REKONSTRUKSI HUKUM PIDANA TERHADAP KEJAHATAN SIBER *(CYBER CRIME)* DALAM SISTEM PERADILAN PIDANA INDONESIA

RECONSTRUCTION OF CRIMINAL LAW AGAINST CYBERCRIME IN THE INDONESIAN CRIMINAL JUSTICE SYSTEM

Soetardi Tri Cahyono [*(a,1)], Wina Erni [(b,2)], Taufik Hidayat [(c,3)].
[a] Universitas Al Azhar Indonesia, Jakarta, Indonesia
[b]Universitas Trisakti, Jakarta, Indonesia
[b]Sekolah Tinggi Agama Islam Nurul Iman, Parung, Bogor, Indonesia

1 Suetarditricagyono23@gmail.com*
[*]Penulis Penanggung Jawab (Suetarditricagyono23@gmail.com)

Abstrak

Upaya rekonstruksi hukum pidana dalam merespons dinamika dan kompleksitas kejahatan siber di era digital. Kejahatan siber yang semakin masif menimbulkan tantangan serius terhadap sistem hukum nasional, terutama dalam aspek substansi hukum, mekanisme penegakan hukum, dan perlindungan hak asasi manusia di ruang digital. Pendekatan normatif-teoretis digunakan untuk menganalisis kelemahan struktur hukum pidana saat ini, termasuk ketertinggalan regulasi, disharmoni antarperaturan, dan lemahnya integrasi teknologi dalam proses penegakan hukum. Kajian ini juga menekankan pentingnya pembaruan paradigma hukum yang tidak hanya represif, tetapi juga preventif dan restoratif, guna menjawab tantangan keadilan digital secara menyeluruh. Penelitian ini merekomendasikan strategi rekonstruksi melalui pembaruan legislasi, peningkatan kapasitas aparat penegak hukum, serta integrasi prinsip-prinsip hak asasi manusia dalam tata kelola keamanan siber nasional. Dengan demikian, sistem hukum pidana Indonesia dapat menjadi lebih adaptif dan responsif dalam menghadapi era digital yang terus berkembang.

Kata Kunci: *Rekonstruksi Hukum, Kejahatan Siber, Keadilan Digital, Penegakan Hukum, Hak Asasi Manusia, Legislasi, Reformasi Hukum Pidana.*

Abstract

Efforts to reconstruct criminal law in response to the dynamics and complexity of cybercrime in the digital era. Cybercrime, which is increasingly massive, poses serious challenges to the national legal system, especially in terms of legal substance, law enforcement mechanisms, and human rights protection in the digital space. A normative-theoretical approach is used to analyze the weaknesses of the current criminal law structure, including regulatory lag, disharmony between regulations, and weak integration of technology in the law enforcement process. This study also emphasizes the importance of reforming the legal paradigm that is not only repressive, but also preventive and restorative, in order to answer the challenges of digital justice as a whole. This study recommends reconstruction strategies through legislative reform, capacity building of law enforcement officials, and integration of human rights principles in national cybersecurity governance. Thus, Indonesia's criminal law system can become more adaptive and responsive in facing the ever-evolving digital era.

Keywords: *Legal Reconstruction, Cybercrime, Digital Justice, Law Enforcement, Human Rights, Legislation, Criminal Law Reform.*

Pendahuluan

Transformasi digital yang terjadi secara masif dalam dua dekade terakhir telah menimbulkan perubahan struktural pada hampir seluruh aspek kehidupan masyarakat. Proses digitalisasi yang merambah sektor pemerintahan, perdagangan, pendidikan, hingga komunikasi sosial tidak hanya membawa efisiensi, tetapi juga menciptakan ruang baru yang rentan terhadap berbagai bentuk pelanggaran hukum. Di Indonesia, percepatan pemanfaatan teknologi informasi telah didorong melalui kebijakan nasional seperti *Roadmap Indonesia Digital 2021–2024* dan *Rencana Induk Transformasi Digital Nasional*. Namun, perlu diakui bahwa pesatnya perkembangan teknologi ini tidak diimbangi dengan kesiapan regulatif yang memadai, terutama dalam ranah hukum pidana.[1] Ruang digital telah menjadi arena baru bagi munculnya kejahatan non-konvensional yang bersifat transnasional, seperti penyusupan sistem elektronik, manipulasi data, penipuan daring, serta eksploitasi anak melalui internet. Karakteristik kejahatan semacam ini memperlihatkan ketimpangan antara realitas kriminalitas digital dengan perangkat hukum yang masih berakar pada paradigma analog. Oleh karena itu, muncul kebutuhan mendesak untuk merefleksikan ulang sejauh mana sistem hukum pidana Indonesia mampu menjawab kompleksitas tantangan di era digital.

Kejahatan siber (cyber crime) sebagai kategori tindak pidana modern memiliki karakteristik unik yang membedakannya dari kejahatan konvensional. Aspek seperti anonimitas pelaku, kemudahan distribusi kejahatan secara massal, serta kemampuan melewati batas-batas yurisdiksi nasional menjadikan kejahatan ini sulit dijangkau dengan pendekatan hukum pidana tradisional.[2] Indonesia telah memiliki beberapa perangkat hukum yang mengatur tentang ruang siber, di antaranya adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, serta didukung oleh instrumen lain seperti Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Meskipun regulasi tersebut bertujuan untuk memberikan dasar hukum terhadap aktivitas elektronik dan menanggulangi kejahatan digital, praktik implementasinya tidak jarang menimbulkan kontroversi. Beberapa pasal dalam UU ITE, seperti Pasal 27 ayat (3) dan Pasal 28 ayat (2), seringkali dipandang mengandung ambiguitas normatif serta digunakan secara eksesif untuk membungkam ekspresi warga negara. Hal ini menunjukkan bahwa selain adanya kekosongan hukum pada jenis-jenis cyber crime tertentu, juga terdapat persoalan dalam aspek perlindungan hak konstitusional yang semestinya dijamin oleh UUD 1945. Situasi ini menunjukkan bahwa perangkat hukum yang ada belum sepenuhnya mampu mengimbangi kompleksitas kejahatan siber yang terus berkembang, baik secara teknis, yuridis, maupun filosofis.[3]

Dari sudut pandang sistem peradilan pidana, tantangan dalam penanganan kejahatan siber tidak hanya bersumber dari ketidakjelasan norma, tetapi juga dari rendahnya kapasitas kelembagaan dalam menjawab dinamika kejahatan digital. Proses penyelidikan dan pembuktian dalam kasus cyber crime memerlukan keahlian forensik digital, infrastruktur teknologi mutakhir, serta kemampuan analisis data elektronik yang belum dimiliki secara merata oleh aparat penegak hukum. Hal ini menjadi hambatan serius dalam upaya penegakan hukum yang efektif dan akuntabel. Sebagai contoh, proses pelacakan pelaku kejahatan siber kerap terhambat oleh keterbatasan kerja sama internasional serta kurangnya mekanisme *mutual legal assistance* yang responsif dan cepat.[4] Selain itu, pendekatan penegakan hukum yang masih bersifat fragmentaris dan sektoral memperlemah koordinasi antara instansi

[1] Nihitha Sallapalli, "Digital Transformation : Reshaping Industries Through Technology" 6, no. 6 (n.d.): 1–9.

[2] Vannya Anastasya et al., "Efektivitas Hukum Dan Kebijakan Publik Dalam Menghadapi Ancaman Siber Terhadap Keamanan Negara" 3, no. 2 (2024): 1710–16.

[3] Abdan Sifa, "Transformasi Digital E-Commerce Dalam Menguasai Kosentrasi Pasar Di Indonesia" 2, no. 12 (2024): 405–13.

[4] Adhitya Chandra Setyawan, "Enhancing Public Service Delivery through Digital Transformation : A Study on the Role of E-Government in Modern Public Administration Open Access," 2024.

terkait, seperti Kepolisian, Kejaksaan, Kementerian Komunikasi dan Informatika, serta Badan Siber dan Sandi Negara. Dalam kondisi seperti ini, hukum pidana tidak hanya mengalami stagnasi dalam hal substansi, tetapi juga menghadapi tantangan kelembagaan dan prosedural. Padahal, Pasal 28G ayat (1) UUD 1945 menjamin perlindungan terhadap rasa aman dan kebebasan dari ancaman. Oleh karena itu, ketidakmampuan negara dalam menghadirkan sistem hukum yang andal dalam menangani kejahatan siber berpotensi melemahkan kepercayaan publik terhadap supremasi hukum dan keadilan.[5]

Artikel ini disusun dengan tujuan untuk memberikan analisis konseptual dan yuridis terhadap kebutuhan rekonstruksi hukum pidana dalam menghadapi tantangan kejahatan siber di Indonesia. Penelitian ini berpijak pada paradigma hukum progresif dan berupaya mengidentifikasi ketimpangan antara realitas kriminalitas digital dengan kesiapan sistem peradilan pidana yang ada. Di samping itu, tulisan ini juga bertujuan untuk menawarkan pendekatan alternatif dalam perumusan kebijakan hukum pidana, yang tidak hanya menekankan pada aspek penindakan, tetapi juga pada aspek pencegahan dan perlindungan hak asasi manusia. Urgensi dari penelitian ini terletak pada semakin meningkatnya eskalasi cyber crime yang mengancam keamanan nasional dan mengganggu ketertiban umum. Apabila tidak segera ditanggulangi dengan pendekatan hukum yang tepat, maka sistem hukum pidana Indonesia akan terus tertinggal dalam merespons dinamika kejahatan digital global. Harapannya, melalui kajian ini, akan terbentuk landasan pemikiran yang kuat bagi proses pembaruan hukum pidana nasional yang lebih responsif, adil, dan berpihak pada kepentingan publik di era transformasi digital.

Pembahasan

A. Karakteristik Kejahatan Siber dan Implikasinya terhadap Pendekatan Hukum Pidana

1. Evolusi Kejahatan Siber Dari Kejahatan Tradisional ke Digital

Transformasi teknologi informasi dan komunikasi telah memicu pergeseran signifikan dalam modus operandi pelaku kejahatan. Aktivitas kriminal yang sebelumnya bersifat fisik, seperti perampokan dan penipuan konvensional, kini telah beralih ke bentuk virtual melalui perangkat digital. Fenomena ini memperlihatkan bahwa ruang siber telah menjadi ladang baru bagi pelaku kejahatan dengan risiko yang lebih rendah namun dampak yang lebih luas. Di Indonesia, lonjakan aktivitas digital sejak satu dekade terakhir menyebabkan meningkatnya intensitas tindak pidana yang dilakukan melalui internet.[6] Bentuk kejahatan seperti pencurian data pribadi, penyebaran konten ilegal, manipulasi transaksi keuangan, hingga penyusupan ke dalam sistem elektronik menunjukkan pergeseran kriminalitas dari yang bersifat konvensional menuju domain digital. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana telah diubah dengan UU Nomor 19 Tahun 2016 (UU ITE), menjadi rujukan normatif utama dalam merespons fenomena ini. Pasal 30 UU ITE, misalnya, mengatur larangan akses tanpa hak terhadap sistem elektronik. Akan tetapi, dalam praktiknya, norma ini belum mampu sepenuhnya mengakomodasi kompleksitas dinamika kejahatan siber yang terus berkembang. Oleh karena itu, transisi ke arah kejahatan digital menuntut pula transformasi dalam aspek substansi, struktur, dan budaya hukum pidana nasional.[7]

Evolusi kriminalitas digital tidak hanya tercermin dari perpindahan medium kejahatan, melainkan juga pada perubahan taktik dan strategi pelaku dalam menghindari deteksi dan hukum. Salah satu bentuk yang paling menonjol adalah serangan siber seperti

[5] Putri Diyah et al., "Electronic Certificates in Indonesia : Enhancing Legal Certainty or Introducing New," 2021, 686–98.

[6] Virginia Valentine, Clara Sinta Septiani, and Jadiaman Parshusip, "Menghadapi Tantangan Dan Solusi Cybercrime Di Era Digital Facing Cybercrime Challenges And Solutions In The Digital Era" 1 (2024): 2–6.

