektronik, sebagaimana diatur dalam Pasal 30 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan perubahannya. Konstruksi delik ini bertujuan untuk melindungi kepentingan hukum terhadap keamanan sistem elektronik yang menjadi tulang punggung kehidupan modern.

Namun, perkembangan dunia keamanan siber telah melahirkan figur paradoksal: *ethical hacker* atau *white hat hacker,* yaitu individu yang menggunakan keterampilan dan teknik yang sama dengan penjahat siber, tetapi tujuannya adalah untuk mengidentifikasi kerentanan sistem dan melaporkannya kepada pemilik sistem demi perbaikan. Aktivitas ini, yang menjadi fondasi dari *vulnerability disclosure* dan *bug bounty* program yang dipromosikan oleh perusahaan teknologi global, secara teknis memenuhi unsur-unsur delik akses ilegal dalam UU ITE. Memasuki sistem tanpa izin, bahkan dengan niat menemukan celah keamanan,

tetap melanggar rumusan "tanpa hak" yang tidak memberikan pengecualian bagi motivasi altruistik.

Persoalan ini bukan sekadar wacana akademis. Beberapa kasus di Indonesia menunjukkan bahwa individu yang melaporkan kerentanan justru berhadapan dengan ancaman pidana dari pemilik sistem yang merasa tersinggung atau malu. Ketiadaan perlindungan hukum bagi pelapor kerentanan (*vulnerability reporter*) menciptakan chilling effect yang justru merugikan keamanan siber nasional, karena celah keamanan tetap terbuka tanpa ada yang berani melaporkan (Sutanto & Hidayat, 2023). Rumusan masalah dalam artikel ini adalah: Pertama, bagaimana konstruksi delik peretasan dan akses ilegal dalam UU ITE dan KUHP nasional? Kedua, bagaimana hukum pidana Indonesia menyikapi aktivitas *ethical hacking*, dan di mana letak persoalan normatifnya? Tujuannya adalah untuk menelaah secara kritis rumusan pidana yang ada dan mengusulkan kerangka hukum yang lebih proporsional.

B. PERETASAN DALAM PERSPEKTIF HUKUM PIDANA DAN TEORI *IMPLIED CONSENT*

Dalam hukum pidana, peretasan dikategorikan sebagai tindak pidana terhadap kerahasiaan, integritas, dan ketersediaan data dan sistem komputer. Konvensi Budapest tentang Kejahatan Siber (2001) dalam Pasal 2 hingga Pasal 6 mengatur secara komprehensif tentang *illegal access*,

illegal interception, data interference, system interference, dan *misuse of devices.* Yang menjadi fondasi adalah konsep "akses tanpa hak" (*access without right*), yang mensyaratkan adanya pelanggaran terhadap hak eksklusif pemilik sistem untuk menentukan siapa yang boleh mengakses.

Namun, Konvensi Budapest tidak memberikan definisi tegas tentang "hak akses". Definisi ini diserahkan kepada hukum nasional masing-masing negara pihak. Di sinilah muncul persoalan interpretasi. Ahli hukum siber Susan W. Brenner (2022) menjelaskan bahwa model delik akses ilegal dapat dibedakan menjadi dua: *broad model* dan *narrow model. Broad model* memidana setiap akses tanpa otorisasi, tanpa memandang niat. *Narrow model* mempersyaratkan adanya niat jahat tertentu, seperti niat mencuri data atau merusak sistem.

Indonesia, melalui rumusan Pasal 30 UU ITE, cenderung mengadopsi broad model. Akses tanpa hak terhadap sistem orang lain sudah merupakan kejahatan, terlepas dari apakah ada data yang diambil atau kerusakan yang ditimbulkan. Di satu sisi, ini memberikan perlindungan kuat terhadap keamanan sistem. Di sisi lain, ia menutup pintu bagi pembelaan berdasarkan niat baik. Teori implied consent yang berkembang dalam hukum perdata tidak dikenal dalam hukum pidana Indonesia. Dalam konteks ethical hacking, implied consent dapat diartikan sebagai persetujuan diam-diam dari pemilik sistem yang telah membuka akses ke publik

(misalnya melalui internet) dan diyakini oleh pelaku akan menerima pelaporan kerentanan. Sayangnya, hukum pidana Indonesia tidak memberikan ruang bagi interpretasi ini.

Di samping itu, teori legal interest atau kepentingan hukum yang dilindungi perlu diperjelas. Jika kepentingan hukum yang dilindungi adalah keamanan sistem semata, maka setiap akses tanpa izin, bagaimana pun motivasinya, melanggar. Namun, jika kepentingan hukum yang dilindungi juga mencakup keamanan siber nasional secara lebih luas, maka ethical hacking yang justru memperkuat keamanan seharusnya tidak dipidana (Kusumawardhani, 2023). Di sinilah letak urgensi untuk menimbang ulang filosofi pemidanaan akses ilegal.

C. KONSTRUKSI DELIK PERETASAN DALAM UU ITE DAN KELEMAHANNYA

1. Pasal 30 UU ITE dan Makna "Tanpa Hak atau Melawan Hukum"

Pasal 30 UU ITE terdiri dari tiga ayat. Ayat (1) mengkriminalisasi akses tanpa hak ke sistem komputer dengan cara apa pun. Ayat (2) menjangkau akses tanpa hak dengan tujuan memperoleh informasi atau data. Ayat (3) menjangkau akses tanpa hak dengan melanggar atau menerobos sistem pengamanan. Unsur "tanpa hak atau melawan hukum" menjadi inti delik, tetapi UU

ITE dan penjelasannya tidak memberikan definisi yang memadai. Ketiadaan definisi ini membuka ruang interpretasi yang sangat luas dan berpotensi sewenang-wenang.

Dalam praktik, "tanpa hak" seringkali disamakan dengan "tidak memiliki izin tertulis". Ini berarti seorang peneliti keamanan yang menemukan celah di situs pemerintah dan mencoba mengakses untuk memverifikasi kerentanannya, meskipun dengan niat melaporkan, dapat dianggap memenuhi unsur delik karena tidak memiliki surat izin resmi. Problemnya, dalam banyak kasus, pemilik sistem justru tidak menyediakan mekanisme pelaporan yang mudah atau program bug bounty resmi. Akibatnya, peneliti menghadapi dilema: melaporkan tanpa mengakses (yang mustahil untuk verifikasi teknis), mengakses lalu melaporkan (risiko pidana), atau diam saja (celah tetap terbuka) (Prasetyo, 2024).

Bandingkan dengan pengaturan di beberapa yurisdiksi lain. Amerika Serikat melalui *Computer Fraud and Abuse Act* (CFAA) juga menggunakan frasa "tanpa otorisasi", tetapi pengadilan di sana telah mengembangkan yurisprudensi yang membedakan antara akses oleh pihak yang sama sekali tidak berwenang dengan akses oleh pihak yang memiliki akses terbatas tetapi melebihi batas otorisasinya (*exceeding authorized access*). Belakangan, terdapat tren untuk mempersempit interpretasi CFAA agar tidak menjerat aktivitas yang secara substansi tidak merugikan. Di Jerman, Pasal 202a KUHP Jerman

mensyaratkan adanya "pengamanan khusus" yang diterobos, sehingga sistem yang tidak memiliki pengamanan tidak dilindungi oleh pasal ini. Ini memberikan ruang lebih besar bagi penemuan kerentanan pada sistem yang terbuka.

