JRH
JURNAL REALITAS HUKUM
P-ISSN -
E-ISSN -
https://jurnal.prestasiku.org
VOLUME 2
NO. 2
MARET 2026

KAJIAN PENEGAKAN HUKUM TINDAK PIDANA CYBERCRIME DI INDONESIA: ANALISIS IMPLEMENTASI UU ITE DAN TANTANGAN DALAM PRAKTIK

Paulana Christian Suryawin[1], Muhammad Raihan Firdaus[2], Eti Haryati[3], Abdul Rahim[4], Prasetia Randiana[5]

[1]*Universitas Langlangbuana, paulana168@gmail.com[1]*
[2]*Universitas Langlangbuana, mraihanfrdaus@gmai.com[2]*
[3]*Universitas Langlangbuana, chintyaa93@yahoo.com[3]*
[4]*Universitas Langlangbuana, abdulrahimbrigade98@gmail.com[4]*
[5]*Universitas Langlangbuana, aangprasetia21@gmail.com[5]*

ABSTRAK

Perkembangan teknologi digital membawa dampak positif sekaligus memunculkan ancaman kejahatan siber yang semakin kompleks di Indonesia. Penelitian ini bertujuan menganalisis implementasi penegakan hukum tindak pidana *cybercrime* dan mengidentifikasi hambatan yang dihadapi aparat penegak hukum dalam praktik. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan deskriptif analitis melalui studi kepustakaan terhadap peraturan perundang-undangan dan literatur hukum yang relevan. Hasil penelitian menunjukkan bahwa Indonesia telah memiliki landasan yuridis melalui UU ITE dan regulasi terkait yang melibatkan koordinasi kepolisian, kejaksaan, dan pengadilan dalam sistem peradilan pidana. Namun implementasi penegakan hukum menghadapi hambatan berupa keterbatasan kompetensi sumber daya manusia dalam memahami aspek teknis teknologi informasi, kompleksitas pembuktian forensik digital, permasalahan yurisdiksi lintas negara, serta minimnya infrastruktur dan anggaran. Penelitian ini menyimpulkan bahwa efektivitas penegakan hukum *cybercrime* memerlukan pendekatan holistik melalui peningkatan kapasitas aparat, investasi infrastruktur teknologi, penguatan kerjasama internasional, dan sinergi seluruh pemangku kepentingan dengan dukungan komitmen politik dan anggaran memadai dari pemerintah.
Kata Kunci : *Cybercrime*, Forensik Digital, Penegakan Hukum, Sistem Peradilan Pidana, UU ITE

PENDAHULUAN

Kemudahan akses internet membawa dampak positif sekaligus membuka celah munculnya bentuk kejahatan baru yang berbasis digital. Kejahatan siber atau *cybercrime* menjadi ancaman serius bagi keamanan nasional dan stabilitas ekonomi Indonesia.[1] Perkembangan digital yang masif menciptakan ruang virtual tanpa batas geografis sehingga memudahkan pelaku kejahatan melakukan aksinya. Fenomena ini menuntut adanya respons hukum yang adaptif dan komprehensif dari negara. Statistik menunjukkan peningkatan kasus *cybercrime* setiap tahunnya dengan modus operandi yang semakin canggih dan terorganisir[2]. Kerugian material maupun immaterial yang ditimbulkan mencapai triliunan rupiah dan

[1] Hapsari, R. D., & Pambayun, K. G. (2023). Ancaman cybercrime di Indonesia: Sebuah tinjauan pustaka sistematis. Jurnal Konstituen, 5(1), hlm. 2-3.

[2] Agustin, N. A., & Firdos, R. M. (2024). Studi literatur: Ancaman cybercrime di Indonesia dan pentingnya pemahaman akan fenomena kejahatan digital. Jurnal Mahasiswa Teknik Informatika, 3(1), hlm. 127.

berdampak pada berbagai sektor kehidupan. Kompleksitas permasalahan ini memerlukan kajian mendalam tentang efektivitas penegakan hukum pidana di Indonesia terhadap tindak kejahatan siber.

Indonesia telah merespons ancaman *cybercrime* melalui pembentukan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Regulasi ini menjadi payung hukum utama dalam mengatur dan menindak berbagai bentuk kejahatan di dunia maya.[3] UU ITE kemudian mengalami revisi melalui UU Nomor 19 Tahun 2016 untuk menyempurnakan ketentuan yang dianggap multitafsir. Perubahan tersebut dimaksudkan untuk memberikan kepastian hukum sekaligus melindungi kebebasan berekspresi masyarakat dalam ruang digital. Regulasi terbaru melalui UU Nomor 1 Tahun 2024 semakin memperkuat landasan yuridis penanganan kejahatan siber di Indonesia.[4] Keberadaan perangkat hukum ini menunjukkan keseriusan pemerintah dalam mengatasi persoalan *cybercrime* yang terus berkembang.

Implementasi UU ITE dalam praktik penegakan hukum menghadapi berbagai tantangan yang kompleks dan multidimensional. Keterbatasan sumber daya manusia yang memiliki kompetensi di bidang teknologi informasi menjadi hambatan utama dalam proses penyidikan.[5] Aparat penegak hukum seringkali kesulitan mengumpulkan dan menganalisis bukti digital yang bersifat teknis dan memerlukan keahlian khusus. Minimnya infrastruktur forensik digital di berbagai daerah mempersulit upaya penanganan kasus *cybercrime* secara optimal. Karakteristik kejahatan siber yang bersifat lintas yurisdiksi menimbulkan persoalan dalam penetapan *locus delicti* atau tempat terjadinya kejahatan.[6] Koordinasi antar lembaga penegak hukum dan instansi terkait masih belum berjalan dengan baik dan terintegrasi. Permasalahan teknis yuridis ini berdampak pada rendahnya tingkat penyelesaian kasus *cybercrime* yang dilaporkan oleh masyarakat kepada pihak berwajib.[7]

Berbagai bentuk kejahatan siber terus bermunculan dengan modus yang semakin canggih mengikuti perkembangan teknologi digital terkini. *Hacking* dan *cracking* sistem informasi

[3] Handoyo, B., Husamuddin, M. Z., & Rahma, I. (2024). Tinjauan Yuridis Penegakkan Hukum Kejahatan Cyber Crime Studi Implementasi Undang-Undang Nomor 11 Tahun 2008. MAQASIDI: Jurnal Syariah Dan Hukum,hlm. 41.