[7] Jiabao Li, "Multi-Governance Model of New Cybercrime under the Risk of New Technologies Risks and Responses" 0, no. August (2024): 22–29, https://doi.org/10.54254/2753-7048/73/2024.BO17965.

ransomware, *phishing*, dan *hacking*, di mana pelaku mengeksploitasi celah sistem informasi untuk mendapatkan keuntungan atau mengacaukan fungsi layanan publik dan swasta. Fenomena ini tidak lagi melibatkan pertemuan langsung antara pelaku dan korban, melainkan bergantung pada rekayasa sosial (social engineering) dan celah teknis yang terdapat dalam perangkat lunak.[8] Dalam konteks Indonesia, serangkaian serangan siber terhadap instansi pemerintah dan lembaga layanan publik telah menjadi bukti bahwa kejahatan ini bersifat lintas sektor dan berpotensi sistemik. Meski UU ITE telah mengatur sanksi terhadap akses ilegal dan gangguan terhadap integritas data, seperti dalam Pasal 32 dan 33, norma tersebut masih bersifat umum dan belum menyentuh aspek-aspek teknis seperti serangan *zero-day* atau penggunaan algoritma kriptografi dalam tindak pidana. Hal ini memperkuat argumen bahwa sistem hukum pidana yang selama ini berlandaskan pada pendekatan represif tradisional belum cukup responsif terhadap dimensi baru kriminalitas. Oleh karenanya, perlu ada pendekatan baru yang bersifat adaptif, berbasis teknologi, dan didukung oleh peningkatan kapasitas penegakan hukum.[9]

Perkembangan bentuk-bentuk kejahatan digital secara tidak langsung turut menggeser struktur aktor kriminal. Jika kejahatan konvensional seringkali melibatkan individu atau kelompok lokal, maka kejahatan siber membuka ruang bagi keterlibatan aktor lintas negara, bahkan negara itu sendiri. Kejahatan seperti *cyber espionage*, *data breach* terhadap server negara, hingga manipulasi informasi dalam skala politik menandai era baru kriminalitas global yang tidak mengenal batas geografis.[10] Hal ini menghadirkan tantangan yuridis baru, terutama terkait yurisdiksi hukum dan kerja sama internasional. Dalam sistem hukum pidana Indonesia, prinsip teritorialitas yang tercantum dalam Pasal 2 KUHP menjadi salah satu kendala utama, karena banyak tindak pidana siber dilakukan oleh pelaku yang berada di luar wilayah negara namun berdampak langsung terhadap warga negara atau kepentingan nasional. Meskipun Indonesia telah meratifikasi beberapa konvensi internasional terkait kejahatan lintas batas, seperti United Nations Convention against Transnational Organized Crime (UNTOC), namun secara substansial belum ada harmonisasi menyeluruh dalam sistem peraturan perundang-undangan.[11] Oleh karena itu, rekonstruksi hukum pidana harus pula mempertimbangkan dimensi globalisasi kriminal, serta memperluas cakupan yurisdiksi melalui pendekatan prinsip universal atau ekstrateritorial yang berbasis pada prinsip perlindungan dan kepentingan nasional.

2. Ciri-Ciri Khas Kejahatan Siber yang Membutuhkan Pendekatan Khusus

Salah satu karakter unik dari kejahatan siber adalah tingginya tingkat anonimitas pelaku. Dalam banyak kasus, pelaku tidak perlu menampakkan identitas secara langsung atau melakukan interaksi fisik dengan korban. Identitas bisa dengan mudah disembunyikan melalui penggunaan jaringan *proxy*, enkripsi, hingga *dark web*. Hal ini menyebabkan proses identifikasi dan penangkapan pelaku menjadi sangat sulit, bahkan ketika kerugian yang ditimbulkan sangat signifikan. Kejahatan semacam ini juga dapat dilakukan secara otomatis melalui bot, script, atau aplikasi yang dijalankan oleh sistem komputer tanpa keterlibatan aktif manusia secara terus-menerus. Dalam konteks hukum pidana Indonesia, tantangan ini belum sepenuhnya diakomodasi.[12] UU ITE memang

[8] Jorge Barros Filho, "Direito à Privacidade. Dignidade Humana. Sociedade Da Informação. Legislação. Crimes Digitais. 3895," 2018.

[9] Sheetal Temara, "The Dark Web and Cybercrime : Identifying Threats and Anticipating Emerging Trends" 6495, no. 10 (2024): 80–93.

[10] Francesco Frank Schiliro, "From Crime to Hypercrime : Evolving Threats and Law Enforcement ' s New Mandate in the AI Age," 2024, 1–28.

[11] Setyawan, "Enhancing Public Service Delivery through Digital Transformation : A Study on the Role of E-Government in Modern Public Administration Open Access."

[12] Naeem AllahRakha, "Transformation of Crimes (Cybercrimes) in Digital Age," *International Journal of Law and Policy* 2, no. 2 (2024): 1–19, https://doi.org/10.59022/ijlp.156.

mengatur mengenai larangan terhadap akses ilegal (Pasal 30) maupun perusakan data elektronik (Pasal 32), namun tidak menjelaskan secara teknis bagaimana proses identifikasi harus dilakukan dalam lingkungan digital yang penuh rekayasa anonimitas. Oleh sebab itu, pendekatan hukum pidana terhadap kejahatan digital harus mencakup dimensi teknis mengenai mekanisme pelacakan digital (*digital traceability*) serta kolaborasi dengan penyedia layanan teknologi untuk mengurai identitas pelaku yang tersembunyi.

Kejahatan siber juga memiliki karakteristik lintas yurisdiksi, yang menjadikannya sangat kompleks untuk ditangani dalam sistem hukum pidana yang masih berbasis teritorial. Dalam konteks ini, pelaku kejahatan bisa saja berada di negara berbeda dari tempat korban, atau bahkan menggunakan server dan jaringan yang tersebar di beberapa negara sekaligus. Ini menyebabkan perbedaan sistem hukum, kebijakan privasi, dan kewenangan otoritas penegak hukum menjadi hambatan dalam proses penanganan kasus. Indonesia masih menggunakan prinsip teritorialitas sebagai dasar utama yurisdiksi pidana sebagaimana diatur dalam Pasal 2 dan Pasal 3 KUHP, sehingga proses penindakan atas kejahatan yang bersifat transnasional menjadi sangat terbatas.[13] UU ITE pun belum memiliki ketentuan eksplisit terkait kerjasama lintas batas secara hukum pidana, meskipun pemerintah telah menjalin kerja sama internasional melalui Mutual Legal Assistance (MLA). Namun, prosedur MLA sering kali lamban dan tidak responsif terhadap kebutuhan mendesak penanganan kejahatan siber yang dinamis. Oleh karena itu, pendekatan baru perlu dirumuskan, termasuk penerapan prinsip yurisdiksi universal dalam kasus tertentu serta pembentukan mekanisme bilateral yang lebih fleksibel antara negara dalam hal pertukaran data dan penyidikan bersama (*joint cybercrime investigation*).[14]

Ciri lain yang menonjol dari kejahatan siber adalah kecepatan dan skalabilitas serangan. Berbeda dengan kejahatan konvensional yang terbatas pada ruang dan waktu, kejahatan digital dapat menyebar secara simultan ke ribuan bahkan jutaan sistem hanya dalam hitungan detik. Contoh ekstrem dapat dilihat pada serangan *Distributed Denial of Service (DDoS)* yang melumpuhkan sistem layanan publik, atau penyebaran *malware* yang merusak data penting dalam waktu singkat. Karakteristik ini menyebabkan dampak kejahatan menjadi jauh lebih luas dan tidak terkendali. Dalam konteks ini, hukum pidana yang bersifat reaktif tidak mampu menjawab secara efektif. Pasal-pasal dalam UU ITE seperti Pasal 33 tentang gangguan terhadap sistem elektronik tidak secara eksplisit menyesuaikan dengan aspek teknis serangan semacam DDoS atau *worms*. Maka, dibutuhkan regulasi yang bersifat prediktif dan preventif, termasuk pengaturan tentang tanggung jawab penyelenggara sistem elektronik dalam mengamankan jaringannya. Selain itu, penguatan deteksi dini berbasis *artificial intelligence* dan algoritma prediktif harus dipadukan dengan sistem hukum pidana agar penanggulangan kejahatan tidak selalu datang terlambat.[15]

Kesulitan dalam pengumpulan dan pembuktian alat bukti digital juga menjadi ciri khas kejahatan siber yang membutuhkan pendekatan hukum tersendiri. Bukti digital sangat mudah dimodifikasi, dihapus, atau disamarkan, dan dalam banyak kasus tidak meninggalkan jejak fisik sama sekali. Meskipun Pasal 5 UU ITE mengakui informasi

[13] Petroleum Microbiology, "This Work Is Licensed under a Creative Commons Attribution- This Work Is Licensed under a Creative Commons Attribution- ShareAlike 4 . 0 International License .," *Jurnal Multidisiplin Saintek* 45, no. 1 (2023): 1–17.

[14] Hamza Azam et al., "Cybercrime Unmasked: Investigating Cases and Digital Evidence," *International Journal of Emerging Multidisciplinaries: Computer Science & Artificial Intelligence* 2, no. 1 (2023): 1–31, https://doi.org/10.54938/ijemdcsai.2023.02.1.255.

[15] Erik Richardson Faria e Sousa, "Legal and Technical Challenges in the Pursuit of Cybercriminals: An Analysis of the Difficulties Faced by the Authorities," *Uniting Knowledge Integrated Scientific Research for Global Development*, 2023, https://doi.org/10.56238/uniknowindevolp-101.

elektronik dan/atau dokumen elektronik sebagai alat bukti yang sah, namun belum tersedia standar hukum dan teknis yang baku mengenai bagaimana proses *digital forensics* harus dilakukan agar hasilnya memiliki legitimasi hukum yang kuat. Banyak aparat penegak hukum masih belum memiliki kompetensi teknis dalam menelusuri *log file*, mengamankan *metadata*, atau memverifikasi keaslian bukti digital.[16] Hal ini berdampak pada kualitas proses peradilan dan memperbesar potensi pelaku lolos dari jeratan hukum. Oleh sebab itu, sistem hukum pidana perlu menyesuaikan diri dengan karakteristik ini melalui penguatan kapasitas institusi peradilan dalam bidang forensik digital, penyusunan regulasi pendukung yang bersifat teknis, dan sertifikasi penyidik dalam pengelolaan barang bukti elektronik. Tanpa pendekatan yang tepat terhadap karakteristik ini, kejahatan siber akan terus berada di luar jangkauan sistem hukum yang ada.[17]

3. Konsep dan Arah Rekonstruksi Hukum Pidana untuk Menangani Kejahatan Siber di Indonesia

Rekonstruksi hukum pidana dalam menghadapi kejahatan siber harus dimulai dari kesadaran bahwa ancaman di ruang digital menuntut respons hukum yang transformatif. Sistem hukum pidana yang bersifat statis, hierarkis, dan terikat pada ruang geografis tidak lagi memadai untuk merespons kejahatan yang bersifat dinamis, lintas negara, dan terdesentralisasi. Dalam konteks Indonesia, revisi Kitab Undang-Undang Hukum Pidana (KUHP) belum sepenuhnya merespons dinamika kejahatan siber, sebab pengaturan mengenai delik-delik siber masih bertumpu pada UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan perubahannya dalam UU No. 19 Tahun 2016. Namun, keduanya belum membentuk suatu sistem hukum pidana siber yang komprehensif. Oleh karena itu, arah rekonstruksi hukum pidana harus meliputi integrasi norma pidana khusus kejahatan siber ke dalam sistem hukum pidana nasional secara sistematis dan tidak parsial. Hal ini penting agar hukum pidana siber tidak bersifat sektoral dan mampu menjawab kompleksitas pelanggaran di ranah digital secara holistik.[18]

Rekonstruksi juga menuntut perubahan dalam asas dan prinsip hukum pidana. Asas legalitas yang rigid perlu diadaptasi agar dapat menampung kejahatan-kejahatan baru yang tidak selalu dapat dirumuskan secara tertulis sebelumnya. Perlu diperkenalkan prinsip *adaptive legality* dalam hukum pidana siber, di mana rumusan delik dapat bersifat terbuka sepanjang merujuk pada parameter teknis yang dapat dipertanggungjawabkan secara ilmiah dan hukum. Selain itu, asas teritorialitas yang menjadi dasar yurisdiksi dalam hukum pidana Indonesia sebagaimana diatur dalam Pasal 2 KUHP perlu dikaji ulang dalam konteks kejahatan siber yang bersifat lintas batas negara. Pembaruan hukum pidana perlu mengadopsi prinsip *extraterritorial jurisdiction* sebagaimana telah digunakan dalam beberapa negara untuk menangani kejahatan digital, utamanya dalam kasus-kasus yang melibatkan serangan terhadap infrastruktur kritikal negara. Integrasi pendekatan ini penting agar Indonesia memiliki landasan hukum kuat dalam menuntut pelaku siber crime meskipun berada di luar wilayah nasional.[19]

Di samping penguatan aspek normatif, rekonstruksi juga menyangkut pembaruan kelembagaan dan prosedural dalam sistem peradilan pidana. Penanganan kejahatan siber tidak hanya membutuhkan penegak hukum yang memiliki kapasitas teknis, tetapi juga

[16] Markus Djarawula, Novita Alfiani, and Hanita Mayasari, "Tinjauan Yuridis Tindak Pidana Kejahatan Teknologi Informasi (Cybercrime) Di Indonesia Ditinjau Dari Perspektif Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," *Jurnal Cakrawala Ilmiah* 2, no. 10 (2023): 3799–3806, https://doi.org/10.53625/jcijurnalcakrawalailmiah.v2i10.5842.