2. Ketidakmampuan Membedakan *White Hat, Grey Hat,* dan *Black Hat*

Dalam dunia keamanan siber, dikenal tiga kategori peretas: *white hat* (etis, dengan izin), *black hat* (jahat, tanpa izin dan merugikan), dan *grey hat* (abu-abu, tanpa izin tetapi tidak merugikan atau justru melaporkan). UU ITE tidak membedakan ketiganya. Semua akses tanpa izin otomatis kena delik. Hal ini menimbulkan persoalan keadilan karena hukum menempatkan peretas yang mencuri data nasabah bank untuk diperjualbelikan sama posisinya dengan peneliti yang mengakses API terbuka untuk membuktikan kerentanan lalu melaporkannya ke publik.

Sejumlah kasus di Indonesia menunjukkan bias represif ini. Pada tahun 2018, seorang mahasiswa di Yogyakarta yang menemukan kerentanan pada portal akademik kampusnya dan melaporkannya ke administrator justru dilaporkan ke polisi oleh pihak kampus atas dugaan peretasan. Kasus ini menjadi preseden buruk yang menunjukkan bahwa pemilik sistem seringkali tidak dewasa dalam menerima laporan kerentanan, dan hukum pidana yang seharusnya menjadi ultimum

remedium dengan mudah dijadikan alat pembungkaman (Sutanto & Hidayat, 2023). Ketiadaan safe harbor provision dalam UU ITE menciptakan ketidakpastian yang menghambat partisipasi publik dalam menjaga keamanan siber.

3. Delik Peretasan dalam KUHP Baru dan Persinggungannya dengan UU ITE

KUHP baru (UU 1/2023) juga mengatur tentang tindak pidana terhadap sistem dan data elektronik dalam Bab tentang Tindak Pidana Terhadap Keamanan Negara dan dalam Bab Tindak Pidana Terhadap Kepercayaan dalam Bertransaksi Elektronik. Pasal 332 KUHP baru, misalnya, mengatur tentang akses ilegal dengan ancaman pidana yang cukup berat. Namun, KUHP baru tidak menciptakan harmoni dengan UU ITE; ia justru menambah lapisan regulasi yang tumpang tindih. Sinkronisasi antara pasal-pasal UU ITE dan KUHP baru sangat diperlukan. Tanpa sinkronisasi, pelaku bisa dijerat dengan dua rezim sekaligus untuk perbuatan yang sama, yang berpotensi melanggar asas *ne bis in idem* (Nugroho, 2024). Lebih dari itu, KUHP baru juga tidak memuat pengecualian bagi ethical hacking, sehingga problem mendasarnya tetap tidak terselesaikan.

D. TIGA WAJAH PERETASAN DAN RESPONS HUKUM

Peretasan Situs Pemerintah oleh "Bjorka" (2022)

Bjorka adalah figur misterius yang meretas berbagai situs pemerintah dan membocorkan data-data pejabat serta dokumen internal ke publik. Aksinya jelas termasuk *black hat* karena bertujuan mencuri data dan membocorkannya, menimbulkan kerugian reputasi maupun potensi keamanan. Pemerintah membentuk satgas dan melakukan upaya penegakan hukum, namun pelaku utama tidak berhasil teridentifikasi. Kasus ini mengekspos kerentanan infrastruktur pemerintah dan kebutuhan akan sistem keamanan yang lebih kuat. Dalam perspektif hukum, kasus Bjorka jelas memenuhi unsur Pasal 30 ayat (2) dan ayat (3) UU ITE, juga Pasal 32 tentang manipulasi data. Tidak ada kontroversi soal kriminalisasi. Namun, ironisnya, kegagalan menangkap pelaku justru menunjukkan kelemahan kapasitas investigasi, bukan kelemahan norma.

Kerentanan Aplikasi PeduliLindungi dan Pelaporan Publik (2021)

Pada masa pandemi, beberapa peneliti keamanan menemukan kerentanan serius pada aplikasi PeduliLindungi yang berpotensi membocorkan data pribadi jutaan pengguna. Mereka melaporkannya secara publik setelah tidak mendapat respons dari pengembang. Bukannya memproses laporan, otoritas sempat mengancam akan memproses hukum para pelapor. Kasus ini adalah contoh nyata bagaimana ketiadaan mekanisme responsible disclosure dan bug bounty

menempatkan peneliti dalam posisi berbahaya. Para peneliti tersebut jelas mengakses data untuk membuktikan kerentanan secara teknis melanggar Pasal 30, tetapi motivasi mereka adalah melindungi publik. Kasus ini menunjukkan betapa hukum kita gagal membedakan antara kejahatan dan kontribusi sosial.

Peretasan Balik (*Hacking Back*) dan Problematika Pertahanan Diri Digital

Salah satu isu hukum yang belum terjamah adalah hacking back atau peretasan balasan yang dilakukan oleh korban untuk melacak atau melumpuhkan penyerang. Dalam satu kasus, sebuah perusahaan swasta yang menjadi korban ransomware berhasil melacak server pelaku dan mencoba menonaktifkannya. Secara teknis, ini adalah akses ilegal. Namun, dari perspektif moral, ini adalah bentuk pertahanan diri. Hukum pidana Indonesia sama sekali tidak mengenal doktrin self-defense dalam konteks digital. Padahal, dalam situasi di mana aparat tidak mampu merespons dengan cepat, korban memiliki kepentingan yang sah untuk melindungi asetnya. Pengaturan tentang active defense masih menjadi wilayah abu-abu yang memerlukan pengkajian mendalam (Brenner, 2022).

E. REFORMULASI HUKUM: MENUJU MODEL DIFERENSIATIF DAN SAFE HARBOR PROVISION

Untuk mengatasi persoalan di atas, hukum pidana Indonesia perlu mengadopsi reformulasi yang lebih diferensiatif. Pertama, perlu ditambahkan pengecualian atau safe harbor provision dalam UU ITE yang menyatakan bahwa akses terhadap sistem komputer tidak dianggap sebagai tindak pidana jika dilakukan dengan iktikad baik untuk mengidentifikasi kerentanan dan melaporkannya kepada pemilik sistem atau otoritas yang berwenang, tanpa menimbulkan kerugian lebih lanjut. Ketentuan ini akan melindungi ethical hacker dari jeratan pidana, sekaligus mendorong budaya vulnerability disclosure yang sehat.

Kedua, konsep "tanpa hak" perlu diperjelas melalui peraturan pelaksana atau pedoman penegakan hukum. Kejaksaan Agung dan Kepolisian dapat mengeluarkan panduan yang menyatakan bahwa akses yang dilakukan untuk riset dan pelaporan kerentanan, sepanjang tidak mengeksploitasi data atau merusak sistem, tidak dituntut pidana. Panduan semacam ini sudah diterapkan di Belanda oleh Public Prosecution Service yang menerbitkan kebijakan tentang penanganan ethical hacking. Ketiga, pemerintah perlu mendorong setiap kementerian, lembaga, dan perusahaan besar untuk membuka vulnerability disclosure program (VDP) resmi. Dengan adanya VDP, peneliti memiliki saluran resmi untuk

melaporkan tanpa perlu mengambil risiko mengakses secara diam-diam. Keempat, Mahkamah Agung dapat berperan melalui pembentukan yurisprudensi progresif. Ketika berhadapan dengan kasus *ethical hacking*, hakim harus mempertimbangkan niat, dampak, dan kontribusi terdakwa, serta tidak menerapkan pasal secara mekanis. Yurisprudensi semacam ini akan menjadi kompas bagi pengadilan di seluruh Indonesia (Simanjuntak, 2024).