[4] Fairuzzen, M. R., Putra, A. A., Reihan, A., & SH, L. P. (2024). Perkembangan Hukum dan Kejahatan Siber "Cybercrime" di Indonesia. Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory, 2(1), hlm. 142.

[5] Bego, K. C., Aziz, F. R., Rahmad, R. A., & Budianto, H. (2025). Tindak Pidana Cybercrime: Tantangan Hukum Pidana Dalam Menanggulangi Kejahatan di Dunia Maya. Jurnal Kolaboratif Sains, 8(1), hlm. 508.

[6] Purwaningsih, R., & Putranto, R. D. (2023). Tinjauan yuridis terhadap penetapan locus delicti dalam kejahatan dunia maya (cyber crime) berkaitan dengan upaya pembaharuan hukum pidana di Indonesia. Mimbar Keadilan, 16(1), hlm. 132.

[7] Ibid., hlm. 133.

menjadi ancaman serius bagi keamanan data pribadi maupun data institusi pemerintah.[8] *Phishing* dan *social engineering* memanfaatkan kelengahan korban untuk mencuri informasi sensitif seperti *password* dan data perbankan. *Carding* atau pencurian data kartu kredit mengakibatkan kerugian finansial yang sangat besar bagi para korban.[9] Penyebaran konten ilegal seperti pornografi dan ujaran kebencian merusak tatanan sosial dan moral masyarakat Indonesia. Penipuan *online* melalui *marketplace* palsu atau investasi bodong semakin marak terjadi di platform media sosial.[10]

Penegakan hukum terhadap *cybercrime* memerlukan pendekatan khusus yang berbeda dengan penanganan kejahatan konvensional pada umumnya. Sifat *virtual* dari ruang siber membuat pelaku dapat dengan mudah menghilangkan jejak digital atau berada di luar yurisdiksi.[11] Pembuktian dalam kasus *cybercrime* sangat bergantung pada kemampuan mengamankan dan menganalisis barang bukti elektronik dengan prosedur yang tepat. Aparat penegak hukum harus memahami teknologi enkripsi, protokol internet, dan berbagai aplikasi yang digunakan dalam kejahatan siber. Keterlambatan dalam pengamanan bukti digital dapat mengakibatkan hilangnya data penting yang diperlukan dalam proses penuntutan.[12] Kerjasama dengan penyedia layanan internet dan platform digital menjadi krusial dalam proses penyidikan kasus *cybercrime*. Hambatan teknis dan yuridis ini seringkali menyebabkan kasus *cybercrime* tidak dapat diproses hingga ke tahap persidangan.

Upaya penanggulangan *cybercrime* di Indonesia dilakukan melalui pendekatan preventif dan represif secara bersamaan dan saling melengkapi. Kepolisian melakukan patroli siber untuk memantau aktivitas mencurigakan di ruang digital dan mengidentifikasi potensi kejahatan.13 Edukasi kepada masyarakat tentang literasi digital dan cara melindungi diri dari ancaman *cybercrime* terus dilakukan secara masif. Program sosialisasi hukum terkait UU ITE diselenggarakan untuk meningkatkan kesadaran masyarakat tentang konsekuensi hukum kejahatan siber. Tindakan *take down* atau pemblokiran konten ilegal dilakukan sebagai langkah cepat mencegah penyebaran informasi yang merugikan. Pemberian teguran langsung kepada

[8] Sitompul, F., Manik, A. P. P., Sinaga, C. D., Purba, A. T., & Satria, A. (2024). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Hukum Indonesia. Jaksa: Jurnal Kajian Ilmu Hukum Dan Politik, 2(2), hlm. 224.

[9] Alamsyah, A., Santoso, E., & Pranadita, N. (2025). Kajian Terhadap Kejahatan Carding Sebagai Bentuk Cybercrime Di Indonesia. Iustitia Omnibus: Jurnal Ilmu Hukum, 6(2), hlm. 62.

[10] Ibid.

[11] Febriansyah, F. I., Indiantoro, A., & Ikhwan, A. (2023). Model Kejahatan Dunia Maya (Cybercrime) Sebagai Upaya Pembentukan Hukum Nasional. Legal Standing: Jurnal Ilmu Hukum, 7(2), hlm. 246.

[12] Pansariadi, R. S. B., & Soekorini, N. (2023). Tindak Pidana Cyber Crime dan Penegakan Hukumnya. Binamulia Hukum, 12(2), hlm. 292.

[13] Wijaya, T. H. D. (2022). Penerapan sanksi sosial sebagai alternatif pemidanaan terhadap pelaku tindak pidana kejahatan siber (cyber crime). Al-Qisth Law Review, 5(2), hlm. 384-385.

pelaku pelanggaran ringan menjadi alternatif sebelum dilakukan tindakan hukum lebih lanjut.[14] Pendekatan represif melalui penegakan hukum pidana tetap menjadi ultimum remedium ketika upaya preventif tidak memberikan hasil.

Kajian tentang penegakan hukum *cybercrime* menjadi sangat penting mengingat dampaknya yang luas terhadap berbagai aspek kehidupan masyarakat. Penelitian ini berupaya menganalisis implementasi UU ITE dalam praktik penegakan hukum pidana terhadap kejahatan siber di Indonesia. Identifikasi terhadap hambatan dan tantangan yang dihadapi aparat penegak hukum menjadi fokus utama dalam kajian ini. Evaluasi terhadap efektivitas regulasi yang ada serta kesesuaiannya dengan perkembangan teknologi akan dibahas secara mendalam dan komprehensif. Kajian ini juga akan mengeksplorasi berbagai upaya yang telah dilakukan oleh pemerintah dalam menanggulangi ancaman *cybercrime*.