[17] Muhammad Randy Ammar et al., "Hukum Teknologi Informasi Tentang Penipuan Transaksi Jual Beli Online," *Jurnal Sosio-Komunika* 2, no. 1 (2023): 2830–39.

[18] AllahRakha, "Transformation of Crimes (Cybercrimes) in Digital Age."

[19] Microbiology, "This Work Is Licensed under a Creative Commons Attribution- This Work Is Licensed under a Creative Commons Attribution- ShareAlike 4 . 0 International License ."

struktur kelembagaan yang adaptif dan responsif terhadap perkembangan teknologi informasi. Oleh karena itu, diperlukan pembentukan unit khusus kejahatan siber di seluruh lini sistem peradilan, mulai dari kepolisian, kejaksaan, pengadilan hingga lembaga pemasyarakatan.[20] Saat ini, Direktorat Tindak Pidana Siber Bareskrim Polri memang telah berjalan, namun keberadaannya belum diimbangi oleh kesiapan kelembagaan di tingkat daerah maupun institusi lain yang terlibat dalam sistem peradilan. Selain itu, penguatan kapasitas aparat dalam melakukan *digital forensics*, pengamanan bukti elektronik, serta pemahaman terhadap kerangka hukum internasional menjadi kunci penting. Tanpa kesiapan kelembagaan yang menyeluruh, rekonstruksi hukum pidana hanya akan berhenti pada level normatif tanpa menghasilkan dampak yang konkret dalam perlindungan masyarakat dari serangan siber.

Rekonstruksi hukum pidana dalam konteks kejahatan siber juga harus mengakomodasi pendekatan keadilan restoratif dan preventif. Konsep keadilan pidana tidak lagi hanya ditujukan untuk pembalasan atau pemenjaraan pelaku, tetapi juga harus mempertimbangkan pemulihan korban, perlindungan hak privasi digital, serta pembentukan sistem keamanan digital kolektif. Oleh karena itu, perlu dikembangkan model penyelesaian sengketa elektronik melalui mekanisme alternatif seperti mediasi siber (*cyber mediation*) atau forum arbitrase digital yang berbasis pada prinsip keadilan. Ketentuan dalam Pasal 38 UU ITE yang memungkinkan penyelesaian sengketa di luar pengadilan dapat diperluas cakupannya dengan memperkuat kerangka hukum dan kelembagaan yang mendukung penyelesaian non-litigasi. Langkah ini akan mempercepat penyelesaian kasus, mengurangi beban lembaga peradilan, serta memberikan ruang keadilan yang lebih inklusif dan efisien bagi korban maupun pelaku, khususnya dalam kasus yang melibatkan pelanggaran ringan atau pertama kali.[21]

Akhirnya, arah rekonstruksi hukum pidana harus memperhatikan perkembangan hukum internasional serta praktik terbaik (*best practices*) dari negara-negara yang telah lebih dahulu membangun sistem hukum pidana siber yang mapan. Konvensi Budapest tentang Kejahatan Siber (Budapest Convention on Cybercrime) merupakan salah satu instrumen internasional yang relevan untuk diadopsi sebagai rujukan utama, karena mencakup pengaturan tentang harmonisasi hukum pidana nasional, kerjasama internasional, dan mekanisme penegakan hukum digital.[22] Meskipun Indonesia belum menjadi pihak dalam konvensi tersebut, namun substansi di dalamnya dapat dijadikan acuan dalam penyusunan perangkat hukum nasional yang kompatibel dengan standar global. Kesesuaian antara regulasi domestik dengan sistem internasional akan memperkuat posisi Indonesia dalam kolaborasi penegakan hukum lintas negara, serta memperkuat daya tahan hukum nasional dalam menghadapi gelombang kejahatan digital yang semakin masif dan kompleks. Dengan demikian, rekonstruksi hukum pidana terhadap kejahatan siber di Indonesia harus bersifat menyeluruh, meliputi pembaruan norma, kelembagaan, prosedur, dan kerangka kerja sama internasional yang saling terintegrasi.

4. Tuntutan Perubahan: Paradigma Hukum Pidana Modern

Perubahan paradigma dalam hukum pidana menjadi sebuah keniscayaan ketika berhadapan dengan kejahatan siber yang sangat dinamis dan disruptif. Paradigma hukum pidana yang selama ini cenderung reaktif, berbasis pada delik materiil, serta mengedepankan penghukuman setelah terjadinya pelanggaran, tidak lagi memadai. Dalam konteks kejahatan siber, tindakan pencegahan dan deteksi dini menjadi jauh lebih

[20] Azam et al., "Cybercrime Unmasked: Investigating Cases and Digital Evidence."

[21] Markus Djarawula, Novita Alfiani, and Hanita Mayasari, "Tinjauan Yuridis Tindak Pidana Kejahatan Teknologi Informasi (Cybercrime) Di Indonesia Ditinjau Dari Perspektif Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik."

[22] Sousa, "Legal and Technical Challenges in the Pursuit of Cybercriminals: An Analysis of the Difficulties Faced by the Authorities."

penting daripada sekadar penghukuman. Oleh karena itu, paradigma baru hukum pidana harus mencakup pendekatan preventif yang didukung oleh regulasi, kebijakan, serta teknologi yang mampu mengidentifikasi potensi serangan sebelum kerugian terjadi.[23] Hal ini dapat diwujudkan melalui perluasan norma hukum pidana yang tidak hanya melarang perbuatan, tetapi juga mewajibkan pengelola sistem elektronik untuk membangun arsitektur keamanan yang andal sebagaimana diatur dalam Pasal 15 dan Pasal 16 UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Ketentuan tersebut harus dipahami tidak semata sebagai tanggung jawab administratif, tetapi juga sebagai dasar pidana bila kelalaian sistem pengamanan menyebabkan kerugian serius bagi publik.

Selain preventif, paradigma hukum pidana modern juga harus bersifat partisipatoris, yaitu melibatkan berbagai elemen masyarakat dalam proses pencegahan dan penanggulangan kejahatan siber. Konsep ini menempatkan warga negara, institusi pendidikan, sektor swasta, hingga komunitas digital sebagai bagian dari sistem pertahanan hukum terhadap kejahatan siber. Pemerintah dapat menginisiasi model kemitraan antara penegak hukum dan masyarakat digital melalui pelaporan insiden siber, pelatihan literasi digital hukum, dan forum konsultasi kebijakan pidana digital. Pasal 40A UU ITE hasil perubahan melalui UU No. 1 Tahun 2024 menegaskan peran serta masyarakat dalam menjaga ekosistem digital yang sehat. Dengan demikian, hukum pidana tidak lagi menjadi domain eksklusif aparat penegak hukum, melainkan instrumen kolektif untuk menciptakan ruang digital yang aman dan tertib. Kolaborasi ini juga dapat meningkatkan kepercayaan publik terhadap sistem hukum, yang selama ini sering kali dipertanyakan terutama dalam kasus-kasus kontroversial terkait ITE.[24]

Paradigma hukum pidana modern juga menuntut reformulasi terhadap tujuan pemidanaan itu sendiri. Dalam konteks kejahatan siber, tujuan pembalasan tidak selalu efektif dalam memberikan efek jera, terutama bila pelaku adalah pelaku nonprofesional atau dilakukan tanpa motif ekonomi. Oleh karena itu, pemidanaan harus difokuskan pada restorasi kerugian korban, edukasi digital bagi pelaku, serta jaminan ketidakberulangan perbuatan.[25] Misalnya, dalam kasus ujaran kebencian atau penyebaran hoaks di media sosial, pendekatan yang mengedepankan rehabilitasi dan edukasi sering kali lebih tepat daripada pemenjaraan, apalagi jika pelaku adalah anak di bawah umur atau pengguna awam. UU No. 11 Tahun 2012 tentang Sistem Peradilan Pidana Anak (SPPA) dapat dijadikan rujukan pendekatan ini, di mana prinsip keadilan restoratif menjadi dasar utama dalam penyelesaian perkara anak, termasuk jika mereka terlibat dalam kejahatan siber. Dengan mengadopsi prinsip yang sama dalam hukum pidana umum untuk kasus tertentu, maka sistem hukum dapat menjadi lebih humanis dan efektif.

B. Analisis Kritis terhadap Kapasitas Sistem Peradilan Pidana Indonesia dalam Menangani Kejahatan Siber

1. Kekuatan dan Kelemahan UU ITE sebagai Dasar Hukum Pidana Siber

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang kemudian direvisi melalui UU Nomor 19 Tahun 2016 dan diperbarui kembali dalam UU Nomor 1 Tahun 2024, merupakan instrumen hukum utama yang menjadi dasar pemidanaan terhadap kejahatan siber di Indonesia. UU ini dirancang untuk menjawab kebutuhan regulasi terhadap penyimpangan perilaku di ruang digital, termasuk konten ilegal, akses tanpa hak, serta manipulasi data elektronik. Pasal-pasal krusial seperti Pasal 27 ayat (1) yang mengatur distribusi konten melanggar kesusilaan, Pasal 28 ayat (2) tentang penyebaran kebencian, serta Pasal 29 tentang ancaman kekerasan secara elektronik menjadi tulang punggung hukum pidana siber. Namun, meskipun memiliki

[23] AllahRakha, "Transformation of Crimes (Cybercrimes) in Digital Age."

[24] Microbiology, "This Work Is Licensed under a Creative Commons Attribution- This Work Is Licensed under a Creative Commons Attribution- ShareAlike 4 . 0 International License ."

[25] Azam et al., "Cybercrime Unmasked: Investigating Cases and Digital Evidence."

kekuatan normatif, substansi beberapa pasal masih menyisakan persoalan multitafsir dan membuka peluang kriminalisasi yang tidak proporsional terhadap ekspresi digital.[26]

Salah satu kelemahan mendasar dari UU ITE terletak pada rumusan norma yang terlalu lentur dan tidak selalu disertai parameter teknis yang jelas. Hal ini menyebabkan banyak pasal bersifat terbuka (*open norm*), yang menimbulkan interpretasi subjektif aparat penegak hukum. Misalnya, frasa "melanggar kesusilaan" pada Pasal 27 ayat (1) dan frasa "menimbulkan kebencian" pada Pasal 28 ayat (2) tidak memiliki indikator objektif yang tegas, sehingga rentan disalahgunakan dalam kasus yang seharusnya berada dalam ranah perdata atau etik.[27] Ketidakjelasan ini tidak hanya mengganggu asas kepastian hukum dalam Pasal 1 ayat (1) KUHP, tetapi juga berisiko menggerus hak-hak konstitusional warga sebagaimana dijamin dalam Pasal 28E dan 28F UUD 1945. Dengan demikian, meskipun UU ITE memberikan pijakan awal dalam kriminalisasi kejahatan siber, reformulasi norma sangat mendesak dilakukan agar hukum tidak menjadi alat represif yang melampaui proporsinya.

Selain masalah multitafsir, UU ITE juga menghadapi tantangan dalam penerapannya di lapangan. Aparat penegak hukum sering kali menghadapi kesulitan dalam mengumpulkan alat bukti elektronik yang sah secara hukum dan memenuhi standar pembuktian pidana. Pasal 5 hingga Pasal 15 UU ITE memang telah mengakui informasi dan dokumen elektronik sebagai alat bukti yang sah, namun belum disertai dengan standar operasional prosedur yang komprehensif dalam praktik. Proses penyitaan, otentikasi, serta integritas data digital sering kali tidak dilakukan sesuai prinsip *chain of custody*, yang mengakibatkan bukti menjadi tidak valid di pengadilan. Selain itu, belum semua aparat memiliki pelatihan khusus dalam digital forensics, menyebabkan pemidanaan terhadap pelaku siber crime menjadi inkonsisten. Oleh karena itu, kelemahan bukan hanya terletak pada substansi pasal, melainkan juga pada lemahnya kapasitas implementasi.[28]

Polemik mengenai UU ITE tidak dapat dipisahkan dari dinamika sosial-politik di ruang digital. Banyak pihak menilai bahwa UU ini lebih sering digunakan untuk membungkam kritik atau mengkriminalisasi aktivisme digital ketimbang menanggulangi kejahatan siber yang merugikan publik secara nyata. Data dari SAFEnet dan LBH Pers menunjukkan lonjakan kasus pelaporan menggunakan pasal-pasal UU ITE justru lebih dominan menyasar ekspresi di media sosial dibanding pelanggaran siber seperti peretasan atau penipuan daring. Hal ini mencerminkan adanya disorientasi dalam penggunaan perangkat hukum pidana, di mana kontrol sosial dan politik menjadi motivasi utama, bukan perlindungan hukum publik. Maka dari itu, rekonstruksi terhadap UU ITE harus diarahkan pada penyempurnaan delik hukum pidana dengan berbasis *harm principle*, yaitu hanya mengkriminalisasi perbuatan yang benar-benar merugikan secara substansial, bukan sekadar melanggar rasa tidak nyaman pihak lain.[29]

Terlepas dari kritik yang muncul, UU ITE tetap memiliki posisi penting dalam sistem peradilan pidana Indonesia di era digital. Keberadaan pasal-pasal yang mengatur akses ilegal, intersepsi tanpa hak, serta gangguan terhadap sistem elektronik sebagaimana diatur dalam Pasal 30 sampai 33 memberikan landasan hukum yang cukup untuk menangani tindakan subversif digital, seperti peretasan terhadap situs pemerintah atau pencurian data. Namun, keberhasilan penegakan hukum bergantung pada harmonisasi UU ITE dengan instrumen hukum lain, seperti UU No. 27 Tahun 2022 tentang Pelindungan Data

[26] Defril Hidayat, Hengki Firmanda, and Mahmud Hibatul Wafi, "Analysis of Hate Speech in the Perspective of Changes to the Electronic Information and Transaction Law," *Fiat Justisia: Jurnal Ilmu Hukum* 18, no. 1 (2024): 31–48, https://doi.org/10.25041/fiatjustisia.v18no1.3146.