F. KESIMPULAN

Konstruksi delik peretasan dan akses ilegal dalam UU ITE menganut model yang sangat luas (broad model), yang memidana setiap akses tanpa hak tanpa mempertimbangkan niat atau dampak. Rumusan ini memberikan perlindungan kuat bagi keamanan sistem, namun di sisi lain menimbulkan ketidakpastian hukum yang serius bagi aktivitas ethical hacking yang berkontribusi positif terhadap ketahanan siber nasional. Menjawab rumusan masalah, hukum pidana Indonesia saat ini belum mampu membedakan secara adil antara peretas jahat dan peretas etis. Frasa "tanpa hak atau melawan hukum" yang tidak didefinisikan secara kontekstual menjadi sumber persoalan yang mengancam partisipasi publik dalam pengamanan sistem digital.

Rekomendasi yang diajukan meliputi: pertama, amendemen UU ITE untuk menyertakan safe harbor provision bagi ethical hacker; kedua,

penerbitan pedoman teknis oleh Kejaksaan dan Kepolisian tentang penanganan kasus peretasan yang melibatkan niat baik dan pelaporan kerentanan; ketiga, pembentukan vulnerability disclosure program wajib bagi instansi pemerintah; dan keempat, pelatihan hakim dan penyidik tentang aspek teknis keamanan siber agar mampu membuat putusan yang proporsional dan informatif. Hanya dengan reformulasi yang memperhitungkan realitas *ethical hacking*, Indonesia dapat membangun ekosistem keamanan siber yang tidak hanya represif, tetapi juga progresif dan inklusif.

REFERENSI:

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

Kusumawardhani, A. (2023). Konsep "Tanpa Hak" dalam Pasal 30 UU ITE dan Pengaruhnya terhadap Riset Keamanan Siber. Jurnal Hukum Siber, 5(1), 15–32.

Nugroho, A. (2024). Sinkronisasi Hukum Pidana Materiil dalam UU ITE Pasca KUHP Baru. Jurnal Hukum Pidana dan Kriminologi, 15(1), 41–60.

Prasetyo, B. (2024). Dilema Ethical Hacking dalam Hukum Pidana Indonesia. Jurnal Hukum dan Masyarakat, 16(1), 88–107.

Simanjuntak, K. (2024). Peran Yurisprudensi dalam Melindungi Vulnerability Reporter. Jurnal Konstitusi, 21(2), 278–296. https://doi.org/10.31078/jk2125

Sutanto, R., & Hidayat, F. (2023). Ethical Hacking dan Ancaman Kriminalisasi: Studi Kasus di Indonesia. Jurnal Kajian Hukum dan Teknologi, 4(2), 112–130.

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 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (Lembaran Negara Tahun 2023 Nomor 1, Tambahan Lembaran Negara Nomor 6842).

ISSN: 2338 4638

Volume 7 Nomor 7 (2023)

'ADALAH

Buletin Hukum & Keadilan

Penyebaran Konten Ilegal di Internet: Tinjauan Yuridis terhadap Regulasi, Penegakan, dan Harmonisasi Hukum di Indonesia

Gilang Rizki Aji Putra*

Universitas Islam Negeri Syarif Hidayatullah Jakarta

10.15408/adalah.v7i7.51841

Abstract:

The dissemination of illegal content on the internet represents a disruptive phenomenon that threatens public order, morality, and national security. This article provides a juridical review of Indonesia's legal framework in addressing illegal online content, examining regulatory instruments, enforcement challenges, and the urgency of legal harmonization. Employing normative legal research with statutory, conceptual, and comparative approaches, the study finds that Indonesia's regulatory regime remains fragmented across various sectoral laws, including the Electronic Information and Transactions Law (ITE Law), the Pornography Law, the Child Protection Law, and the Penal Code. This fragmentation creates overlapping norms, legal uncertainty, and the risk of criminalizing legitimate expression. Analysis of cases involving hate speech, pornography, and disinformation highlights the tension between effective enforcement and human rights protection. Cross-border jurisdictional issues and reliance on foreign platforms further complicate enforcement. The article concludes that regulatory harmonization, stronger due process safeguards in content blocking, and ratification of the Budapest Convention are essential for a fair and secure digital ecosystem.

Keywords: Illegal Content, Electronic Information and Transactions Law (ITE Law), Legal Harmonization, Content Blocking, Digital Jurisdiction.

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

A. PENDAHULUAN

Internet telah menjelma menjadi ruang publik global yang meniscayakan kebebasan berekspresi, berbagi informasi, dan berinteraksi tanpa sekat geografis. Namun, kebebasan ini acapkali disalahgunakan untuk menyebarkan konten ilegal, seperti pornografi, ujaran kebencian berbasis SARA, berita bohong (*hoaks*), hingga propaganda terorisme. Karakter internet yang anonim, instan, dan mendunia membuat konten ilegal dapat diproduksi dan disebarluaskan secara masif dalam hitungan detik, menimbulkan dampak destruktif yang meluas: mulai dari degradasi moral, polarisasi sosial, hingga ancaman terhadap keamanan negara.

Indonesia, sebagai salah satu negara dengan populasi pengguna internet terbesar, merespons fenomena ini dengan menerbitkan berbagai perangkat hukum. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 merupakan payung hukum utama yang mengkriminalisasi penyebaran konten ilegal. Selain itu, terdapat undang-undang sektoral lain seperti Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi, Undang-Undang Nomor 35 Tahun 2014 tentang Perlindungan Anak, serta ketentuan dalam Kitab Undang-Undang Hukum Pidana (KUHP) yang juga relevan. Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik

(PP PSTE) turut mengatur kewenangan pemerintah untuk melakukan pemutusan akses (*takedown*) terhadap konten ilegal.

Namun, pluralitas regulasi ini justru menimbulkan persoalan harmonisasi. Definisi konten ilegal yang tidak seragam, rumusan delik yang tumpang tindih, serta kewenangan lembaga yang tersebar menciptakan ketidakpastian hukum bagi pengguna internet maupun penegak hukum. Lebih jauh, pendekatan represif yang dominan melalui kriminalisasi dan pemblokiran seringkali mengabaikan prinsip due process dan kebebasan berekspresi yang dijamin konstitusi (Butt & Lindsey, 2023). Rumusan masalah dalam artikel ini adalah: Pertama, bagaimana kerangka hukum Indonesia mengatur penyebaran konten ilegal di internet? Kedua, apa tantangan yuridis utama dalam penanggulangan penyebaran konten ilegal dan bagaimana upaya harmonisasi yang diperlukan? Tujuannya adalah untuk menelaah secara komprehensif dan kritis terhadap instrumen hukum yang ada, mengidentifikasi kelemahan dan celah, serta merumuskan rekomendasi kebijakan yang berorientasi pada kepastian hukum dan perlindungan hak asasi digital.