Urgensi penelitian ini semakin kuat mengingat prediksi bahwa kejahatan siber akan terus meningkat seiring digitalisasi yang semakin masif. Penggunaan artificial *intelligence* dan *big data* oleh pelaku kejahatan menciptakan ancaman baru yang lebih sophisticated dan sulit dideteksi.[15] Perlindungan data pribadi menjadi isu krusial setelah berlakunya UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Integrasi antara regulasi perlindungan data dengan UU ITE perlu dikaji untuk memastikan tidak ada tumpang tindih atau kekosongan hukum. Peran sektor swasta dan masyarakat sipil dalam ekosistem keamanan siber juga perlu mendapat perhatian dalam kajian penegakan hukum.[16] Membangun budaya keamanan siber yang kuat memerlukan sinergi antara pemerintah, sektor bisnis, akademisi, dan masyarakat umum. Penelitian ini diharapkan dapat memberikan pemahaman komprehensif tentang penegakan hukum *cybercrime* di Indonesia.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan yuridis normatif untuk mengkaji penegakan hukum tindak pidana *cybercrime* di Indonesia. Pendekatan yuridis normatif dipilih karena fokus kajian tertuju pada analisis peraturan perundang-undangan. Jenis penelitian ini bersifat deskriptif analitis yang bertujuan memberikan gambaran sistematis tentang fakta hukum dan menganalisis permasalahan. Sumber data yang digunakan adalah data sekunder yang terdiri dari sumber primer dan sekunder yang relevan dengan penelitian. Bahan hukum primer mencakup UU Nomor 11 Tahun 2008 tentang ITE beserta perubahannya, UU Nomor 1 Tahun 2023 tentang KUHP, dan UU Nomor 27 Tahun

[14] Maskun, S. H. (2022). Kejahatan Siber (Cyber Crime): Suatu Pengantar. Prenada Media, hlm. 156.

[15] Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing cybercrime: Definitions, typologies and taxonomies. Forensic Sciences, 2(2), 392-393.

[16] Bahri, I. S. (2023). Cyber Crime dalam Sorotan Hukum Pidana (Edisi 2023). Bahasa Rakyat, 78-79.

2022 tentang Perlindungan Data Pribadi. Bahan hukum sekunder berupa buku-buku teks dan artikel ilmiah yang membahas tentang *cybercrime* dan penegakan hukumnya. Teknik pengumpulan data dilakukan melalui studi kepustakaan dengan cara mengumpulkan, membaca, mencatat, dan menganalisis berbagai literatur.

Analisis data dalam penelitian ini menggunakan metode kualitatif dengan pendekatan interpretasi sistematis dan analisis konseptual terhadap norma hukum yang berlaku. Teknik analisis yang digunakan adalah analisis isi atau *content analysis* terhadap substansi peraturan perundang-undangan dan literatur hukum yang relevan. Penarikan kesimpulan dilakukan secara deduktif dengan berangkat dari premis umum berupa teori dan ketentuan hukum. Validitas data dijaga melalui triangulasi sumber dengan membandingkan berbagai literatur dan memverifikasi konsistensi informasi dari berbagai referensi akademis yang kredibel. Hasil analisis kemudian disajikan secara deskriptif dalam bentuk uraian naratif yang sistematis untuk menjawab permasalahan penelitian.

PEMBAHASAN DAN DISKUSI

Studi Kasus *Cybercrime* dan Pola Kejahatan Digital di Indonesia

Pusat Data Nasional Sementara mengalami serangan *ransomware* Brain Cipher pada Juni 2024 yang melumpuhkan sistem layanan publik. Serangan dimulai tanggal 17 Juni dengan mematikan Windows Defender sehingga *ransomware* dapat beroperasi tanpa hambatan di server PDN. Layanan imigrasi di bandara mengalami down pada 20 Juni dan gangguan meluas ke berbagai layanan publik online nasional. Pemerintah mengonfirmasi jenis *ransomware* empat hari setelahnya dan pelaku meminta maaf kepada masyarakat Indonesia atas kekacauan yang terjadi. Kasus ini menunjukkan kerentanan infrastruktur digital pemerintah terhadap serangan ransomware yang terorganisir. Dampak sosial dari serangan ini sangat luas karena mengganggu pelayanan publik yang bersifat esensial bagi masyarakat.

Hacker Bjorka menjadi sorotan publik sepanjang tahun 2022 melalui serangkaian aksi pencurian data milik lembaga pemerintahan dan institusi penting. Setidaknya tujuh kasus besar pembobolan data dilakukan oleh Bjorka di tahun 2022 yang menggemparkan jagat maya Indonesia. Pelaku mengaku berhasil membobol situs Kementerian Komunikasi dan Informatika serta mencuri data registrasi kartu SIM yang dikelola oleh Kominfo. Data pribadi milik Bank Indonesia juga menjadi target Bjorka di awal Januari 2022 yang kemudian diperjualbelikan di forum gelap. Kasus ini menunjukkan sistem keamanan server Kominfo memiliki kelemahan yang sangat serius dan dapat dieksploitasi dengan mudah. Modus operandi Bjorka menggunakan teknik *social engineering* dan eksploitasi celah keamanan sistem yang tidak terdeteksi oleh administrator.[17] Pola kejahatan yang dilakukan Bjorka menunjukkan karakteristik *cybercrime* modern yang memanfaatkan kelemahan infrastruktur digital untuk

[17] Sitompul, F., Manik, A. P. P., Sinaga, C. D., Purba, A. T., & Satria, A. Op.cit., hlm. 224.

kepentingan ekonomi. Dampak psikologis dari aksi Bjorka menciptakan ketidakpercayaan publik terhadap kemampuan pemerintah dalam melindungi data pribadi warga negara.