[27] Sudarta, "**済無**No Title No Title No Title" 16, no. 1 (2022): 1–23.

[28] Xudaybergenov Azamat, "International Journal of Law and Policy | Volume: 1 Issue: 5 2023," *International Journal of Law and Policy* 1, no. 5 (2023): 1–8.

[29] Muhammad Arrullah Safriawan, "Legal Aspects of E-Commerce in the Law on Electronic Information and Transactions," *Focus Journal Law Review* 4, no. 1 (2024), https://doi.org/10.62795/fjl.v4i1.257.

Pribadi, UU No. 8 Tahun 2010 tentang TPPU, serta KUHAP dalam hal prosedur penyidikan dan pembuktian. Ke depan, dibutuhkan kodifikasi yang menyeluruh terhadap hukum pidana siber dalam satu regulasi khusus yang terintegrasi agar tidak terjadi tumpang tindih maupun kekosongan hukum dalam pelaksanaan di lapangan.[30]

2. Evaluasi Kelembagaan: Polisi, Kejaksaan, Pengadilan, dan Lembaga Pendukung

Evaluasi terhadap kapasitas kelembagaan dalam sistem peradilan pidana Indonesia menjadi aspek penting dalam menilai sejauh mana penegakan hukum terhadap kejahatan siber dapat dijalankan secara efektif. Kepolisian Negara Republik Indonesia (Polri), melalui Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri, telah menjadi ujung tombak dalam merespons serangan digital. Namun, persoalan mendasar yang masih menjadi hambatan adalah kesenjangan kompetensi sumber daya manusia, khususnya dalam bidang digital forensics dan cyber intelligence.[31] Walaupun Polri telah menjalin kerja sama dengan lembaga internasional dan melakukan pelatihan secara berkala, jumlah penyidik yang benar-benar menguasai teknik penyelidikan berbasis teknologi informasi masih sangat terbatas dibandingkan dengan kompleksitas dan volume kasus yang terus meningkat. Dalam konteks ini, kemampuan lembaga dalam menafsirkan dan mengimplementasikan ketentuan Pasal 43 UU ITE tentang penyidikan menjadi sangat krusial.

Kejaksaan, sebagai institusi penuntutan, juga memiliki peran penting dalam membawa kasus siber ke pengadilan. Namun demikian, hambatan yang dihadapi tidak jauh berbeda, yaitu belum optimalnya pemahaman jaksa terhadap karakteristik bukti digital dan cara pembuktiannya di persidangan. Jaksa sering kali masih berorientasi pada alat bukti konvensional, padahal Pasal 5 ayat (1) UU ITE telah menyatakan bahwa informasi dan dokumen elektronik memiliki kekuatan hukum yang sama dengan alat bukti lain. Tanpa pelatihan berkelanjutan dan modul teknis khusus tentang cyber crime, proses penuntutan rawan melemahkan kasus meskipun unsur-unsur pidana telah terpenuhi secara substansial. Kejaksaan Agung perlu memperluas keberadaan jaksa khusus bidang siber di tiap daerah serta membangun sistem pembaruan kompetensi yang adaptif terhadap perkembangan teknologi digital.[32]

Dari sisi peradilan, Mahkamah Agung sebagai pemegang kekuasaan kehakiman telah mengambil langkah positif dengan mengadopsi sistem persidangan elektronik melalui Peraturan Mahkamah Agung (Perma) No. 1 Tahun 2019. Namun, dalam konteks perkara pidana siber, pengadilan masih menghadapi tantangan dalam hal penilaian terhadap keabsahan dan integritas bukti elektronik. Hakim tidak hanya dituntut memahami aspek yuridis, tetapi juga aspek teknis dari mekanisme pengumpulan dan analisis bukti digital. Tanpa pemahaman tersebut, maka independensi dan objektivitas putusan menjadi rentan. Oleh karena itu, diperlukan pembentukan majelis hakim yang memiliki spesialisasi di bidang kejahatan siber, setidaknya di tingkat pengadilan negeri tertentu yang memiliki yurisdiksi atas wilayah dengan tingkat kerawanan digital yang tinggi. Langkah ini dapat meningkatkan kualitas putusan dan mencegah disparitas dalam penegakan hukum.[33]

Selain ketiga institusi utama, peran lembaga pendukung seperti Kementerian Komunikasi dan Informatika (Kominfo), Badan Siber dan Sandi Negara (BSSN), serta Lembaga Sandi Negara sangat strategis dalam memberikan dukungan teknis dan regulatif. Kominfo berwenang dalam pemutusan akses dan pemblokiran konten sebagaimana diatur

[30] Endang Lestari, Fakultas Hukum, and Universitas Tarumanagara, "Legal Study on Personal Data Protection Based on Indonesian Legislation 1,2" 6, no. 2 (2024): 471–77.

[31] Kharisma Ika Nurkhasanah and Zydane Maheswara Prasetyo, "Law Enforcement of State Jurisdiction in Hacking Crimes," *Indonesian Journal of Applied and Industrial Sciences (ESA)* 3, no. 3 (2024): 319–28, https://doi.org/10.55927/esa.v3i3.9438.

[32] Richart Sahatatua et al., "Cyber Law Analysis of E-KTP Data Leakage: A Case Approach of 102 Million KTP Data Allegedly Leaked from the Ministry of Social Affairs to a Hacker Forum," *Journal of Multidisciplinary Academic and Practice Studies* 2, no. 3 (2024): 261–65, https://doi.org/10.35912/jomaps.v2i3.2219.

[33] Economically Disadvantaged Community, "SIGn Jurnal Hukum" 5, no. 1 (2023): 59–73.

dalam Pasal 40 UU ITE, sedangkan BSSN berfungsi sebagai otoritas nasional dalam bidang keamanan siber yang dapat membantu proses investigasi teknis atas insiden digital. Meski demikian, koordinasi antar lembaga sering kali belum berjalan optimal karena keterbatasan sistem komando terpadu dan perbedaan mandat institusional. Untuk memperkuat sinergi, pemerintah perlu mempertimbangkan pembentukan badan koordinasi lintas lembaga yang memiliki kewenangan langsung terhadap penanganan kejahatan siber secara terintegrasi, termasuk dalam perumusan strategi nasional dan penyusunan regulasi teknis.[34]

Evaluasi kelembagaan juga mencakup kebutuhan akan tata kelola kelembagaan yang fleksibel namun tetap berbasis prinsip akuntabilitas. Kejahatan siber memerlukan respons cepat dan presisi tinggi, namun prosedur birokratis di banyak lembaga penegak hukum masih menjadi penghambat. Sebagai contoh, koordinasi lintas divisi dalam kasus cyber fraud yang melibatkan beberapa yurisdiksi membutuhkan waktu yang lama, padahal penanganan secara teknis harus dilakukan dalam waktu singkat agar pelaku tidak sempat menghapus jejak digital. Dalam hal ini, perlu adanya reformasi prosedural yang memungkinkan pembentukan satuan tugas ad hoc dengan kewenangan lintas sektoral yang dapat bergerak cepat dengan tetap tunduk pada prinsip hukum acara pidana sebagaimana diatur dalam KUHAP. Perubahan ini menjadi krusial untuk menyesuaikan irama kerja kelembagaan dengan karakteristik kejahatan siber yang cepat dan kompleks.

3. Analisis Studi Kasus Penegakan Hukum terhadap Cyber Crime

Analisis terhadap studi kasus penegakan hukum terhadap kejahatan siber di Indonesia menunjukkan adanya variasi respons yang cukup signifikan antara satu kasus dengan lainnya. Misalnya, dalam kasus peretasan situs Komisi Pemilihan Umum (KPU) pada 2023 oleh seorang pemuda asal Brebes yang berhasil mengakses jutaan data pemilih, proses penanganannya menunjukkan respons cepat dari kepolisian melalui Dittipidsiber Bareskrim Polri. Pelaku dikenakan Pasal 30 dan 32 UU ITE karena telah melakukan akses ilegal dan modifikasi sistem elektronik tanpa hak. Meski demikian, munculnya kasus tersebut mengindikasikan lemahnya sistem keamanan siber lembaga negara, serta menunjukkan belum adanya sistem mitigasi digital yang efektif sebelum insiden terjadi. Ini juga mencerminkan belum maksimalnya fungsi pengawasan oleh BSSN dan kurangnya integrasi sistem keamanan antar lembaga pemerintahan.[35]

Selain itu, kasus penipuan daring berbasis aplikasi investasi bodong seperti "Binomo" dan "Quotex" yang menyeret sejumlah figur publik ke dalam proses hukum, juga memperlihatkan tantangan penegakan hukum siber. Dalam kasus ini, pelaku dijerat menggunakan Pasal 28 ayat (1) UU ITE terkait penyebaran informasi menyesatkan dan merugikan konsumen dalam transaksi elektronik. Namun, proses penanganan hukum lebih banyak menyorot aspek pidana umum seperti penipuan dan penggelapan sebagaimana diatur dalam KUHP, ketimbang menitikberatkan pada penegakan aspek pidana siber secara menyeluruh. Hal ini menunjukkan masih belum optimalnya integrasi antara hukum pidana umum dan hukum pidana khusus dalam sistem peradilan siber, serta belum adanya pendekatan holistik yang mampu menangkap kompleksitas modus operandi digital.

Dalam laporan tahunan Bareskrim Polri dan Kominfo, terdapat peningkatan jumlah laporan kejahatan siber dari tahun ke tahun, terutama yang berkaitan dengan penipuan online dan pencemaran nama baik melalui media sosial. Namun, dari jumlah laporan tersebut, hanya sebagian kecil yang berhasil dibawa hingga ke meja hijau. Rendahnya tingkat keberhasilan ini salah satunya disebabkan oleh hambatan teknis dalam pengumpulan dan verifikasi bukti elektronik, serta keterbatasan kerja sama lintas lembaga dan yurisdiksi. Selain itu, proses hukum yang panjang dan kurang ramah terhadap korban juga menjadi penyebab banyaknya perkara yang tidak dilanjutkan atau diselesaikan melalui

[34] Dwi Nurahman et al., "Formation Of the Commissioner Judge Institution as A Court Supervision Policy (Judicial Scrutiny) Indonesian Criminal Justice System" 2, no. 4 (2024): 333–39.