B. KONTEN ILEGAL, *INTERMEDIARY LIABILITY*, DAN PRINSIP *DUE PROCESS*

Konten ilegal dapat didefinisikan sebagai segala bentuk informasi atau dokumen elektronik

yang pembuatan, penyimpanan, atau penyebarannya dilarang oleh hukum. Kategorinya sangat luas, mulai dari konten yang melanggar kesusilaan, perjudian, penghinaan, pemerasan, berita bohong, hingga konten yang melanggar hak kekayaan intelektual. Dalam konteks hukum internasional, Konvensi Budapest tentang Kejahatan Siber (2001) secara khusus mengatur tentang tindak pidana terkait konten, khususnya pornografi anak, dalam Pasal 9-nya. Sementara itu, pendekatan intermediary liability membebankan tanggung jawab hukum kepada penyelenggara platform atau penyedia layanan internet atas konten yang disebarkan oleh penggunanya.

Secara global, terdapat tiga model pengaturan intermediary liability: (1) *strict liability*, di mana penyelenggara bertanggung jawab penuh atas konten pengguna; (2) *safe harbor* dengan kewajiban *notice and takedown*, di mana penyelenggara baru bertanggung jawab setelah diberitahu dan tidak segera menghapus konten; dan (3) *conditional safe harbor* dengan kewajiban proaktif tertentu. Indonesia, melalui UU ITE dan PP PSTE, mengadopsi sistem conditional safe harbor, di mana penyelenggara wajib melakukan pemutusan akses setelah menerima perintah dari pemerintah, dan dapat dimintai pertanggungjawaban jika lalai atau sengaja membiarkan konten ilegal (DeNardis, 2020). Namun, penerapan mekanisme ini kerap

menyimpan persoalan transparansi dan akuntabilitas.

Di sisi lain, penanggulangan konten ilegal tidak boleh mengabaikan prinsip *due process of law* dan standar hak asasi manusia. Pembatasan terhadap kebebasan berekspresi, sebagaimana digariskan dalam Pasal 19 Kovenan Internasional tentang Hak-Hak Sipil dan Politik (ICCPR), hanya dapat dilakukan melalui hukum yang jelas, untuk tujuan yang sah, dan dengan cara yang proporsional. Ketiadaan definisi yang jelas, mekanisme keberatan yang aksesibel, dan pengawasan yudisial terhadap tindakan administratif seperti pemblokiran dapat menjerumuskan negara ke dalam praktik otoritarianisme digital (Setiawan, 2023). Kerangka ini menjadi landasan untuk menguji sejauh mana regulasi Indonesia selaras dengan prinsip rule of law.

C. REGULASI KONTEN ILEGAL DI INDONESIA DAN PROBLEMATIKANYA

1. Bentuk dan Substansi Pengaturan Konten Ilegal dalam Hukum Positif

Hukum positif Indonesia mengatur konten ilegal dalam berbagai peraturan perundang-undangan. UU ITE menjadi instrumen paling komprehensif. Pasal 27 ayat (1) melarang pendistribusian dan/atau pentransmisian konten yang melanggar kesusilaan. Ayat (2) tentang

perjudian, ayat (3) tentang pencemaran nama baik, dan ayat (4) tentang pemerasan. Pasal 28 ayat (1) mengatur berita bohong dan penyesatan yang merugikan konsumen, sedangkan ayat (2) melarang penyebaran informasi yang menimbulkan kebencian atau permusuhan berdasarkan SARA. Pasal 29 mengatur ancaman kekerasan atau menakut-nakuti secara pribadi. Semuanya dipidana dengan ancaman penjara yang cukup berat.

Di luar UU ITE, UU Pornografi mengkriminalisasi setiap orang yang memproduksi, menyebarluaskan, atau mengakses konten pornografi, dengan definisi pornografi yang cukup luas. UU Perlindungan Anak memberikan sanksi khusus bagi konten yang mengeksploitasi anak secara seksual. UU Penghapusan Kekerasan Seksual turut melarang penyebaran konten bermuatan kekerasan seksual non-konsensual. Sementara itu, UU Terorisme melarang penyebaran konten yang mendukung atau merekrut untuk kegiatan terorisme. KUHP baru (UU 1/2023) juga memuat delik-delik yang relevan, khususnya terkait penyebaran berita bohong yang dapat menimbulkan keonaran. Spektrum pengaturan yang luas ini menunjukkan intensi negara untuk mengontrol konten ilegal, tetapi juga menciptakan multi-regime yang kompleks.

2. Problem Fragmentasi dan Tumpang Tindih Norma

Fragmentasi menjadi persoalan utama. Sebuah konten yang sama, misalnya sebuah video asusila yang direkam tanpa izin dan mengandung unsur pemerasan, dapat sekaligus dijerat dengan UU ITE (Pasal 27 ayat 1 dan 4), UU Pornografi (Pasal 4 jo. 29), dan UU TPKS (Pasal 14). Tumpang tindih ini tidak hanya membingungkan penyidik dalam menentukan pasal yang tepat, tetapi juga berpotensi melanggar asas ne bis in idem jika terjadi penuntutan berganda. Lebih dari itu, perbedaan ancaman pidana antara UU satu dengan lainnya menimbulkan disparitas keadilan yang tidak terstruktur.

Lebih problematik lagi, UU ITE menggunakan frasa-frasa yang tidak memiliki definisi hukum yang ketat, seperti "kesusilaan" dan "menimbulkan kebencian". Frasa "kesusilaan" dalam UU ITE tidak dirumuskan secara spesifik, sehingga penilaiannya sangat bergantung pada moralitas lokal dan subjektivitas penegak hukum. Kasus di mana seorang seniman dijerat karena mengunggah karya seni yang menampilkan ketelanjangan menunjukkan betapa rumitnya menerapkan standar "kesusilaan" yang seragam untuk masyarakat Indonesia yang majemuk. Sedangkan frasa "menimbulkan kebencian" dalam Pasal 28 ayat (2) tidak memiliki ambang batas yang jelas, sehingga kritik terhadap kebijakan keagamaan suatu kelompok tertentu dapat ditafsirkan sebagai ujaran kebencian oleh kelompok yang dikritik (Prasetyo, 2024). Ketidakjelasan ini

tidak hanya merusak kepastian hukum, tetapi juga berdampak pada perlindungan kebebasan berekspresi.

3. Mekanisme *Takedown* dan Kewenangan Pemerintah antara Efektivitas dan Transparansi

Pemerintah, melalui Kementerian Komunikasi dan Informatika (Kominfo), memiliki kewenangan untuk melakukan pemutusan akses (takedown) terhadap konten ilegal berdasarkan Pasal 40 ayat (2) UU ITE dan PP PSTE. Dalam praktiknya, Kominfo melakukan patroli siber dan merespons laporan masyarakat untuk kemudian memblokir akses ke konten atau situs tertentu. Mekanisme ini sangat cepat, mampu menghentikan penyebaran konten negatif dalam waktu singkat, terutama untuk kategori darurat seperti terorisme dan pornografi anak.