Tokopedia mengalami kebocoran data pengguna pada tahun 2020 yang melibatkan lebih dari 60 juta akun pengguna aktif platform *e-commerce* tersebut. Data pribadi pengguna yang bocor kemudian diperjualbelikan di situs website gelap dengan harga yang cukup tinggi di pasar gelap.[4] Informasi yang bocor mencakup nama pengguna, alamat email, nomor telepon, dan data transaksi yang bersifat sensitif dan pribadi. Kejadian ini menimbulkan kekhawatiran massal masyarakat akan keamanan data yang tersimpan dalam platform digital komersial besar seperti Tokopedia. Platform *e-commerce* besar seharusnya memiliki sistem keamanan berlapis yang mampu mencegah akses tidak sah terhadap database pengguna. Pola kejahatan dalam kasus ini menunjukkan pelaku menargetkan platform dengan basis pengguna besar untuk memaksimalkan nilai jual data curian.

Kepolisian Republik Indonesia menjadi korban peretasan pada November 2021 yang mengakibatkan bocornya 28 ribu data detail login dan informasi pribadi. Seorang *hacker* dengan nama pengguna @son1x666 mengaku berhasil masuk ke dalam database Polri melalui akun Twitter pribadinya. Pelaku melampirkan sampel data yang dicurinya melalui *link* yang dapat diakses publik untuk membuktikan keberhasilan aksi peretasannya. Data yang bocor mencakup informasi nama, tempat lahir, NIK, alamat, golongan darah, satuan kerja, ras, email, hingga pangkat keanggotaan. Peretasan terhadap database Polri menunjukkan bahwa tidak ada institusi yang benar-benar aman dari ancaman *cybercrime* termasuk lembaga penegak hukum.[18] Pola kejahatan dalam kasus Polri menunjukkan pelaku memiliki kemampuan teknis tinggi dalam mengeksploitasi kelemahan sistem keamanan database pemerintah. Dampak dari kebocoran ini sangat serius karena data anggota Polri dapat disalahgunakan untuk kepentingan kriminal atau terorisme yang membahayakan.

Ribuan situs pemerintahan dengan ekstensi .go.id disisipi halaman promosi judi *online* sepanjang tahun 2023 yang sempat viral di media sosial. Peristiwa ini terungkap setelah seorang pengguna X mengunggah hasil pencarian terkait situs judi slot menggunakan *keyword* tertentu di Google. Penyebab peristiwa ini adalah lemahnya keamanan situs web pemerintahan yang memungkinkan *hacker* memanfaatkan celah keamanan untuk menyisipkan halaman judi ilegal. Fungsi halaman tersebut adalah sebagai *backlink* yang dapat meningkatkan peringkat situs judi *online* di mesin pencari dan menarik lebih banyak pengunjung. Bareskrim Polri menyatakan meski sudah memblokir hampir 850 ribu situs judi selama lima tahun terakhir, ada 3 juta halaman judi terposting di situs pemerintahan. Pola kejahatan dalam kasus ini menunjukkan pelaku memanfaatkan otoritas domain pemerintah untuk meningkatkan kredibilitas situs judi

[18] Pansariadi, R. S. B., & Soekorini, N. Op.cit., hlm. 292.

ilegal di mata mesin pencari.[19] Dampak dari kasus ini adalah menurunnya kepercayaan publik terhadap integritas dan profesionalisme pengelolaan infrastruktur digital pemerintahan Indonesia.

Pengaturan Pertanggungjawaban Pidana Pelaku Cybercrime dalam Sistem Hukum Indonesia

Pertanggungjawaban pidana pelaku *cybercrime* dalam sistem hukum Indonesia diatur secara khusus melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Regulasi ini menjadi landasan hukum utama untuk menindak pelaku kejahatan siber di Indonesia dengan sanksi pidana yang tegas dan proporsional. UU ITE kemudian mengalami perubahan melalui UU Nomor 19 Tahun 2016 untuk menyempurnakan ketentuan yang dianggap multitafsir dan memberikan kepastian hukum lebih baik. Perubahan kedua dilakukan melalui UU Nomor 1 Tahun 2024 yang semakin memperkuat landasan yuridis penanganan kejahatan siber dengan mengakomodasi perkembangan teknologi terkini. Pengaturan pertanggungjawaban pidana dalam UU ITE didasarkan pada prinsip-prinsip hukum pidana umum yang terdapat dalam KUHP dengan adaptasi khusus karakteristik kejahatan digital. Sanksi pidana yang diatur dalam UU ITE bervariasi tergantung pada jenis kejahatan siber yang dilakukan dan tingkat kerugian yang ditimbulkan.

Anatomi kejahatan siber berdasarkan UU ITE dapat dibagi menjadi dua kelompok besar yaitu kejahatan yang menargetkan sistem elektronik dan kejahatan konten ilegal. Kelompok pertama mencakup tujuh jenis kejahatan yang dianggap sebagai kejahatan kontemporer yang menghasilkan bentuk kejahatan baru dalam dunia digital. Kejahatan yang menargetkan internet, komputer, dan teknologi terkait termasuk *illegal access, illegal interception, data interference,* dan *system interference* yang diatur dalam Pasal 30-35 UU ITE. Kelompok kedua adalah kejahatan konten ilegal yang menggunakan internet sebagai media untuk melakukan kejahatan yang sebenarnya sudah ada sebelumnya seperti pornografi dan pencemaran nama baik. Publikasi dan distribusi konten ilegal diatur dalam Pasal 27-29 UU ITE dengan sanksi pidana yang bervariasi sesuai dengan tingkat bahaya dan dampak sosialnya. Pembagian kategori kejahatan ini memudahkan aparat penegak hukum dalam mengidentifikasi jenis tindak pidana dan menerapkan pasal yang tepat dalam proses penuntutan.