[35] Nurkhasanah and Prasetyo, "Law Enforcement of State Jurisdiction in Hacking Crimes."

mediasi di luar pengadilan. Hal ini menandakan perlunya reformasi dalam prosedur penanganan kasus siber agar lebih adaptif dan efisien.[36]

Di sisi lain, studi kasus yang berhasil seperti pengungkapan sindikat pencurian data kartu kredit lintas negara bekerja sama dengan INTERPOL menunjukkan bahwa keberhasilan penegakan hukum kejahatan siber sangat bergantung pada kerja sama internasional. Dalam kasus ini, aparat Indonesia bekerja sama dengan otoritas Malaysia dan Singapura dalam melacak pelaku yang menjalankan operasinya dari luar negeri dengan korban warga Indonesia. Penegakan dilakukan dengan menggunakan prinsip ekstrateritorial sebagaimana diatur dalam Pasal 2 KUHP dan dikuatkan dengan ketentuan Pasal 43A ayat (2) UU ITE yang memungkinkan kerja sama antarnegara dalam penyidikan dan penuntutan. Studi ini menunjukkan bahwa tanpa kerangka kerja sama lintas negara, banyak kejahatan siber akan tetap berada di luar jangkauan yurisdiksi nasional.[37]

Secara keseluruhan, studi kasus dalam praktik penegakan hukum terhadap cyber crime di Indonesia menunjukkan adanya dualitas antara kesiapan normatif dan tantangan operasional. Di satu sisi, Indonesia telah memiliki kerangka hukum yang memungkinkan penindakan terhadap kejahatan digital, namun di sisi lain, implementasinya masih menghadapi berbagai kendala, baik dalam aspek teknis, sumber daya manusia, maupun koordinasi kelembagaan. Oleh karena itu, diperlukan penguatan sistem pembelajaran kelembagaan berbasis kasus (case-based learning) serta pengembangan sistem dokumentasi dan analisis putusan yang sistematis untuk membentuk preseden hukum pidana siber di Indonesia. Penguatan ini akan menjadi landasan bagi rekonstruksi hukum pidana yang lebih responsif dan berorientasi pada keadilan digital.[38]

4. Tantangan Penegakan Hukum: Regulasi, Infrastruktur, dan Kerja Sama Internasional

Tantangan paling mendasar dalam penegakan hukum terhadap kejahatan siber di Indonesia terletak pada aspek regulasi yang belum sepenuhnya adaptif terhadap dinamika perkembangan teknologi informasi. Meskipun Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) telah direvisi melalui UU Nomor 19 Tahun 2016, banyak ketentuan yang masih multitafsir dan belum mengatur secara komprehensif seluruh bentuk kejahatan siber yang terus bermunculan. Contohnya, ketentuan dalam Pasal 27 ayat (3) mengenai pencemaran nama baik masih menimbulkan kontroversi karena kerap disalahgunakan untuk membungkam kritik. Selain itu, tidak adanya klausul yang secara eksplisit mengatur tentang serangan siber terhadap infrastruktur kritis negara juga menjadi celah besar yang dapat dimanfaatkan pelaku kejahatan siber untuk merusak sistem vital nasional. Ketiadaan ketentuan spesifik ini menunjukkan bahwa sistem regulasi nasional belum sepenuhnya berparadigma pencegahan, melainkan masih bersifat reaktif dan sporadis.[39]

Selain regulasi, infrastruktur penunjang penegakan hukum terhadap kejahatan siber juga masih belum merata, terutama di tingkat daerah. Banyak unit cyber crime di kepolisian daerah belum memiliki perangkat forensik digital yang memadai, baik dari sisi perangkat keras maupun perangkat lunak. Situasi ini membuat investigasi terhadap kasus kejahatan siber kerap bergantung pada Jakarta sebagai pusat, yang menyebabkan keterlambatan dalam penanganan kasus. Padahal, menurut Pasal 43 ayat (1) UU ITE, penyidikan terhadap

[36] Melinda Dina Gussela et al., "Fenomena ' No Viral No Justice ' Perspektif Teori Penegakkan Hukum" 7, no. 2 (2025): 792–800.

[37] Menurut Perspektif, Hukum Dan, and Hak Asasi, "KEBEBASAN BERBICARA VERSUS PERTIMBANGAN KEAMANAN CYBER : MENURUT PERSPEKTIF HUKUM DAN HAK ASASI MANUSIA FREEDOM OF SPEECH VERSUS CYBER SECURITY CONSIDERATIONS : FROM A LEGAL AND HUMAN RIGHTS Sejarah Artikel" 5, no. 1 (2023): 32–47.

[38] Ahmad Fatoni, Pipit Yuliarpan, and Hj Imas, "Kejahatan Pidana Dalam Pemilu Di Indonesia" 3, no. 5 (2024): 981–89.

[39] Gussela et al., "Fenomena ' No Viral No Justice ' Perspektif Teori Penegakkan Hukum."

tindak pidana siber seharusnya dapat dilakukan oleh seluruh pejabat penyidik yang ditunjuk. Namun dalam praktiknya, keterbatasan infrastruktur menghambat pelaksanaan kewenangan tersebut secara efektif. Kesenjangan digital ini juga diperparah oleh minimnya alokasi anggaran negara untuk pengembangan infrastruktur penegakan hukum digital di wilayah-wilayah yang menjadi titik rawan kejahatan siber.[40]

Kerja sama internasional menjadi dimensi yang tidak bisa diabaikan dalam konteks kejahatan siber yang bersifat lintas batas. Sayangnya, Indonesia belum secara aktif terlibat dalam banyak perjanjian bilateral atau multilateral khusus yang menangani kejahatan siber secara teknis. Meskipun Indonesia tergabung dalam ASEAN Cybercrime Initiative dan telah bekerja sama dengan INTERPOL, Mutual Legal Assistance Treaty (MLAT) yang dimiliki Indonesia masih terbatas cakupannya. Hal ini menyulitkan proses ekstradisi atau pertukaran informasi digital yang diperlukan dalam penyidikan. Ketentuan Pasal 43A UU ITE tentang kerja sama internasional pun belum memiliki peraturan pelaksana yang konkret, sehingga aparat penegak hukum tidak memiliki pedoman operasional yang jelas dalam menjalin koordinasi dengan pihak luar negeri. Akibatnya, banyak kasus kejahatan digital lintas negara berhenti di tahap investigasi karena terhambat akses hukum lintas yurisdiksi.[41]

Ketimpangan akses terhadap teknologi antara pelaku dan aparat penegak hukum juga menjadi tantangan yang cukup krusial. Di banyak kasus, pelaku kejahatan siber telah menggunakan teknologi enkripsi, jaringan dark web, dan metode pembayaran kripto untuk menyamarkan identitas serta mempersulit pelacakan. Sementara itu, aparat hukum masih mengandalkan metode investigasi konvensional yang tidak mampu menjangkau ruang digital tertutup. Hal ini memerlukan pembaruan metode investigasi digital, pelatihan penyidik berbasis teknologi, serta kerja sama erat dengan penyedia layanan digital (internet service providers/ISPs) sebagai mitra utama dalam penanganan kejahatan daring. Meskipun UU ITE Pasal 38 memberikan wewenang kepada pemerintah untuk melakukan intersepsi atas informasi elektronik tertentu, mekanisme operasionalnya belum diatur secara rinci dan akuntabel. Ini menimbulkan kekhawatiran mengenai potensi pelanggaran hak privasi apabila tidak diawasi oleh mekanisme pengendalian eksternal.

Untuk mengatasi kompleksitas tantangan ini, Indonesia perlu segera menyusun Rancangan Undang-Undang Keamanan dan Ketahanan Siber (RUU KKS) yang telah lama masuk Prolegnas namun belum disahkan. RUU ini diharapkan dapat menjadi instrumen hukum yang komprehensif dalam mengatur keamanan siber nasional, termasuk mekanisme pencegahan, mitigasi, pemulihan, dan penindakan terhadap ancaman digital. Selain itu, penting juga membentuk satuan tugas nasional siber terpadu yang terdiri dari Polri, BSSN, Kejaksaan, dan Mahkamah Agung, dengan dukungan teknologi dan regulasi yang adaptif. Dengan demikian, rekonstruksi penegakan hukum pidana terhadap kejahatan siber tidak hanya berbasis pada hukum normatif, tetapi juga bertumpu pada infrastruktur institusional dan kerja sama global yang solid. Ini menjadi langkah strategis untuk menghadirkan sistem hukum yang mampu menjawab tantangan zaman digital secara holistik dan berkelanjutan.[42]

---

[40] Perspektif, Dan, and Asasi, "KEBEBASAN BERBICARA VERSUS PERTIMBANGAN KEAMANAN CYBER : MENURUT PERSPEKTIF HUKUM DAN HAK ASASI MANUSIA FREEDOM OF SPEECH VERSUS CYBER SECURITY CONSIDERATIONS : FROM A LEGAL AND HUMAN RIGHTS Sejarah Artikel."

[41] Ahya Amalia Deyanti and Neni Ruhaeni, "Implementasi Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik (Uu Ite) Terhadap Pelaku Judi Online Dan Penegakkan Perjudian Online Di Kabupaten Garut," *Bandung Conference Series: Law Studies* 4, no. 1 (2024): 151–59, https://doi.org/10.29313/bcsls.v4i1.9785.

[42] Edi Ribut Harwanto, "The Disguise of Cyber Crime in Illegal Investment Entities Post the Re-Formulation of Law No. 11 of 2020 Concerning Job Creation in Indonesia," *Eduvest - Journal of Universal Studies* 4, no. 1 (2024): 158–72, https://doi.org/10.59188/eduvest.v4i1.1005.

C. Rekonstruksi Hukum Pidana sebagai Respons terhadap Tantangan Kejahatan Siber

1. Konsep Rekonstruksi Hukum Pidana: Teoretis dan Normatif

Rekonstruksi hukum pidana dalam konteks kejahatan siber bukan sekadar upaya modifikasi atau amandemen terhadap norma-norma yang telah ada, melainkan merupakan pendekatan progresif yang bertolak dari kebutuhan zaman digital yang terus berkembang. Dalam teori hukum progresif yang dikembangkan oleh Satjipto Rahardjo, hukum tidak dilihat sebagai sistem tertutup yang kaku, tetapi sebagai sarana untuk mewujudkan keadilan substantif dan perlindungan terhadap masyarakat dari berbagai bentuk ancaman baru, termasuk yang muncul di ruang siber. Oleh karena itu, rekonstruksi hukum pidana digital harus dimulai dari pemahaman bahwa kejahatan siber memiliki karakteristik tersendiri yang tidak dapat dijawab hanya dengan pendekatan hukum konvensional yang bersifat represif dan terfragmentasi.[43]

Fenomena kriminalitas digital dewasa ini menunjukkan kompleksitas yang tinggi, baik dari segi modus operandi, lintas yurisdiksi, hingga kerugian yang ditimbulkan. Kejahatan siber tidak hanya menyasar individu, tetapi juga mengancam stabilitas negara, keamanan nasional, hingga integritas sistem demokrasi. Oleh karena itu, urgensi pembaruan hukum pidana dalam konteks ini menjadi semakin penting. Dalam ranah normatif, sistem hukum pidana yang berlaku, termasuk Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), dinilai masih memiliki banyak kekosongan normatif dan tumpang tindih aturan. Hal ini disebabkan karena UU yang ada umumnya lahir dari paradigma hukum yang dibentuk pada masa pra-digital, sehingga tidak memadai untuk menjawab tantangan zaman digital yang disruptif.[44]

Rekonstruksi hukum dalam hal ini mencakup tiga dimensi utama: konseptualisasi ulang terhadap delik digital, pembaruan struktur norma pidana, dan adaptasi prinsip-prinsip hukum pidana dalam konteks siber. Secara konseptual, perlu dirumuskan ulang definisi kejahatan siber agar dapat mencakup bentuk-bentuk kejahatan baru seperti manipulasi algoritma, deepfake, pencurian data biometrik, dan penggunaan artificial intelligence untuk tujuan kriminal. Reformulasi norma-norma pidana juga harus memperhatikan prinsip lex certa dan lex scripta agar tidak menimbulkan ketidakpastian hukum dan pelanggaran terhadap prinsip non-retroaktif dalam hukum pidana.

Selain itu, pendekatan normatif dalam rekonstruksi hukum pidana digital juga perlu memperhatikan prinsip-prinsip hak asasi manusia sebagai parameter etis dan konstitusional. Pembentukan norma baru tidak boleh mengorbankan kebebasan sipil seperti kebebasan berekspresi, privasi, dan hak atas informasi. Oleh karena itu, paradigma rekonstruksi harus bersifat responsif, inklusif, dan berbasis prinsip keadilan. Ini menuntut keterlibatan berbagai pemangku kepentingan, termasuk akademisi, praktisi hukum, lembaga negara, hingga masyarakat sipil dalam proses legislasi dan penyusunan kebijakan.

Dengan demikian, rekonstruksi hukum pidana sebagai respons terhadap kejahatan siber tidak dapat dilakukan secara parsial atau sektoral.[45] Ia memerlukan pendekatan sistemik yang mengintegrasikan pembaruan substansi hukum, penguatan struktur penegakan hukum, serta internalisasi nilai-nilai keadilan dan konstitusionalitas. Dalam kerangka inilah, rekonstruksi hukum pidana tidak hanya dimaknai sebagai pembaruan teknis, tetapi sebagai upaya transformatif untuk membangun sistem hukum yang adaptif, adil, dan berkelanjutan di tengah era digital yang penuh tantangan.

---

[43] Saifullah et al., *The Evaluation of the Indonesian Fintech Law From the Perspective of Regulatory Technology Paradigms To Mitigate Illegal Fintech*, *Jurisdictie: Jurnal Hukum Dan Syariah*, vol. 14, 2023, https://doi.org/10.18860/j.v14i2.24025.

[44] Putri Hasian Silalahi, Fiorella Angella Dameria, and Fiorella Angella Dameria, "Perlindungan Data Pribadi Mengenai Kebocoran Data Dalam Lingkup Cyber Crime Sebagai Kejahatan Transnasional," *Wajah Hukum* 7, no. 2 (2023): 614, https://doi.org/10.33087/wjh.v7i2.1244.

[45] Nurkhasanah and Prasetyo, "Law Enforcement of State Jurisdiction in Hacking Crimes."