Namun, mekanisme ini beroperasi dalam wilayah administratif yang minim transparansi. Publik tidak memiliki akses terhadap data akurat tentang konten apa saja yang diblokir, atas dasar apa, dan bagaimana mekanisme pengajuan keberatan. Ketiadaan judicial oversight terhadap keputusan pemblokiran membuka ruang penyalahgunaan kekuasaan. Beberapa organisasi masyarakat sipil mencatat bahwa sejumlah situs berita dan blog yang memuat konten kritik terhadap pemerintah juga ikut diblokir dengan dalih "mengganggu ketertiban umum" tanpa penjelasan

memadai (Fitriani, 2023). Praktik seperti ini bertentangan dengan prinsip due process dan dapat dikategorikan sebagai sensor sepihak yang tidak sah dalam negara hukum.

D. TANTANGAN YURISDIKSI DAN KERJASAMA INTERNASIONAL

Salah satu tantangan terbesar dalam penanggulangan konten ilegal adalah sifatnya yang lintas batas. Server tempat konten ilegal disimpan seringkali berada di luar yurisdiksi Indonesia, sementara pengelola platform digital raksasa adalah korporasi multinasional yang enggan tunduk sepenuhnya pada hukum nasional. Ketika Kominfo memblokir sebuah situs, pengguna masih dapat mengaksesnya melalui *Virtual Private Network* (VPN) atau mirror site. Ketika pemerintah meminta Google atau Meta untuk menghapus konten, prosesnya bergantung pada kebijakan community guidelines yang tidak selalu selaras dengan hukum Indonesia.

Hingga saat ini, Indonesia belum meratifikasi Konvensi Budapest tentang Kejahatan Siber, yang menyediakan kerangka kerja sama formal untuk penegakan hukum lintas batas, termasuk dalam pertukaran bukti elektronik. Ketidakikutsertaan ini membuat proses *Mutual Legal Assistance* (MLA) berjalan lambat dan birokratis. Selain itu, Indonesia juga belum memiliki perjanjian bilateral yang kuat dengan negara-negara yang menjadi tempat bernaungnya server utama dunia. Akibatnya, otak di

balik penyebaran konten ilegal berskala besar seringkali lolos dari jeratan hukum, sementara hanya aktor lokal kecil yang dapat ditindak. Ketergantungan pada itikad baik platform asing adalah posisi yang sangat rentan bagi penegakan kedaulatan hukum (Brenner, 2022).

E. PENYEBARAN HOAKS DAN KONTEN BERNUANSA SARA

Kasus Buni Yani pada tahun 2017 merupakan contoh klasik penyebaran konten ilegal yang memiliki implikasi politik dan sosial yang dalam. Buni Yani dijerat karena mengedit dan mengunggah video pidato Basuki Tjahaja Purnama (Ahok) yang diberi pertanyaan "apakah umat Islam dibohongi?" Video tersebut dianggap sebagai konten yang menyebarkan kebencian berbasis SARA dan menimbulkan kegaduhan nasional. Pengadilan menyatakan Buni Yani bersalah melanggar Pasal 28 ayat (2) UU ITE. Kontroversi muncul karena sebagian kalangan menilai tindakan Buni Yani adalah murni menyebarkan informasi yang sudah ada di ruang publik, bukan membuat konten baru yang memprovokasi. Putusan ini dianggap sebagai preseden bahwa siapa pun yang menyebarkan konten, meski bukan pembuatnya, dapat dikriminalisasi.

Kasus lain yang tak kalah penting adalah penyebaran video asusila mirip artis pada tahun 2022 yang melibatkan publik figur. Konten tersebut

menyebar dengan sangat cepat melalui platform pesan instan terenkripsi. Meskipun pelaku penyebaran pertama berhasil ditangkap dan dijerat dengan UU ITE dan UU Pornografi, video tersebut tetap beredar luas karena sifat enkripsi end-to-end yang tidak bisa diintersepsi. Kasus ini mengekspos kelemahan fundamental: hukum mampu menjerat beberapa orang, tetapi tidak mampu menghapus konten dari ruang digital setelah viral. Di sisi lain, korban dalam kasus ini, perempuan yang videonya disebar tanpa persetujuan, mengalami pengucilan sosial dan trauma mendalam, sementara efektivitas pemulihan hak korban masih dipertanyakan. Kedua kasus ini menegaskan bahwa pendekatan represif semata tidak akan pernah cukup; pencegahan melalui pendidikan dan desain platform yang aman sangat diperlukan (Wahyuni, 2024).

F. HARMONISASI REGULASI DAN MENUJU PENGATURAN YANG HOLISTIK

Menyadari persoalan fragmentasi dan ketidakpastian hukum, langkah harmonisasi regulasi menjadi mutlak. Pertama, perlu dipertimbangkan penyusunan undang-undang khusus tentang konten ilegal yang menyatukan berbagai ketentuan yang tersebar, dengan definisi yang lebih ketat dan spesifik. Undang-undang ini harus memberikan parameter objektif untuk setiap kategori konten ilegal, misalnya: apakah suatu konten dianggap "melanggar kesusilaan" harus dinilai berdasarkan konteks, audiens, dan medium, bukan sekadar isi

literalnya. Demikian pula "ujaran kebencian" harus menetapkan ambang batas berupa niat, dampak, dan konteks sosial yang jelas sebagaimana diatur dalam Rabat Plan of Action PBB.

Kedua, mekanisme pemblokiran dan takedown harus direformasi untuk memenuhi standar due process. Kominfo perlu menerbitkan laporan transparansi berkala yang merinci jumlah konten yang diblokir, dasar hukumnya, dan mekanisme banding yang tersedia. Harus ada lembaga pengawas independen atau pengadilan yang dapat menguji legalitas perintah pemblokiran. Ketiga, kerjasama internasional harus ditingkatkan. Selain ratifikasi Konvensi Budapest, Indonesia dapat mempelopori perjanjian regional di ASEAN tentang penanganan konten ilegal, mengingat karakter budaya dan hukum yang lebih dekat.

Keempat, regulasi platform harus diperkuat. Korporasi platform harus diwajibkan memiliki pusat kepatuhan di Indonesia dengan sistem respons yang cepat dan akuntabel. Regulasi dapat mendorong pengembangan automated filtering yang etis dan proporsional, serta penegakan kewajiban untuk memberitahu dan memulihkan hak pengguna yang kontennya dihapus. Pada akhirnya, penanganan konten ilegal harus proporsional, tidak hanya represif tetapi juga preventif, dengan melibatkan edukasi literasi digital yang massif (Harahap & Nugroho, 2023).

G. KESIMPULAN

Kerangka hukum Indonesia dalam menanggulangi penyebaran konten ilegal di internet bersifat multi-layer dan fragmentaris. UU ITE sebagai payung utama, bersama dengan undang-undang sektoral lainnya, memberikan dasar pemidanaan yang cukup luas. Namun, kelemahan fundamental terletak pada ketidakjelasan definisi, tumpang tindih delik, dan mekanisme takedown administratif yang minim pengawasan yudisial. Menjawab rumusan masalah, tantangan yuridis utama meliputi ketidakpastian hukum akibat multitafsir, kesenjangan yurisdiksi dalam ekosistem digital lintas batas, serta ketegangan antara kebutuhan akan ketertiban dan perlindungan kebebasan berekspresi. Studi kasus menegaskan bahwa represi saja tidak cukup dan bahkan dapat menimbulkan ketidakadilan baru.