Pasal 27 UU ITE mengatur tentang distribusi dan transmisi informasi elektronik dengan muatan yang melanggar hukum seperti pornografi, perjudian, dan pencemaran nama baik. Setiap orang yang dengan sengaja dan tanpa hak mendistribusikan informasi elektronik yang memiliki muatan melanggar kesusilaan dapat dipidana penjara maksimal 6 tahun. Ketentuan ini bertujuan melindungi moralitas publik dari penyebaran konten pornografi yang semakin masif di era digital melalui berbagai platform media sosial. Pasal 27 ayat 3 mengatur tentang

[19] Handoyo, B., Husamuddin, M. Z., & Rahma, I. Op.cit., hlm. 41.

pencemaran nama baik di ruang siber yang menyamakan penghinaan online dengan penghinaan konvensional yang diatur KUHP. Sanksi pidana untuk pencemaran nama baik dapat mencapai penjara maksimal 4 tahun dan denda maksimal Rp 750 juta yang cukup memberatkan pelaku. Pasal 27 ayat 2 juga mengatur tentang perjudian online yang semakin marak dengan modus yang semakin canggih dan sulit dilacak oleh aparat. Penerapan Pasal 27 dalam praktik seringkali menimbulkan kontroversi karena dianggap dapat menjerat kebebasan berekspresi di ruang digital yang dijamin konstitusi.

Pasal 30 UU ITE mengatur tentang akses ilegal terhadap komputer dan sistem elektronik dengan cara melanggar, menerobos, atau menjebol sistem pengamanan yang ada. Setiap orang yang dengan sengaja dan tanpa hak mengakses komputer dengan melanggar sistem pengamanan dapat dipidana penjara maksimal 8 tahun. Pasal ini menargetkan aktivitas *hacking* dan *cracking* yang menjadi ancaman serius bagi keamanan data pribadi maupun data institusi pemerintah dan swasta. Ketentuan dalam Pasal 30 ayat 3 memberikan sanksi lebih berat karena unsur pelanggaran sistem pengamanan menunjukkan niat jahat yang jelas dari pelaku. Ancaman pidana denda dalam pasal ini mencapai Rp 800 juta yang dimaksudkan untuk memberikan efek jera kepada pelaku peretasan sistem elektronik. Penerapan Pasal 30 memerlukan pembuktian yang kuat tentang adanya akses tanpa hak dan pelanggaran sistem pengamanan yang dilakukan secara sengaja.

Pasal 33 UU ITE mengatur tentang tindakan yang berakibat terganggunya sistem elektronik atau menyebabkan sistem tidak bekerja sebagaimana mestinya seperti serangan DDoS. Setiap orang yang dengan sengaja melakukan tindakan yang mengakibatkan gangguan sistem elektronik dapat dipidana dengan sanksi yang cukup berat untuk memberikan efek jera. Pasal ini relevan dengan kasus serangan terhadap website DPR RI dan berbagai situs pemerintahan yang mengalami down akibat serangan siber terkoordinasi. Gangguan terhadap sistem elektronik dapat menimbulkan kerugian yang sangat besar terutama jika menyasar infrastruktur kritis yang menunjang pelayanan publik seperti kasus PDN. Pasal 33 juga mengakomodasi berbagai bentuk serangan seperti malware, virus, dan ransomware yang dapat melumpuhkan sistem elektronik secara masif. Penerapan pasal ini harus mempertimbangkan tingkat dampak gangguan yang ditimbulkan terhadap kepentingan publik dan keamanan nasional secara proporsional.

Pasal 35 UU ITE mengatur tentang manipulasi, penciptaan, perubahan, atau penghilangan informasi elektronik dengan tujuan seolah-olah data tersebut asli dan sah. Tindak pidana pemalsuan data elektronik ini dapat dipidana dengan sanksi penjara dan denda yang cukup tinggi untuk memberikan *deterrence effect*. Pemalsuan data elektronik semakin canggih dengan memanfaatkan teknologi *deepfake* dan *artificial intelligence* yang sulit dibedakan dari data asli oleh korban. Ketentuan Pasal 35 bertujuan melindungi integritas data dan informasi elektronik yang menjadi dasar kepercayaan dalam transaksi digital dan pelayanan publik. Pembuktian

pemalsuan data elektronik memerlukan keahlian khusus dalam *digital forensics* untuk mendeteksi manipulasi yang telah dilakukan oleh pelaku.

Prosedur penuntutan pidana terhadap pelaku *cybercrime* diatur dalam Pasal 42 dan 43 UU ITE yang mengatur tentang penyidikan oleh Polri dan PPNS. Korban yang merasa haknya dilanggar dapat datang langsung membuat laporan kepada penyidik Polri pada unit *Cybercrime* atau PPNS pada Sub Direktorat Penyidikan Kementerian Kominfo. Penyidik akan melakukan penyelidikan yang dapat dilanjutkan dengan proses penyidikan sesuai Hukum Acara Pidana dan ketentuan khusus dalam UU ITE yang mengatur pemeriksaan elektronik. Setelah proses penyidikan selesai, berkas perkara akan dilimpahkan kepada penuntut umum untuk dilakukan penuntutan di muka pengadilan sesuai dengan ketentuan KUHAP. Ketentuan penyidikan dalam UU ITE berlaku pula terhadap penyidikan tindak pidana siber dalam arti luas termasuk tindak pidana konvensional dengan unsur elektronik. Penyidik harus memperhatikan kelancaran layanan publik sebelum melakukan penggeledahan atau penyitaan terhadap server yang menyimpan data penting untuk pelayanan masyarakat. Apabila tindakan penyitaan server akan mengganggu pelayanan publik, tindakan tersebut tidak boleh dilakukan dan harus dicari alternatif lain yang lebih proporsional.

Implementasi Penegakan Hukum Tindak Pidana Cybercrime di Indonesia

Penegakan hukum tindak pidana *cybercrime* di Indonesia dilaksanakan melalui mekanisme sistem peradilan pidana yang melibatkan berbagai institusi. Kepolisian Republik Indonesia membentuk unit khusus Direktorat Tindak Pidana Siber Bareskrim untuk menangani kejahatan berbasis teknologi informasi. Unit ini menerapkan pendekatan proaktif dengan melakukan patroli siber guna mendeteksi aktivitas mencurigakan di ruang digital. Implementasi UU ITE dalam praktik penyidikan menunjukkan kompleksitas tersendiri terutama dalam pengumpulan barang bukti elektronik yang sah. Penyidik harus memahami prosedur digital forensik untuk menjaga integritas bukti agar tidak terkontaminasi selama proses investigasi.[20] Penerapan *chain of custody* menjadi prinsip dasar dalam penanganan bukti digital untuk memastikan validitasnya di pengadilan.