2. Arah dan Strategi Pembaruan Substansi Hukum Pidana

Arah pembaruan hukum pidana dalam menghadapi kejahatan siber menuntut kerangka legislasi yang tanggap terhadap dinamika zaman dan perkembangan teknologi. Hal ini bukan sekadar soal modernisasi hukum, tetapi menyangkut perlindungan hak konstitusional warga negara dalam ruang digital. Dalam konteks ini, pembaruan terhadap Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) menjadi urgensi mutlak. Pasal-pasal seperti Pasal 27 ayat (3) tentang pencemaran nama baik dan Pasal 28 ayat (2) tentang penyebaran informasi kebencian telah menuai kontroversi akibat multitafsir dan implementasi yang tidak proporsional terhadap prinsip-prinsip hak asasi manusia.[46]

Selain itu, pasal-pasal dalam Kitab Undang-Undang Hukum Pidana (KUHP) yang diadopsi dari warisan kolonial juga belum sepenuhnya responsif terhadap bentuk-bentuk kriminalitas digital. Revisi KUHP yang tertuang dalam Undang-Undang Nomor 1 Tahun 2023 telah memperkenalkan beberapa ketentuan baru, namun belum secara khusus mengatur kejahatan siber secara komprehensif. Oleh karena itu, langkah reformulasi substansi hukum pidana perlu diarahkan pada penyusunan undang-undang khusus yang berfungsi sebagai *Cyber Penal Code*, sebagai lex specialis dalam menanggulangi kejahatan dunia maya.[47] Rujukan terhadap Konvensi Budapest tentang Cybercrime 2001 dapat dijadikan pijakan awal dalam menyusun rancangan tersebut, terutama dalam pengaturan terkait illegal access, data interference, dan system interference yang masih lemah dalam legislasi nasional.

Langkah strategis lainnya ialah menyisipkan pendekatan *risk-based regulation* ke dalam kerangka legislasi pidana. Ini berarti, hukum tidak semata-mata hadir setelah kejahatan terjadi, tetapi mampu mengidentifikasi dan merespons risiko kejahatan digital secara preventif. Dalam hal ini, prinsip kehati-hatian dan prinsip perlindungan data pribadi sebagaimana tercantum dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) perlu diintegrasikan ke dalam sistem pemidanaan yang lebih responsif. Pasal 65 hingga Pasal 73 UU PDP, misalnya, telah memuat sanksi pidana atas penyalahgunaan data, tetapi belum terkoordinasi secara menyeluruh dengan sistem pidana umum.[48]

Lebih jauh, arah legislasi juga harus menjamin sinkronisasi antara hukum pidana dengan peraturan administratif, perdata, dan konstitusional. Banyak pelanggaran dalam ruang siber yang bersifat lintas domain hukum, seperti kasus kebocoran data atau manipulasi algoritma yang menyentuh aspek hak ekonomi, kebebasan sipil, dan integritas digital warga negara. Oleh sebab itu, pembaruan substansi pidana harus diarahkan pada pembentukan sistem hukum yang *interdisciplinary* dan mampu menjawab kompleksitas realitas digital. Di sini, Pasal 28G ayat (1) dan Pasal 28H ayat (4) UUD 1945 yang menjamin hak atas rasa aman dan perlindungan terhadap data pribadi menjadi landasan normatif yang tidak dapat diabaikan.[49]

---

[46] Abdurrahman Harits Ketaren, "Juridical Review Of Cybercrime In The Criminal Act Of Defamation According To Ite Law And Criminal Law," *International Journal of Society and Law* 2, no. 1 (2024): 1–8, https://doi.org/10.61306/ijsl.v2i1.68.

[47] Hoover Wadiht Ruíz Rengifo, "Contribuciones Para Una Estrategia Pragmática En La Cuestión de La Responsabilidad Criminal de Las Personas Jurídicas," *Dos Mil Tres Mil* 25 (2023): 1–10, https://doi.org/10.35707/dostresmil/25385.

[48] Moh Iqbal Nuruddin and Mochammad Rofiqul Iqbal, "Dinamika Sistem Hukum Tata Negara Dalam Konteks Perubahan," *Reslaj : Religion Education Social Laa Roiba Journal* 6, no. 4 (2024): 2089–98, https://doi.org/10.47476/reslaj.v6i4.2067.

[49] Nina Yu. Skripchenko, "The Use of Information and Telecommunication Networks for Criminal Purposes: Regulatory Accounting and Prospects for Expanding Criminal Law Authority," *RUDN Journal of Law* 28, no. 1 (2024): 196–214, https://doi.org/10.22363/2313-2337-2024-28-1-196-214.

Penting pula menekankan bahwa reformulasi norma pidana harus menjunjung tinggi prinsip *legal clarity*, *necessity*, dan *proportionality* sebagaimana dijamin dalam Pasal 28J ayat (2) UUD 1945 dan Pasal 19 ayat (3) Kovenan Internasional tentang Hak Sipil dan Politik (ICCPR), yang telah diratifikasi melalui Undang-Undang Nomor 12 Tahun 2005. Hukum pidana tidak boleh menjadi instrumen represif yang melanggar kebebasan berekspresi, tetapi sebaliknya harus menjadi alat pelindung keadilan, kebenaran, dan integritas digital dalam masyarakat.[50]

Dengan merujuk dan menyinergikan berbagai regulasi yang ada, serta dengan keberanian politik dan visi keadilan digital yang progresif, maka arah dan strategi pembaruan substansi hukum pidana dapat mewujudkan sistem hukum yang tidak hanya represif, tetapi juga restoratif dan transformatif. Ini adalah wujud konkret dari tanggung jawab negara dalam memberikan jaminan hukum atas kehidupan digital yang adil, aman, dan beradab di era siber.

3. Rekonstruksi Proses dan Sistem Penegakan Hukum

Penegakan hukum dalam ranah kejahatan siber menghadapi tantangan yang sangat kompleks, baik dari sisi teknis, kelembagaan, maupun koordinasi antarinstansi. Oleh karena itu, rekonstruksi sistem penegakan hukum tidak dapat hanya bersandar pada pendekatan konvensional. Perlu dilakukan reformasi menyeluruh terhadap struktur, prosedur, dan teknologi yang digunakan oleh lembaga penegak hukum, guna menjawab dinamika kejahatan digital yang semakin canggih dan berskala lintas batas negara.[51] Dalam konteks ini, penguatan kapasitas *digital forensics* menjadi fondasi utama. Hal ini dapat dijabarkan melalui pembentukan unit khusus *cyber crime* dalam tubuh kepolisian, kejaksaan, dan lembaga peradilan, yang bekerja dengan standar interoperabilitas data, kecepatan penanganan, serta akurasi bukti digital.

Secara normatif, dasar hukum penguatan sistem penegakan ini dapat ditemukan dalam Pasal 14 ayat (1) dan (2) Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia, yang memberikan kewenangan kepada Polri untuk melakukan penyidikan terhadap seluruh bentuk tindak pidana, termasuk yang terjadi di ruang siber.[52] Selain itu, Keputusan Kapolri Nomor: Kep/74/I/2005 tentang Organisasi dan Tata Kerja Direktorat Tindak Pidana Tertentu Bareskrim Polri telah membuka jalan bagi penguatan unit khusus *cyber crime*, namun penguatan tersebut masih perlu didukung oleh infrastruktur forensik digital yang canggih dan regulasi teknis pendukung.

Dalam tataran prosedural, urgensi implementasi *electronic evidence* (e-evidence) menjadi krusial dalam proses peradilan. Peraturan Mahkamah Agung (Perma) Nomor 1 Tahun 2019 tentang Administrasi Perkara dan Persidangan di Pengadilan secara Elektronik merupakan langkah awal yang positif, namun belum secara khusus mengatur sistematisasi pembuktian elektronik untuk perkara pidana. Oleh karena itu, pembentukan regulasi khusus yang mengatur tata cara pengumpulan, autentikasi, penyimpanan, dan presentasi barang bukti digital dalam persidangan menjadi kebutuhan mendesak. Hal ini sejalan dengan ketentuan Pasal 5 ayat (1) huruf c Undang-Undang Nomor 11 Tahun 2008 (UU ITE), yang menyatakan bahwa informasi elektronik dapat dijadikan alat bukti hukum yang

[50] Ronaldo Silva, "VIOLÊNCIA SEXUAL NA ERA DIGITAL : UM ESTUDO SOBRE A CRIMINALIZAÇÃO DO ESTUPRO VIRTUAL SEXUAL VIOLENCE IN THE DIGITAL AGE : A STUDY ON THE VIRTUAL RAPE CRIMINALIZATION Luiza Lopes-Flois a Criminalização Do Estupro Virtual Tem Ganhado Destaque , à Medida Que Os Reparação de Danos Pelas Vítimas . Por Sua Vez , o Embate Normativo Em Torno," 2024, 269–97, https://doi.org/10.25110/rcjs.v27i1.2024-11341.

[51] Andrea Di Nicola, "Towards Digital Organized Crime and Digital Sociology of Organized Crime," *Trends in Organized Crime*, no. 0123456789 (2022), https://doi.org/10.1007/s12117-022-09457-y.

[52] Dwi Putri Melati Januri Hanafiah, "Implementasi Upaya Penanggulangan Tindak Pidana Cyber Di Era Teknologi," *Muhammadiyah Law Review* 6, no. 2 (2022): 32, https://doi.org/10.24127/lr.v6i2.2213.

sah. Namun, dalam praktiknya, belum semua aparat penegak hukum memahami mekanisme *chain of custody* dan validitas forensik digital dalam proses pembuktian.[53]

Selanjutnya, pengadilan juga perlu mulai menerapkan *AI-assisted justice* dalam menangani kasus kejahatan siber. Pemanfaatan teknologi kecerdasan buatan dalam proses adjudikasi dapat mendukung analisis pola kejahatan, mempercepat proses yuridis, dan meningkatkan akurasi pengambilan keputusan. Model ini telah diadopsi dalam sistem peradilan beberapa negara, seperti Estonia dan China, yang memanfaatkan *automated decision support system* dalam proses verifikasi awal perkara. Di Indonesia, implementasi teknologi ini dapat dimulai dari pengadilan niaga dan tindak pidana ekonomi khusus, sebagai pilot project yang dapat dikembangkan ke peradilan umum, sepanjang tidak melanggar prinsip *due process of law* dan independensi hakim.[54]

Lebih lanjut, rekonstruksi sistem penegakan hukum juga mensyaratkan sinergi antarlembaga, termasuk Badan Siber dan Sandi Negara (BSSN), Kementerian Komunikasi dan Informatika (Kominfo), serta lembaga perlindungan data seperti Komisi Informasi dan Komnas HAM. Sinergi ini harus didasarkan pada koordinasi yang jelas, pembagian tugas yang tidak tumpang tindih, serta penggunaan platform terpadu untuk pelaporan dan pelacakan kejahatan siber.[55] Dalam hal ini, keberadaan *National Cyber Security Strategy* sebagai bagian dari kebijakan nasional keamanan siber perlu dirancang ulang agar menjadi dokumen hukum yang operasional, tidak hanya sebagai pedoman administratif.

Di atas semua itu, sistem penegakan hukum pidana dalam menghadapi kejahatan digital juga harus memperhatikan prinsip keadilan substantif. Artinya, proses hukum tidak boleh menjadi alat represi yang melanggar hak warga negara, tetapi harus menjamin adanya perlindungan, kepastian, dan keadilan. Pasal 28D ayat (1) UUD 1945 secara tegas menyatakan bahwa setiap orang berhak atas pengakuan, jaminan, perlindungan dan kepastian hukum yang adil serta perlakuan yang sama di hadapan hukum. Oleh karena itu, rekonstruksi sistem penegakan hukum harus ditujukan untuk membangun kepercayaan publik terhadap lembaga hukum, terutama dalam perkara-perkara yang melibatkan ruang digital yang sangat sensitif dan kompleks.[56]

4. Integrasi Prinsip Hak Asasi dan Perlindungan Konstitusional dalam Ruang Siber

Ruang siber telah menjadi arena baru dalam perbincangan hak asasi manusia, di mana batas antara kebebasan dan kontrol menjadi semakin kabur. Di satu sisi, negara dituntut untuk menjaga keamanan siber dari ancaman kejahatan digital, seperti peretasan, penipuan daring, penyebaran disinformasi, hingga serangan siber lintas negara. Namun di sisi lain, pendekatan represif terhadap aktivitas digital berisiko melanggar hak asasi manusia, khususnya hak atas privasi, kebebasan berekspresi, serta perlindungan data pribadi. Dalam konteks ini, rekonstruksi hukum pidana digital harus mengintegrasikan prinsip-prinsip hak asasi secara utuh dan konstitusional.[57]

Konstitusi Republik Indonesia, khususnya dalam Pasal 28G ayat (1) dan Pasal 28F UUD 1945, memberikan jaminan atas hak untuk memperoleh perlindungan diri, rasa aman,

---

[53] G. M. Meretukov, S. I. Gritsaev, and V. V. Pomazanov, "Current Issues of Digitalization of Criminal Proceedings: A Look into the Future," *Law Enforcement Review* 6, no. 3 (2022): 172–85, https://doi.org/10.52468/2542-1514.2022.6(3).172-185.