Rekomendasi yang diajukan adalah: pertama, penyusunan undang-undang konten ilegal yang harmonis dan definitif; kedua, pembentukan otoritas pengawas independen untuk mengawasi pelaksanaan takedown; ketiga, ratifikasi Konvensi Budapest untuk memperkuat kerjasama internasional; dan keempat, pengarusutamaan literasi digital yang kritis di seluruh jenjang pendidikan. Dengan pendekatan yang holistik, Indonesia dapat menciptakan ruang siber yang aman tanpa mengorbankan demokrasi.

REFERENSI:

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

Butt, S., & Lindsey, T. (2023). Indonesian Law: Continuity and Change. Oxford University Press.

DeNardis, L. (2020). The Internet in Everything: Freedom and Security in a World with No Off Switch. Yale University Press.

Fitriani, R. (2023). Transparansi Pemblokiran Konten dan Akuntabilitas Kominfo. Jurnal Media dan Hukum, 11(1), 33–50.

Harahap, A., & Nugroho, B. (2023). Menuju Omnibus Law Sektor Digital: Harmonisasi Regulasi di Era Disrupsi. Jurnal Legislasi Indonesia, 20(2), 112–130.

Prasetyo, B. (2024). Ketidakpastian Hukum Pasal 28 Ayat (2) UU ITE. Jurnal Hukum dan Masyarakat, 16(1), 88–107.

Setiawan, R. (2023). Pengawasan Digital dan Batas-Batas Privasi di Indonesia. Jurnal Konstitusi, 20(4), 801–822. https://doi.org/10.31078/jk2045

Wahyuni, T. (2024). Tanggung Jawab Platform dalam Kasus Revenge Porn. Jurnal Hukum dan Etika Digital, 2(1), 40–58.

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).

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Lembaran Negara Tahun 2022 Nomor 196, Tambahan Lembaran Negara Nomor 6820).

ISSN: 2338 4638

Volume 7 Nomor 7 (2023)

'ADALAH

Buletin Hukum & Keadilan

Perkembangan Cybercrime dan Dampaknya terhadap Keamanan Nasional Indonesia: Analisis Ancaman Asimetris dan Strategi Ketahanan Siber

Gilang Rizki Aji Putra*

Universitas Islam Negeri Syarif Hidayatullah Jakarta

10.15408/adalah.v7i7.51842

Abstract:
Cybercrime has transformed from conventional computer-based offenses into a multidimensional threat targeting critical infrastructure, political stability, and national economic resilience. This article analyzes the evolving modus operandi of cybercrime in Indonesia over the past decade and assesses its impact on national security within a multidimensional security framework. Using normative legal research with conceptual, statutory, and case study approaches, the study finds that cybercrime in Indonesia has progressed from online fraud and hacking to structured cyberattacks against national data infrastructure, digital espionage, and large-scale disinformation campaigns threatening political stability. The analysis indicates that existing regulatory frameworks, including the Electronic Information and Transactions Law and the Personal Data Protection Law, as well as institutional bodies such as the National Cyber and Crypto Agency (BSSN), remain largely reactive and insufficient to address the asymmetric and transnational nature of these threats. The article concludes that cybercrime constitutes an existential challenge to Indonesia's digital sovereignty and requires comprehensive legislative, institutional, and regional intelligence cooperation reforms.

Keywords: Cybercrime, National Security, Asymmetric Threats, BSSN, Hybrid Warfare.

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

A. PENDAHULUAN

Perkembangan *cybercrime* global menunjukkan eskalasi yang mengkhawatirkan. *World Economic Forum* dalam *Global Risks Report* 2024 menempatkan serangan siber sebagai salah satu dari lima risiko global teratas, bersama dengan kegagalan mitigasi perubahan iklim dan konflik geopolitik. Biaya ekonomi yang diakibatkan oleh *cybercrime* global diperkirakan mencapai 10,5 triliun dolar AS pada tahun 2025, menjadikannya sebagai ekonomi kriminal terbesar ketiga di dunia setelah perdagangan narkoba dan pemalsuan (Brenner, 2022). Angka ini menunjukkan bahwa cybercrime bukan lagi sekadar kenakalan digital, melainkan telah menjadi industri kejahatan terorganisasi yang sistematis, profesional, dan lintas negara.

Di Indonesia, eskalasi cybercrime memperlihatkan pola yang serupa. Laporan tahunan Badan Siber dan Sandi Negara (BSSN) mencatat peningkatan lebih dari 300% anomali lalu lintas data dan serangan siber dalam empat tahun terakhir, dengan sektor perbankan, pemerintahan, dan kesehatan sebagai target utama (BSSN, 2023). Lebih dari itu, modus operandi yang berkembang tidak lagi terbatas pada penipuan daring (*online fraud*) atau peretasan (*hacking*) sederhana, tetapi telah merambah ke ranah ransomware terhadap fasilitas publik, pencurian data strategis berskala besar, hingga kampanye disinformasi politik yang terstruktur dan sistematis. Fenomena ini menimbulkan pertanyaan

serius: apabila *cybercrime* kini mampu melumpuhkan layanan publik dan memanipulasi persepsi politik, apakah ia masih bisa dikategorikan sebagai masalah kriminal biasa, ataukah sudah bertransformasi menjadi ancaman nyata bagi keamanan nasional?

Sayangnya, perspektif arus utama di Indonesia masih cenderung menempatkan cybercrime dalam kerangka hukum pidana biasa, belum sepenuhnya mengintegrasikannya ke dalam doktrin pertahanan dan keamanan negara. Padahal, konsep keamanan nasional kontemporer telah bergeser dari pendekatan tradisional yang berfokus pada ancaman militer menuju pendekatan multidimensional yang mencakup keamanan ekonomi, politik, sosial, dan informasi (Buzan, Wæver, & de Wilde, 1998). Rumusan masalah dalam artikel ini adalah: Pertama, bagaimana dinamika perkembangan modus dan skala *cybercrime* di Indonesia dalam perspektif ancaman terhadap keamanan nasional? Kedua, mengapa kerangka hukum dan kelembagaan yang ada belum mampu merespons secara efektif, dan strategi apa yang harus ditempuh? Tujuannya adalah untuk menganalisis cybercrime sebagai ancaman asimetris yang memiliki dampak struktural terhadap kedaulatan digital nasional, serta merumuskan pendekatan yang lebih holistik dalam menanganinya.

B. *CYBERCRIME* DALAM PARADIGMA KEAMANAN MULTIDIMENSIONAL

Untuk memahami dampak *cybercrime* terhadap keamanan nasional, diperlukan perluasan kerangka analisis dari kriminologi konvensional menuju studi keamanan kritis. *Copenhagen School* melalui teori sekuritisasi (*securitization*) yang dikembangkan oleh Buzan et al. (1998) menawarkan kerangka yang relevan. Menurut teori ini, sebuah isu dapat dikategorikan sebagai ancaman keamanan jika ia dieksistensialkan oleh aktor negara sebagai ancaman terhadap objek referensi, seperti kedaulatan negara, integritas teritorial, atau stabilitas masyarakat dan memerlukan tindakan luar biasa di luar prosedur politik normal. Dalam konteks ini, *cybercrime* yang semula dipandang sebagai isu kriminal telah mengalami proses sekuritisasi di banyak negara, termasuk melalui pembentukan komando siber militer dan anggaran keamanan siber yang masif.