Jaksa penuntut umum berperan melakukan penuntutan berdasarkan hasil penyidikan yang telah dinyatakan lengkap oleh pihak kepolisian. Kejaksaan menghadapi tantangan dalam membuktikan unsur-unsur tindak pidana *cybercrime* yang seringkali bersifat abstrak dan teknis di persidangan. Kemampuan jaksa dalam merumuskan dakwaan yang tepat sangat bergantung pada pemahaman teknologi yang digunakan dalam modus kejahatan.[21] Teori sistem peradilan pidana Mardjono Reksodiputro menekankan pentingnya sinkronisasi kerja antar subsistem kepolisian, kejaksaan, dan pengadilan. Kesenjangan kompetensi teknis antara jaksa dan penyidik dapat menyebabkan kelemahan konstruksi dakwaan yang berujung pada putusan

[20] Maskun, S. H. Op.cit., hlm. 156.
[21] Handoyo, B., Husamuddin, M. Z., & Rahma, I. Op.cit., hlm. 45.

bebas. Peningkatan kapasitas melalui pelatihan berkala tentang perkembangan teknologi menjadi kebutuhan mendesak bagi para jaksa.

Mekanisme *take down* atau pemblokiran konten negatif menjadi instrumen preventif yang diterapkan oleh Kementerian Komunikasi dan Informatika. Kewenangan pemblokiran konten tanpa perintah pengadilan menuai kritik dari kalangan pemerhati kebebasan berekspresi dan hak asasi manusia. Transparansi dalam proses pengambilan keputusan pemblokiran menjadi tuntutan untuk menjaga akuntabilitas pemerintah terhadap masyarakat luas.[22] Keseimbangan antara perlindungan kepentingan umum dengan hak individu menjadi dilema dalam implementasi kewenangan ini secara proporsional. *Judicial review* terhadap keputusan pemblokiran seharusnya dapat diakses oleh pihak yang merasa hak konstitusionalnya dilanggar. Pendekatan preventif melalui edukasi literasi digital kepada masyarakat perlu diperkuat untuk mengurangi ketergantungan pada tindakan represif.

Kerjasama internasional dalam penegakan hukum *cybercrime* menjadi keniscayaan mengingat karakteristik kejahatan yang melampaui batas teritorial negara. Indonesia telah menjalin *mutual legal assistance* dengan berbagai negara untuk memfasilitasi pertukaran informasi dan bantuan hukum timbal balik. Perbedaan sistem hukum antar negara menjadi hambatan dalam proses ekstradisi pelaku yang melarikan diri ke luar yurisdiksi. Harmonisasi regulasi *cybercrime* dengan standar internasional seperti Budapest Convention diperlukan untuk memperkuat basis kerjasama antarnegara yang efektif.[23] Diplomasi digital menjadi dimensi baru dalam hubungan internasional yang harus dikembangkan secara serius oleh pemerintah Indonesia. Keterbatasan infrastruktur teknologi informasi di Indonesia menyulitkan pelacakan jejak digital pelaku yang menggunakan server di negara lain.

Hambatan dan Tantangan Penegakan Hukum Tindak Pidana Cybercrime di Indonesia

Penegakan hukum terhadap tindak pidana *cybercrime* menghadapi berbagai hambatan struktural yang menghambat efektivitas penanganan kasus secara menyeluruh. Kompleksitas permasalahan tidak hanya terletak pada aspek yuridis namun juga dimensi teknis operasional yang memerlukan pendekatan multidisipliner. Teori penegakan hukum Soerjono Soekanto mengidentifikasi lima faktor yang mempengaruhi efektivitas hukum yaitu substansi, struktur, budaya, sarana, dan masyarakat.[^6] Keterbatasan sumber daya manusia yang kompeten menjadi kendala mendasar dalam proses penyidikan hingga tahap penuntutan dan persidangan. Kurangnya infrastruktur teknologi forensik digital di berbagai daerah memperparah kesenjangan kapasitas antara pusat dan wilayah terpencil. Karakteristik cybercrime yang dinamis menuntut adaptasi berkelanjutan dari aparat penegak hukum terhadap perkembangan teknologi yang sangat cepat. Hambatan-hambatan ini mencerminkan ketidaksesuaian antara tuntutan penegakan hukum dengan realitas kapasitas yang tersedia dalam sistem peradilan pidana.

[22] Djarawula, M., Alfiani, N., & Mayasari, H. Op.cit., hlm. 3802.
[23] Sitompul, F., Manik, A. P. P., Sinaga, C. D., Purba, A. T., & Satria, A. Op.cit., hlm. 225.

1. Keterbatasan Kompetensi Sumber Daya Manusia

Kualitas sumber daya manusia aparat penegak hukum menjadi faktor krusial yang menentukan keberhasilan penanganan kasus *cybercrime* di lapangan. Mayoritas penyidik kepolisian tidak memiliki latar belakang pendidikan teknologi informasi yang memadai untuk memahami modus operandi kejahatan siber. Pelatihan yang diberikan seringkali bersifat umum dan tidak mencakup teknik investigasi digital yang spesifik serta mendalam.[24] Disparitas kompetensi antara penyidik di kota besar dengan daerah terpencil semakin memperburuk kesenjangan dalam kapasitas penanganan.

Jaksa penuntut umum menghadapi kendala serupa dalam memahami aspek teknis yang menjadi dasar pembuktian tindak pidana di persidangan. Kesulitan dalam mengkonstruksi hubungan kausalitas antara perbuatan pelaku dengan dampak yang ditimbulkan seringkali menjadi kelemahan fatal dalam penuntutan. Keterbatasan akses terhadap ahli teknologi informasi yang dapat memberikan keterangan di persidangan mempersulit proses pembuktian secara komprehensif.[25] Hakim sebagai pihak yang memutus perkara juga memerlukan pemahaman teknologi untuk dapat menilai keterangan saksi ahli secara kritis. Peningkatan kapasitas melalui pendidikan dan pelatihan berkelanjutan menjadi kebutuhan yang harus diprioritaskan oleh lembaga penegak hukum.