[54] Anri Nishnianidze, "Some New Challenges of Cybercrime and Reasons Why Regulations Are Outdated," *European Scientific Journal ESJ* 9, no. September (2022): 288–302, https://doi.org/10.19044/esipreprint.9.2022.p288.

[55] T.O. Postolov, "Problems of Legal Security of the Interaction of Pre-Judicial Investigation Bodies and Cyberpolice Operational Units During the Fighting of Crimes in the Sphere of Intellectual Property," *Juridical Scientific and Electronic Journal*, no. 2 (2023): 494–97, https://doi.org/10.32782/2524-0374/2023-2/116.

[56] Hui Li et al., "A Technical Solution for the Rule of Law, Peace, Security, and Evolvability of Global Cyberspace -- Solve the Three Genetic Defects of IP Network," 2024, http://arxiv.org/abs/2412.10722.

[57] Azza Fitrahul Faizah and Muhammad Rifqi Hariri, "Pelindungan Hukum Terhadap Korban Revenge Porn Sebagai Bentuk Kekerasan Berbasis Gender Online Ditinjau Dari Undang-Undang Nomor 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual," *Jurnal Hukum Lex Generalis* 3, no. 7 (2022): 1–6, https://doi.org/10.56370/jhlg.v3i7.281.

serta hak untuk mencari, memperoleh, menyimpan, dan menyampaikan informasi dengan segala jenis saluran yang tersedia. Ini berarti, setiap pembatasan terhadap aktivitas digital warga negara harus melalui mekanisme yang sah, proporsional, dan berdasarkan hukum. Pembatasan tidak boleh dilakukan secara sewenang-wenang atas nama keamanan nasional semata, sebagaimana ditegaskan pula dalam Pasal 28J ayat (2) UUD 1945 yang menyatakan bahwa pembatasan hak asasi hanya dapat dilakukan untuk tujuan yang sah, seperti menjaga ketertiban umum, moralitas, atau hak orang lain.[58]

Lebih jauh, pengaturan hak asasi dalam ruang digital juga harus mengacu pada standar internasional, seperti *International Covenant on Civil and Political Rights* (ICCPR), yang telah diratifikasi oleh Indonesia melalui UU No. 12 Tahun 2005. Dalam Pasal 19 ICCPR, dinyatakan bahwa setiap orang berhak untuk berpendapat tanpa campur tangan dan memiliki kebebasan untuk mencari, menerima, serta menyampaikan informasi dalam berbagai bentuk. Oleh karena itu, regulasi nasional terkait kejahatan siber, seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta revisinya (UU No. 19 Tahun 2016), harus ditinjau ulang agar selaras dengan prinsip-prinsip tersebut. Salah satu kritik utama terhadap UU ITE adalah sifatnya yang kerap multitafsir dan membuka ruang kriminalisasi terhadap ekspresi digital, terutama melalui pasal-pasal tentang pencemaran nama baik dan penyebaran informasi yang dianggap melanggar kesusilaan.[59]

Oleh karena itu, perlu adanya harmonisasi antara upaya penegakan hukum siber dan perlindungan hak asasi, agar tidak terjadi kontradiksi antara tujuan keamanan dan demokrasi digital. Upaya ini dapat diwujudkan melalui perumusan *Bill of Digital Rights* sebagai kerangka normatif yang menjamin hak digital warga negara Indonesia. Inisiatif ini bukan semata simbolis, melainkan menjadi fondasi etis dan legal dalam membangun regulasi ruang siber yang manusiawi dan adil. Selain itu, penguatan lembaga pengawasan independen terhadap kebijakan siber juga diperlukan, seperti pembentukan *Ombudsman Digital*, atau penguatan peran Komnas HAM dan Komisi Informasi Publik untuk turut terlibat dalam evaluasi kebijakan dan tindakan penegak hukum dalam menangani perkara siber.

Pada aspek perlindungan data pribadi, integrasi prinsip hak asasi menjadi sangat penting. Dengan disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), negara memiliki kewajiban untuk menjamin bahwa data individu tidak disalahgunakan baik oleh pihak swasta maupun aparat negara. Namun implementasinya menuntut kesiapan kelembagaan dan mekanisme pengawasan yang kuat. Pasal 3 UU PDP menyebutkan bahwa pengolahan data pribadi harus dilakukan dengan prinsip transparansi, proporsionalitas, dan akuntabilitas. Prinsip-prinsip ini harus terintegrasi dalam sistem penyidikan, penuntutan, dan pengadilan pidana siber, agar tidak terjadi pelanggaran atas privasi yang sah.[60]

5. Rekomendasi Kebijakan dan Peta Jalan Rekonstruksi

Menyikapi kompleksitas dan dinamika kejahatan siber yang terus berkembang, negara perlu merumuskan kebijakan strategis dan peta jalan legislasi yang bersifat jangka pendek dan jangka panjang. Hal ini penting agar rekonstruksi hukum pidana tidak hanya bersifat reaktif terhadap perkembangan teknologi, tetapi juga bersifat antisipatif, inklusif, dan adaptif terhadap perubahan sosial serta norma hak asasi manusia yang berlaku. Rekomendasi kebijakan ini seyogianya tidak hanya difokuskan pada pembaruan substansi

[58] Ruíz Rengifo, "Contribuciones Para Una Estrategia Pragmática En La Cuestión de La Responsabilidad Criminal de Las Personas Jurídicas."

[59] Dorothy Estrada Tanck, "Cyberspace and Women's Human Rights in the International Legal Order: Transnational Risks and Gender-Based Violence," *Cuadernos de Derecho Transnacional* 16, no. 1 (2024): 192–207, https://doi.org/10.20318/cdt.2024.8420.

[60] В О Кучер, "ПРАВА ЛЮДИНИ ТА ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ ВІЙСЬКОВОЇ АГРЕСІЇ," 2024, 125–30.

hukum, tetapi juga pada reformasi kelembagaan, tata kelola, hingga penguatan kesadaran digital masyarakat.[61]

Pada level jangka pendek, langkah pertama yang harus dilakukan adalah revisi selektif terhadap pasal-pasal multitafsir dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), terutama Pasal 27, 28, dan 29 yang selama ini rawan digunakan untuk menjerat ekspresi publik secara berlebihan. Revisi ini harus dilakukan secara partisipatif dan melibatkan aktor lintas sektor, termasuk akademisi, praktisi hukum, organisasi masyarakat sipil, dan pelaku industri digital.[62] Di samping itu, penguatan kapasitas aparat penegak hukum dalam memahami dan menangani kejahatan siber harus menjadi prioritas. Hal ini mencakup pelatihan tentang digital forensics, etika penggunaan Artificial Intelligence (AI) dalam proses hukum, serta perlindungan data pribadi selama proses penyidikan.[63]

Dalam rencana jangka menengah, diperlukan penyusunan *Cyber Penal Code* atau *Kitab Undang-Undang Hukum Pidana Siber* sebagai regulasi *lex specialis* yang khusus menangani delik-delik digital, baik yang bersifat individual, transnasional, maupun berbasis teknologi tinggi. Cyber Penal Code ini harus memiliki struktur normatif yang jelas dan tidak tumpang tindih dengan KUHP, UU ITE, UU PDP, dan UU lainnya. Pengaturan ini diharapkan mencakup delik siber baru seperti deepfake manipulation, pemalsuan identitas digital, penyalahgunaan algoritma, dan manipulasi big data. Penegasannya dapat melibatkan prinsip *precautionary legal framework* yang mengatur batasan, larangan, serta kewajiban perlindungan bagi semua pihak dalam ekosistem digital.[64]

Selanjutnya, peta jalan legislasi jangka panjang perlu diarahkan pada integrasi sistem hukum nasional dengan kerangka hukum internasional, terutama Konvensi Budapest (Budapest Convention on Cybercrime) yang menjadi acuan global dalam pengaturan kejahatan siber. Meskipun Indonesia belum meratifikasi konvensi ini, penting bagi pemerintah untuk menyesuaikan substansi hukum pidana siber dengan standar global agar memiliki daya jangkau terhadap kejahatan lintas batas. Selain itu, rekonstruksi hukum pidana juga harus melibatkan sinkronisasi lintas sektor, mulai dari lembaga legislatif, yudikatif, hingga regulator digital seperti Kominfo dan Badan Siber dan Sandi Negara (BSSN).[65]

Pada aspek kelembagaan, penting untuk dibentuk unit khusus penegakan hukum siber di setiap tingkatan penegak hukum, mulai dari kepolisian, kejaksaan, hingga pengadilan. Unit ini perlu dilengkapi dengan laboratorium digital forensik, perangkat pemantauan real-time, serta personel dengan keahlian interdisipliner (hukum, teknologi, psikologi digital).[66] Dalam Pasal 14 UU No. 5 Tahun 2014 tentang ASN, disebutkan bahwa peningkatan kapasitas dan profesionalisme aparatur negara adalah bagian dari reformasi birokrasi yang wajib dilaksanakan untuk pelayanan publik yang responsif dan adaptif terhadap tantangan zaman, termasuk di ranah siber.[67]

Akhirnya, dalam mengawal keseluruhan proses rekonstruksi hukum pidana digital, diperlukan kebijakan pendidikan literasi digital dan etika hukum siber bagi masyarakat luas,

---

[61] Alfendo Yefta Argastya, "Penanggulangan Terhadap Kejahatan Cyber-Terrorism Melalui Politik Hukum Pidana," *Jurist-Diction* 7, no. 2 (2024): 245–62, https://doi.org/10.20473/jd.v7i2.44633.

[62] Rani Purwaningsih and Rahmat Dwi Putranto, "Tinjauan Yuridis Terhadap Penetapan Locus Delicti Dalam Kejahatan Dunia Maya (Cyber Crime) Berkaitan Dengan Upaya Pembaharuan Hukum Pidana Di Indonesia," *Mimbar Keadilan* 16, no. 1 (2023): 130–38.

[63] Vrizlynn L. L. Thing Jonathan W. Z. Lim, "Towards Effective Cybercrime Intervention," 2022.

[64] Jonathan W. Z. Lim.

[65] Rani Purwaningsih and Rahmat Dwi Putranto, "Tinjauan Yuridis Terhadap Penetapan Locus Delicti Dalam Kejahatan Dunia Maya (Cyber Crime) Berkaitan Dengan Upaya Pembaharuan Hukum Pidana Di Indonesia."

[66] François Delerue and Monica Kaminska, "Governing Cyber Crises: Policy Lessons from a Comparative Analysis," *Policy Design and Practice* 6, no. 2 (2023): 127–30, https://doi.org/10.1080/25741292.2023.2213061.

[67] WIDYA SETIABUDI SUMADINATA, "Cybercrime and Global Security Threats: A Challenge in International Law," *Russian Law Journal* 11, no. 3 (2023): 438–44, https://doi.org/10.52783/rlj.v11i3.1112.

sebagai bagian dari pendekatan non-penal. Hal ini penting untuk membangun kesadaran hukum dari bawah (bottom-up legal awareness), agar masyarakat tidak hanya menjadi objek hukum, tetapi juga subjek aktif dalam menciptakan ekosistem digital yang sehat. Pemerintah bersama perguruan tinggi, lembaga swadaya masyarakat, serta sektor swasta digital perlu bersinergi dalam membangun budaya hukum yang inklusif, adil, dan berkelanjutan dalam era transformasi digital.[68] Dengan demikian, peta jalan rekonstruksi hukum pidana bukan sekadar agenda normatif, tetapi harus menjadi proyek nasional yang melibatkan seluruh elemen bangsa demi mewujudkan keadilan substantif dan perlindungan hak-hak konstitusional dalam lanskap digital yang semakin kompleks dan cepat berubah.

Kesimpulan

Analisis terhadap sila kelima Pancasila, yaitu "Keadilan Sosial bagi Seluruh Rakyat Indonesia", menunjukkan bahwa falsafah dasar ini tidak hanya merupakan prinsip moral, tetapi juga menjadi landasan konstitusional dan arah kebijakan dalam mewujudkan keadilan distributif, prosedural, dan substantif di tengah kehidupan berbangsa. Pancasila sebagai etika nasional seharusnya menjadi fondasi dalam membangun sistem hukum, sosial, dan ekonomi yang berkeadilan. Namun, realitas empirik menunjukkan adanya ketimpangan sosial yang cukup tajam, baik dalam akses terhadap sumber daya, layanan publik, maupun perlakuan hukum. Ketimpangan tersebut memperlihatkan bahwa implementasi nilai-nilai Pancasila masih mengalami deviasi dalam praktik.