Ancaman siber, termasuk *cybercrime*, memiliki karakteristik asimetris. Pelaku bisa individu, kelompok kriminal, atau aktor negara yang menggunakan *proxy*, dengan biaya serangan yang relatif murah tetapi dampak yang luar biasa besar. Konsep *asymmetric threat* dalam keamanan siber menggambarkan situasi di mana aktor yang lemah secara konvensional dapat menimbulkan kerusakan yang tidak proporsional terhadap negara yang kuat (Libicki, 2009). Serangan terhadap infrastruktur

informasi vital seperti jaringan listrik, sistem perbankan, atau pusat data pemerintahan dapat melumpuhkan fungsi-fungsi dasar negara tanpa perlu mengerahkan satu pun pasukan militer. Selain itu, munculnya fenomena *cyber-enabled crime*, yaitu kejahatan yang menggunakan infrastruktur digital sebagai pengganda kekuatan, mengaburkan batas antara kejahatan ekonomi dan ancaman terhadap keamanan nasional.

Dalam spektrum yang lebih luas, *cybercrime* telah menjadi komponen integral dari *hybrid warfare* strategi konflik yang menggabungkan operasi militer konvensional dengan perang informasi, perang siber, dan perang ekonomi. Kampanye disinformasi yang didanai oleh aktor kriminal atau negara asing untuk mempolarisasi masyarakat, melemahkan legitimasi pemerintah, atau memengaruhi hasil pemilihan umum adalah contoh nyata *hybrid threat* (Schmitt, 2017). Di sinilah letak urgensi pembahasan: Indonesia harus membaca *cybercrime* bukan hanya dalam KUHP atau UU ITE, tetapi juga dalam strategi pertahanan dan doktrin keamanan nasional.

C. PERKEMBANGAN MODUS *CYBERCRIME* DAN DAMPAKNYA TERHADAP PILAR KEAMANAN NASIONAL

1. Dari Penipuan Daring ke Serangan Sistematis terhadap Infrastruktur Publik

Modus *cybercrime* di Indonesia telah mengalami eskalasi kualitatif. Lima tahun lalu,

dominasi pemberitaan masih terfokus pada phishing, penipuan *e-commerce*, dan carding. Kini, ancaman yang paling mengkhawatirkan adalah serangan *ransomware* terhadap institusi pemerintahan. Insiden serangan terhadap Pusat Data Nasional Sementara (PDNS) pada Juni 2024 oleh varian Brain Cipher merupakan *game changer*. Server-server yang menyimpan data berbagai kementerian dan layanan publik disandera, menyebabkan lumpuhnya layanan imigrasi, perizinan, dan administrasi publik lainnya selama berhari-hari. Serangan ini jelas menunjukkan bahwa kedaulatan digital Indonesia sangat rentan. Apabila pusat data yang mengelola data kependudukan, keamanan, atau pertahanan berhasil dibobol, implikasinya tidak hanya kerugian finansial, tetapi juga ancaman terhadap kerahasiaan negara dan keselamatan warga (Nugroho, 2024).

Serangan terhadap infrastruktur kritis adalah direct assault terhadap keamanan nasional. Ia berbeda dari penipuan daring yang merugikan individu. Kerugiannya bersifat massal dan sistemik, menurunkan kepercayaan publik terhadap kemampuan negara, dan membuka celah bagi sabotase lebih lanjut. Dalam konteks hukum internasional, serangan siber terhadap infrastruktur kritis suatu negara dapat dikategorikan sebagai pelanggaran kedaulatan atau bahkan *use of force* jika memiliki dampak setara dengan serangan bersenjata (Schmitt, 2017). Namun, karena sulitnya atribusi

yakni memastikan secara teknis dan politis siapa pelaku di balik serangan negara seringkali kesulitan untuk memberikan respons yang proporsional.

2. Spionase Digital dan Pencurian Data Strategis

Kasus "Bjorka" yang mencuat pada tahun 2022 dan 2023 menjadi fenomena spionase digital yang paling mengganggu. Seorang atau sekelompok aktor anonim berhasil meretas dan membocorkan data-data sensitif milik pejabat tinggi negara, dokumen kementerian, serta data pribadi warga negara. Kebocoran ini tidak hanya mempermalukan pemerintah di forum internasional, tetapi juga mengekspos kerentanan sistem komunikasi dan penyimpanan data rahasia negara. Dalam doktrin intelijen, hilangnya data rahasia akibat spionase baik yang dilakukan oleh aktor negara maupun non-negara adalah pukulan langsung terhadap keamanan nasional karena informasi tersebut dapat dimanfaatkan oleh pihak asing untuk kepentingan politik, ekonomi, atau militer (ID-SIRTII, 2023).

Lebih jauh, maraknya perdagangan data pribadi di dark web menimbulkan ancaman serius terhadap keamanan warga negara. Data Nomor Induk Kependudukan (NIK), data perbankan, dan riwayat kesehatan yang bocor dapat digunakan untuk penipuan identitas, spionase korporasi, hingga profiling politik. Akumulasi data ini, jika jatuh ke tangan aktor yang berniat destabilisasi, dapat menjadi senjata untuk pemerasan massal atau

manipulasi elektoral. Dalam konteks ini, *cybercrime* pencurian data bukan lagi sekadar pelanggaran privasi, melainkan fondasi bagi ancaman *hybrid* yang lebih luas.

3. Disinformasi Terstruktur dan Ancaman terhadap Stabilitas Politik

Perkembangan mutakhir *cybercrime* yang paling berdampak terhadap keamanan nasional adalah penyalahgunaan platform digital untuk kampanye disinformasi. Pada Pemilihan Umum 2024, berbagai riset menunjukkan adanya jejaring akun bot dan *coordinated inauthentic behavior* yang menyebarkan narasi polarisasi, ujaran kebencian, serta klaim kecurangan terstruktur (Mulyadi, 2024). Banyak dari kampanye ini bukan sekadar ulah buzzer politik, melainkan bagian dari bisnis jasa *disinformation-as-a-service* yang digerakkan oleh motif ekonomi. Artinya, pelaku menyewakan infrastruktur disinformasi kepada pihak-pihak yang membayar, tanpa peduli terhadap dampak sosialnya.

Efek disinformasi terhadap keamanan nasional sangat nyata: polarisasi sosial akut dapat melemahkan kohesi nasional, memicu konflik horizontal, dan merusak kepercayaan publik terhadap lembaga demokrasi. Dalam jangka panjang, masyarakat yang terfragmentasi menjadi lahan subur bagi radikalisasi dan ekstremisme. Ketika polarisasi mencapai titik tertentu, legitimasi pemerintah untuk memerintah pun dipertanyakan,

menciptakan krisis konstitusional. Maka, memerangi disinformasi bukan hanya soal melindungi individu dari hoaks, melainkan soal mempertahankan kedaulatan politik negara. Sayangnya, pendekatan hukum Indonesia saat ini masih melalui kacamata pasal-pasal penyebaran berita bohong (Pasal 28 ayat (1) UU ITE) yang bersifat reaktif dan individual, belum mampu membongkar infrastruktur dan model bisnis di balik industri disinformasi (Harahap & Nugroho, 2023).