2. Kompleksitas Teknis Pembuktian dan Forensik Digital

Pembuktian dalam kasus *cybercrime* memiliki karakteristik unik yang berbeda signifikan dengan kejahatan konvensional dalam sistem peradilan pidana. Barang bukti elektronik bersifat *volatile* dan mudah rusak atau hilang jika tidak ditangani dengan prosedur yang tepat. Proses pengamanan bukti digital memerlukan peralatan khusus seperti *write blocker* untuk mencegah perubahan data selama penyitaan dilakukan.[26] Keterbatasan laboratorium forensik digital yang tersebar di Indonesia menyebabkan penumpukan kasus di beberapa lokasi tertentu yang memiliki fasilitas. Waktu yang diperlukan untuk analisis forensik digital seringkali sangat panjang sehingga menghambat proses penyelesaian perkara secara cepat.

Rantai penyimpanan atau *chain of custody* bukti digital harus dijaga dengan ketat untuk memastikan integritas dan autentisitas bukti. Standar operasional prosedur forensik digital belum sepenuhnya dipahami dan diterapkan secara konsisten oleh seluruh penyidik di lapangan.[27] Perbedaan interpretasi terhadap hasil analisis forensik antara penyidik dan ahli dapat menimbulkan kebingungan dalam proses persidangan. Ketiadaan sertifikasi forensik digital yang diakui secara nasional menyebabkan variasi kualitas laporan forensik dari

[24] Agung, A., Hafrida, H., & Erwin, E. (2022). Pencegahan Kejahatan Terhadap Cybercrime. PAMPAS: Journal of Criminal Law, 3(2), hlm. 217.

[25] Bego, K. C., Aziz, F. R., Rahmad, R. A., & Budianto, H. Op.cit., hlm. 508.

[26] [^9]: Febriansyah, F. I. Op.cit., hlm. 78.

[27] Fairuzzen, M. R., Putra, A. A., Reihan, A., & SH, L. P. Op.cit., hlm. 146.

berbagai institusi. Validitas bukti digital di pengadilan masih menjadi perdebatan terutama terkait *admissibility* dan *reliability* dari bukti tersebut. Pengembangan standar nasional forensik digital dan akreditasi laboratorium menjadi langkah penting untuk meningkatkan kualitas pembuktian kasus *cybercrime*.

3. Permasalahan Yurisdiksi dan Sifat Lintas Batas

Kejahatan siber memiliki karakteristik transnasional yang melampaui batas teritorial negara sehingga menimbulkan persoalan yurisdiksi yang sangat kompleks. Penetapan tempus dan *locus delicti* dalam *cybercrime* menjadi perdebatan karena pelaku dapat berada di negara berbeda dengan korban.[28] UU ITE telah mengatur prinsip yurisdiksi ekstrateritorial namun implementasinya menghadapi kendala teknis dan politis dalam praktik penegakan hukum. Pelaku yang berada di luar negeri seringkali tidak dapat dijangkau oleh proses hukum Indonesia karena keterbatasan kewenangan teritorial. Proses ekstradisi memerlukan waktu sangat panjang dan bergantung pada kesediaan negara tempat pelaku berada untuk memberikan kerjasama.

Penggunaan *virtual private network* dan *proxy server* memungkinkan pelaku menyamarkan lokasi geografis sehingga menyulitkan pelacakan identitas asli mereka. Server yang digunakan untuk melakukan kejahatan seringkali berada di negara dengan regulasi privasi sangat ketat atau tidak kooperatif. Ketergantungan pada kerjasama penyedia layanan internet asing menjadi kendala ketika perusahaan tersebut tidak tunduk pada hukum Indonesia.[29] Ketiadaan perjanjian bilateral atau multilateral dengan beberapa negara mempersulit upaya penanganan kasus yang melibatkan yurisdiksi ganda atau majemuk.

4. Keterbatasan Infrastruktur dan Anggaran

Penegakan hukum *cybercrime* memerlukan investasi infrastruktur teknologi dan pengembangan sistem informasi yang canggih serta mutakhir. Peralatan forensik digital seperti *hardware write blocker, software analisis,* dan *storage* forensik memiliki harga yang sangat mahal. Keterbatasan anggaran yang dialokasikan untuk unit *cybercrime* menyebabkan banyak instansi tidak mampu memperbarui peralatan secara berkala.[30] Perkembangan teknologi yang sangat cepat membuat peralatan forensik menjadi usang dalam waktu relatif singkat sehingga memerlukan investasi berkelanjutan. Sistem informasi manajemen perkara yang terintegrasi antar lembaga penegak hukum belum sepenuhnya berfungsi dengan baik dan efisien.

Minimnya alokasi anggaran untuk pelatihan dan pengembangan kapasitas sumber daya manusia berdampak pada rendahnya kompetensi aparat penegak hukum. Institusi penegak hukum seringkali mengandalkan bantuan dari pihak swasta atau komunitas untuk

[28] Purwaningsih, R., & Putranto, R. D. Op.cit., hlm. 134.
[29] Hapsari, R. D., & Pambayun, K. G. Op.cit., hlm. 12.
[30] Gunawan, F., Fadhilah, A., & Sakti, E. M. S. Op.cit., hlm. 160.

mendapatkan pelatihan dan asistensi teknis.[31] Ketergantungan pada pihak eksternal ini menimbulkan risiko konflik kepentingan dan ketidakmandirian dalam penanganan kasus tertentu yang sensitif. Pembangunan laboratorium forensik digital regional memerlukan komitmen anggaran jangka panjang yang belum menjadi prioritas dalam perencanaan pembangunan nasional. Pengadaan lisensi *software* forensik legal yang mahal seringkali menjadi kendala sehingga beberapa unit menggunakan *tools* ilegal.

