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,