4. Dampak Ekonomi dan Kedaulatan Finansial Digital

Cybercrime juga memukul pilar ekonomi keamanan nasional. Sektor jasa keuangan digital adalah target favorit bagi sindikat penipuan dan peretasan. Kasus penipuan *binary option* yang melibatkan influencer nasional mencatat kerugian hingga puluhan triliun rupiah. Selain itu, serangan terhadap *payment gateway* dan dompet elektronik berpotensi melumpuhkan sistem pembayaran nasional. Ketika masyarakat kehilangan kepercayaan terhadap keamanan transaksi digital, dampak ekonominya sangat besar, terutama bagi negara yang sedang gencar mendorong digitalisasi keuangan seperti Indonesia. Ancaman terhadap stabilitas sistem keuangan adalah salah satu dimensi keamanan ekonomi yang diakui dalam doktrin pertahanan siber (BSSN, 2023). Tanpa keamanan siber yang andal, cita-cita Indonesia menjadi digital economy powerhouse hanya akan menjadi ilusi.

D. KELEMAHAN STRUKTURAL DALAM PENANGANAN *CYBERCRIME* DI INDONESIA

Mengapa *cybercrime* yang dampaknya begitu nyata terhadap keamanan nasional masih sulit ditanggulangi? Setidaknya ada tiga kelemahan struktural. Pertama, legal gap dan fragmentasi kelembagaan. Indonesia belum memiliki Undang-Undang Keamanan dan Ketahanan Siber yang komprehensif yang mengintegrasikan aspek pertahanan, penegakan hukum, intelijen, dan diplomasi siber. BSSN sebagai otoritas keamanan siber masih memiliki kewenangan yang terbatas, lebih fokus pada audit dan respons insiden, bukan pada koordinasi penindakan dan ofensif siber. Sementara itu, Polri, TNI, Kominfo, dan BIN memiliki mandat parsial yang seringkali tumpang tindih.

Kedua, kapasitas sumber daya manusia dan teknologi yang asimetris. Jumlah pakar forensik digital dan analis ancaman siber di Indonesia sangat terbatas, baik di sektor publik maupun swasta. Laboratorium forensik digital belum merata di seluruh daerah, sementara pelaku *cybercrime* terus meningkatkan kecanggihan alat dan metodenya. Ketiga, ketiadaan kerangka kerjasama internasional yang kuat. *Cybercrime* bersifat transnasional, namun Indonesia belum meratifikasi Konvensi Budapest dan belum memiliki perjanjian ekstradisi dan bantuan hukum timbal balik yang memadai dengan negara-negara yang menjadi basis operasi sindikat

siber (Santoso, 2023). Akibatnya, aktor utama di balik banyak serangan besar tetap bebas berkeliaran di luar negeri tanpa dapat disentuh.

E. MENEMPATKAN *CYBERCRIME* SEBAGAI ANCAMAN KEAMANAN NASIONAL

Untuk merespons secara efektif, Indonesia harus merekonstruksi paradigma penanganan cybercrime. Perubahan pertama adalah mengadopsi doktrin *active defense* dan *deterrence by denial*. Negara tidak cukup hanya memasang tembok, tetapi harus memiliki kemampuan untuk mendeteksi, melacak, dan membalas serangan siber secara proporsional. Ini memerlukan pembentukan komando siber yang terintegrasi di bawah TNI atau lembaga khusus, yang juga diperkuat dengan regulasi yang jelas tentang *rules of engagement* di ranah siber.

Kedua, legislasi harus segera diselesaikan. Rancangan Undang-Undang Keamanan dan Ketahanan Siber yang sudah digodok bertahun-tahun harus segera disahkan. Undang-undang ini harus memberikan kewenangan yang memadai kepada otoritas siber nasional, menetapkan standar keamanan yang ketat bagi infrastruktur informasi vital, serta memberikan perlindungan hukum bagi aparat yang melakukan operasi siber defensif. Ketiga, kerjasama internasional harus diintensifkan. Indonesia harus segera meratifikasi Konvensi Budapest dan aktif dalam ASEAN *Cybersecurity Cooperation Strategy.* Hanya dengan kolaborasi lintas

batas, upaya penegakan hukum tidak akan berhenti pada aktor lapangan, tetapi mampu mencapai otak sindikat di kancah global (Kusumawardhani, 2024).

Keempat, literasi keamanan siber dan ketahanan masyarakat terhadap disinformasi harus menjadi program nasional yang masif. Keamanan siber tidak bisa hanya bertumpu pada pemerintah; ia harus menjadi tanggung jawab bersama antara negara, sektor swasta, akademisi, dan masyarakat sipil (*multistakeholder approach*). Masyarakat yang cerdas secara digital adalah benteng paling kokoh melawan cybercrime.

F. KESIMPULAN

Cybercrime di Indonesia telah melampaui definisi kriminal biasa. Modusnya yang terus berevolusi dari *ransomware* terhadap pusat data nasional, spionase dan kebocoran data strategis, hingga kampanye disinformasi yang mempolarisasi bangsa telah membuktikan bahwa ia adalah ancaman nyata bagi keamanan nasional dalam dimensi politik, ekonomi, dan sosial. Menjawab rumusan masalah pertama, *cybercrime* adalah ancaman asimetris yang memiliki kapasitas melumpuhkan fungsi vital negara dan menggerogoti kedaulatan digital. Menjawab rumusan kedua, kelemahan regulasi yang fragmentaris, kapasitas SDM yang timpang, dan minimnya kerjasama internasional adalah hambatan utama yang membuat respons negara masih jauh dari memadai.

Rekomendasi yang diajukan mencakup: pertama, percepatan pengesahan Undang-Undang Keamanan dan Ketahanan Siber yang memberikan kewenangan penuh kepada otoritas siber nasional; kedua, pembangunan kapasitas ofensif dan defensif siber melalui pendidikan dan rekrutmen talenta; ketiga, ratifikasi Konvensi Budapest dan penguatan aliansi siber regional; serta keempat, integrasi perspektif *cybercrime* ke dalam doktrin pertahanan negara. Tanpa langkah-langkah strategis ini, Indonesia akan terus menjadi raksasa digital yang rentan, mudah dilumpuhkan oleh entitas yang tidak terlihat dan tidak terprediksi.

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.

Buzan, B., Wæver, O., & de Wilde, J. (1998). Security: A New Framework for Analysis. Lynne Rienner Publishers.

Harahap, A., & Nugroho, B. (2023). Menuju Tata Kelola Multi-Pemangku Kepentingan dalam Penegakan Hukum Siber Indonesia. Jurnal Legislasi Indonesia, 20(4), 512–530.

ID-SIRTII. (2023). Laporan Aktivitas Serangan Siber terhadap Domain Indonesia tahun 2022.

Indonesia Security Incident Response Team on Internet Infrastructure.

Kusumawardhani, A. (2024). Kecerdasan Buatan dan Kekosongan Hukum Pidana di Indonesia. Jurnal Hukum Siber, 6(1), 15–32.

Libicki, M. C. (2009). Cyberdeterrence and Cyberwar. RAND Corporation.

Mulyadi, L. (2024). Disinformasi dan Kedaulatan Politik: Studi Pemilu 2024. Jurnal Komunikasi dan Politik, 12(1), 45–63.

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

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

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