PENUTUPAN

Penegakan hukum tindak pidana *cybercrime* di Indonesia memiliki landasan yuridis yang cukup komprehensif melalui UU ITE dan peraturan terkait lainnya. Implementasi penegakan hukum melibatkan koordinasi antara kepolisian, kejaksaan, dan pengadilan dalam sistem peradilan pidana yang terintegrasi. Namun efektivitas penegakan hukum masih terhambat oleh berbagai kendala struktural yang bersifat multidimensional dan kompleks. Keterbatasan kompetensi sumber daya manusia aparat penegak hukum dalam memahami aspek teknis teknologi informasi menjadi hambatan utama. Kompleksitas pembuktian forensik digital, permasalahan yurisdiksi lintas negara, serta minimnya infrastruktur dan anggaran memperburuk situasi penanganan kasus. Karakteristik *cybercrime* yang terus berkembang mengikuti perkembangan teknologi menuntut adaptasi berkelanjutan dari sistem hukum dan aparatnya. Diperlukan pendekatan holistik melalui peningkatan kapasitas sumber daya manusia, investasi infrastruktur teknologi, penguatan kerjasama internasional, dan sinergi seluruh pemangku kepentingan.

DAFTAR PUSTAKA

Agung, A., Hafrida, H., & Erwin, E. (2022). Pencegahan Kejahatan Terhadap Cybercrime. *PAMPAS: Journal of Criminal Law*, 3(2), 212-222.

Agustin, N. A., & Firdos, R. M. (2024). Studi literatur: Ancaman cybercrime di Indonesia dan pentingnya pemahaman akan fenomena kejahatan digital. *Jurnal Mahasiswa Teknik Informatika*, 3(1), 126-131.

Alamsyah, A., Santoso, E., & Pranadita, N. (2025). Kajian Terhadap Kejahatan Carding Sebagai Bentuk Cybercrime Di Indonesia. *Iustitia Omnibus: Jurnal Ilmu Hukum*, 6(2), 60-68.

Aldriano, M. A., & Priyambodo, M. A. (2022). Cyber crime dalam sudut pandang hukum pidana. *Jurnal Kewarganegaraan*, 6(1), 2169-2175.

Bahri, I. S. (2023). *Cyber Crime dalam Sorotan Hukum Pidana (Edisi 2023)*. Bahasa Rakyat.

Bego, K. C., Aziz, F. R., Rahmad, R. A., & Budianto, H. (2025). Tindak Pidana Cybercrime: Tantangan Hukum Pidana Dalam Menanggulangi Kejahatan di Dunia Maya (Desember 2024). *Jurnal Kolaboratif Sains*, 8(1), 506-511.

Djarawula, M., Alfiani, N., & Mayasari, H. (2023). Tinjauan Yuridis Tindak Pidana Kejahatan

[31] Agustin, N. A., & Firdos, R. M. Op.cit., hlm. 129.

Teknologi Informasi (Cybercrime) Di Indonesia Ditinjau Dari Perspektif Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *Jurnal Cakrawala Ilmiah*, 2(10), 3799-3806.

Fairuzzen, M. R., Putra, A. A., Reihan, A., & SH, L. P. (2024). Perkembangan Hukum dan Kejahatan Siber "Cybercrime" di Indonesia. *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory*, 2(1), 139-153.

Febriansyah, F. I. (2025). *Cybercrime: Kejahatan di Balik Layar Digital*. Najaha.

Febriansyah, F. I., Indiantoro, A., & Ikhwan, A. (2023). Model Kejahatan Dunia Maya (Cybercrime) Sebagai Upaya Pembentukan Hukum Nasional. *Legal Standing: Jurnal Ilmu Hukum*, 7(2), 242-255.

Gunawan, F., Fadhilah, A., & Sakti, E. M. S. (2024). Membangun benteng digital untuk memperkuat etika cyber security melawan ancaman cyber crime. *Jurnal Ilmiah Teknik Informatika (TEKINFO)*, 25(1), 154-167.

Handoyo, B., Husamuddin, M. Z., & Rahma, I. (2024). Tinjaun Yuridis Penegakkan Hukum Kejahatan Cyber Crime Studi Implementasi Undang-Undang Nomor 11 Tahun 2008. *MAQASIDI: Jurnal Syariah Dan Hukum*, 40-55.

Hapsari, R. D., & Pambayun, K. G. (2023). Ancaman cybercrime di indonesia: Sebuah tinjauan pustaka sistematis. *Jurnal Konstituen*, 5(1), 1-17.

Maskun, S. H. (2022). *Kejahatan Siber (Cyber Crime): Suatu Pengantar*. Prenada Media.

Pansariadi, R. S. B., & Soekorini, N. (2023). Tindak Pidana Cyber Crime dan Penegakan Hukumnya. *Binamulia Hukum*, 12(2), 287-298.

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing cybercrime: Definitions, typologies and taxonomies. *Forensic Sciences*, 2(2), 379-398.

Purwaningsih, R., & Putranto, R. D. (2023). Tinjauan yuridis terhadap penetapan locus delicti dalam kejahatan dunia maya (cyber crime) berkaitan dengan upaya pembaharuan hukum pidana di Indonesia. *Mimbar Keadilan*, 16(1), 130-138.

Sitompul, F., Manik, A. P. P., Sinaga, C. D., Purba, A. T., & Satria, A. (2024). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Hukum Indonesia. *Jaksa: Jurnal Kajian Ilmu Hukum Dan Politik*, 2(2), 222-228.

Widianingrum, A. R. (2024). Analisis Implementasi Kebijakan Hukum Terhadap Penanganan Kejahatan Siber Di Era Digital. *Journal Iuris Scientia*, 2(2), 90-102.

Wijaya, T. H. D. (2022). Penerapan sanksi sosial sebagai alternatif pemidanaan terhadap pelaku tindak pidana kejahatan siber (cyber crime). *Al-Qisth Law Review*, 5(2), 371-404.