Upaya rekonstruksi hukum pidana yang responsif terhadap tantangan zaman, khususnya di era digital, menuntut pendekatan interdisipliner yang mengintegrasikan prinsip keadilan sosial dalam setiap formulasi dan implementasi kebijakan hukum. Reformasi substansi hukum pidana, sistem penegakan hukum yang transparan dan akuntabel, serta integrasi nilai-nilai HAM dalam ruang siber menjadi kebutuhan mendesak. Dengan demikian, sila kelima Pancasila bukan hanya menjadi simbol, tetapi benar-benar mewujud sebagai instrumen praksis keadilan yang menyentuh setiap sendi kehidupan rakyat.

Saran

1. Penguatan literasi etika pancasila pemerintah, institusi pendidikan, dan lembaga masyarakat sipil perlu memperkuat literasi publik mengenai nilai-nilai etika Pancasila, khususnya sila kelima, agar menjadi bagian dari kesadaran kolektif dalam menuntut dan menjalankan kehidupan yang berkeadilan.
2. Dekonstruksi kebijakan publik yang inklusif para pembuat kebijakan di semua level harus memastikan bahwa seluruh regulasi dan kebijakan pembangunan berorientasi pada prinsip keadilan sosial, tidak diskriminatif, dan sensitif terhadap kelompok rentan dan marjinal.
3. Rekonstruksi hukum progresif perlu dilakukan evaluasi menyeluruh terhadap perangkat hukum pidana nasional, termasuk hukum siber, agar tidak bersifat represif, melainkan mengedepankan pendekatan restoratif, partisipatif, dan menjamin hak atas keadilan bagi seluruh warga.
4. Integrasi ham dalam digital governance mengingat pesatnya perkembangan ruang digital, maka regulasi dan tata kelola dunia siber harus dilandasi oleh prinsip perlindungan HAM dan keadilan sosial, guna mencegah penyalahgunaan kekuasaan dan pelanggaran terhadap kebebasan sipil.
5. Pemetaan Ketimpangan sebagai Basis Perubahan: Dibutuhkan pemetaan yang akurat terhadap bentuk dan wilayah ketimpangan sosial, baik dalam dimensi ekonomi, hukum, maupun politik, yang dapat dijadikan sebagai dasar dalam merancang kebijakan transformatif yang selaras dengan nilai-nilai Pancasila.

[68] Siti Sumartiningsih, Susanto Santiago Pararuk, and Ngestu Dwi Setyo Pambudi, "Mechanism for Protecting Personal Data Against Crimes in Cyber-Space (Cyber Crime)," *Journal of Development Research* 7, no. 1 (2023): 95–103, https://doi.org/10.28926/jdr.v7i1.278.

Daftar Pustaka

Abdurrahman Harits Ketaren. "Juridical Review Of Cybercrime In The Criminal Act Of Defamation According To Ite Law And Criminal Law." *International Journal of Society and Law* 2, no. 1 (2024): 1–8. https://doi.org/10.61306/ijsl.v2i1.68.

Ahya Amalia Deyanti, and Neni Ruhaeni. "Implementasi Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik (Uu Ite) Terhadap Pelaku Judi Online Dan Penegakkan Perjudian Online Di Kabupaten Garut." *Bandung Conference Series: Law Studies* 4, no. 1 (2024): 151–59. https://doi.org/10.29313/bcsls.v4i1.9785.

Alfendo Yefta Argastya. "Penanggulangan Terhadap Kejahatan Cyber-Terrorism Melalui Politik Hukum Pidana." *Jurist-Diction* 7, no. 2 (2024): 245–62. https://doi.org/10.20473/jd.v7i2.44633.

AllahRakha, Naeem. "Transformation of Crimes (Cybercrimes) in Digital Age." *International Journal of Law and Policy* 2, no. 2 (2024): 1–19. https://doi.org/10.59022/ijlp.156.

Ammar, Muhammad Randy, Richardo Nezar M, Jievello Leonardo D, and Raihana Nasution. "Hukum Teknologi Informasi Tentang Penipuan Transaksi Jual Beli Online." *Jurnal Sosio-Komunika* 2, no. 1 (2023): 2830–39.

Anastasya, Vannya, Christine S T Kansil, Jurusan Hukum, Fakultas Hukum, Univeristas Tarumanagara Jakarta, and Kota Jakarta Barat. "Efektivitas Hukum Dan Kebijakan Publik Dalam Menghadapi Ancaman Siber Terhadap Keamanan Negara" 3, no. 2 (2024): 1710–16.

Diyah, Putri, Ayu Anggraini, Aqhina Dzikrah Aurora, Aprilia Niravita, Muhammad Adymas Hikal, and Harry Nugroho. "Electronic Certificates in Indonesia : Enhancing Legal Certainty or Introducing New," 2021, 686–98.

Estrada Tanck, Dorothy. "Cyberspace and Women's Human Rights in the International Legal Order: Transnational Risks and Gender-Based Violence." *Cuadernos de Derecho Transnacional* 16, no. 1 (2024): 192–207. https://doi.org/10.20318/cdt.2024.8420.

Faizah, Azza Fitrahul, and Muhammad Rifqi Hariri. "Pelindungan Hukum Terhadap Korban Revenge Porn Sebagai Bentuk Kekerasan Berbasis Gender Online Ditinjau Dari Undang-Undang Nomor 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual." *Jurnal Hukum Lex Generalis* 3, no. 7 (2022): 1–6. https://doi.org/10.56370/jhlg.v3i7.281.

Fatoni, Ahmad, Pipit Yuliarpan, and Hj Imas. "Kejahatan Pidana Dalam Pemilu Di Indonesia" 3, no. 5 (2024): 981–89.

Filho, Jorge Barros. "Direito à Privacidade. Dignidade Humana. Sociedade Da Informação. Legislação. Crimes Digitais. 3895," 2018.

Gussela, Melinda Dina, Mila Kurniawati, Jemmy Satria N, Denny Hermanto, Silvanus Fauziansah, and Beni Ahmad Saebani. "Fenomena ' No Viral No Justice ' Perspektif Teori Penegakkan Hukum" 7, no. 2 (2025): 792–800.

Hanafiah, Dwi Putri Melati Januri. "Implementasi Upaya Penanggulangan Tindak Pidana Cyber Di Era Teknologi." *Muhammadiyah Law Review* 6, no. 2 (2022): 32. https://doi.org/10.24127/lr.v6i2.2213.

Harwanto, Edi Ribut. "The Disguise of Cyber Crime in Illegal Investment Entities Post the Re-Formulation of Law No. 11 of 2020 Concerning Job Creation in Indonesia." *Eduvest - Journal of Universal Studies* 4, no. 1 (2024): 158–72. https://doi.org/10.59188/eduvest.v4i1.1005.

Hidayat, Defril, Hengki Firmanda, and Mahmud Hibatul Wafi. "Analysis of Hate Speech in the Perspective of Changes to the Electronic Information and Transaction Law." *Fiat Justisia: Jurnal Ilmu Hukum* 18, no. 1 (2024): 31–48. https://doi.org/10.25041/fiatjustisia.v18no1.3146.

Jonathan W. Z. Lim, Vrizlynn L. L. Thing. "Towards Effective Cybercrime Intervention," 2022.

Lestari, Endang, Fakultas Hukum, and Universitas Tarumanagara. "Legal Study on Personal Data Protection Based on Indonesian Legislation 1,2" 6, no. 2 (2024): 471–77.

Li, Hui, Kedan Li, Jiaqing Lv, Yuanshao Liang, Feng Han, and Shuo-Yen Robert Li. "A Technical Solution for the Rule of Law, Peace, Security, and Evolvability of Global Cyberspace -- Solve the Three Genetic Defects of IP Network," 2024. http://arxiv.org/abs/2412.10722.

Li, Jiabao. "Multi-Governance Model of New Cybercrime under the Risk of New Technologies Risks and Responses" 0, no. August (2024): 22–29. https://doi.org/10.54254/2753-7048/73/2024.BO17965.

Markus Djarawula, Novita Alfiani, and Hanita Mayasari. "Tinjauan Yuridis Tindak Pidana Kejahatan Teknologi Informasi (Cybercrime) Di Indonesia Ditinjau Dari Perspektif Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik." *Jurnal Cakrawala Ilmiah* 2, no. 10 (2023): 3799–3806. https://doi.org/10.53625/jcijurnalcakrawalailmiah.v2i10.5842.

Meretukov, G. M., S. I. Gritsaev, and V. V. Pomazanov. "Current Issues of Digitalization of Criminal Proceedings: A Look into the Future." *Law Enforcement Review* 6, no. 3 (2022): 172–85. https://doi.org/10.52468/2542-1514.2022.6(3).172-185.

Microbiology, Petroleum. "This Work Is Licensed under a Creative Commons Attribution- This Work Is Licensed under a Creative Commons Attribution- ShareAlike 4 . 0 International License ." *Jurnal Multidisiplin Saintek* 45, no. 1 (2023): 1–17.

Muhammad Arrullah Safriawan. "Legal Aspects of E-Commerce in the Law on Electronic Information and Transactions." *Focus Journal Law Review* 4, no. 1 (2024). https://doi.org/10.62795/fjl.v4i1.257.

Nicola, Andrea Di. "Towards Digital Organized Crime and Digital Sociology of Organized Crime." *Trends in Organized Crime*, no. 0123456789 (2022). https://doi.org/10.1007/s12117-022-09457-y.

Nishnianidze, Anri. "Some New Challenges of Cybercrime and Reasons Why Regulations Are Outdated." *European Scientific Journal ESJ* 9, no. September (2022): 288–302. https://doi.org/10.19044/esipreprint.9.2022.p288.

Nurahman, Dwi, A Irzal Fardiansyah, Muhammad Akib, and H S Tisnanta. "Formation Of the Commissioner Judge Institution as A Court Supervision Policy (Judicial Scrutiny) Indonesian Criminal Justice System" 2, no. 4 (2024): 333–39.

Nurkhasanah, Kharisma Ika, and Zydane Maheswara Prasetyo. "Law Enforcement of State Jurisdiction in Hacking Crimes." *Indonesian Journal of Applied and Industrial Sciences (ESA)* 3, no. 3 (2024): 319–28. https://doi.org/10.55927/esa.v3i3.9438.

Nuruddin, Moh Iqbal, and Mochammad Rofiqul Iqbal. "Dinamika Sistem Hukum Tata Negara Dalam Konteks Perubahan." *Reslaj : Religion Education Social Laa Roiba Journal* 6, no. 4 (2024): 2089–98. https://doi.org/10.47476/reslaj.v6i4.2067.

Perspektif, Menurut, Hukum Dan, and Hak Asasi. "KEBEBASAN BERBICARA VERSUS PERTIMBANGAN KEAMANAN CYBER : MENURUT PERSPEKTIF HUKUM DAN HAK ASASI MANUSIA FREEDOM OF SPEECH VERSUS CYBER SECURITY CONSIDERATIONS : FROM A LEGAL AND HUMAN RIGHTS Sejarah Artikel" 5, no. 1 (2023): 32–47.

Postolov, T.O. "Problems of Legal Security of the Interaction of Pre-Judicial Investigation Bodies and Cyberpolice Operational Units During the Fighting of Crimes in the Sphere of Intellectual Property." *Juridical Scientific and Electronic Journal*, no. 2 (2023): 494–97. https://doi.org/10.32782/2524-0374/2023-2/116.

Rani Purwaningsih, and Rahmat Dwi Putranto. "Tinjauan Yuridis Terhadap Penetapan Locus Delicti Dalam Kejahatan Dunia Maya (Cyber Crime) Berkaitan Dengan Upaya Pembaharuan Hukum Pidana Di Indonesia." *Mimbar Keadilan* 16, no. 1 (2023): 130–38.

Ruíz Rengifo, Hoover Wadiht. "Contribuciones Para Una Estrategia Pragmática En La Cuestión de La Responsabilidad Criminal de Las Personas Jurídicas." *Dos Mil Tres Mil* 25 (2023): 1–10. https://doi.org/10.35707/dostresmil/25385.

Sallapalli, Nihitha. "Digital Transformation : Reshaping Industries Through Technology" 6, no. 6 (n.d.): 1–9.

Schiliro, Francesco Frank. "From Crime to Hypercrime : Evolving Threats and Law Enforcement

’ s New Mandate in the AI Age,” 2024, 1–28.

Setyawan, Adhitya Chandra. “Enhancing Public Service Delivery through Digital Transformation : A Study on the Role of E-Government in Modern Public Administration Open Access,” 2024.

Sifa, Abdan. “Transformasi Digital E-Commerce Dalam Menguasai Kosentrasi Pasar Di Indonesia” 2, no. 12 (2024): 405–13.

Silalahi, Putri Hasian, Fiorella Angella Dameria, and Fiorella Angella Dameria. “Perlindungan Data Pribadi Mengenai Kebocoran Data Dalam Lingkup Cyber Crime Sebagai Kejahatan Transnasional.” *Wajah Hukum* 7, no. 2 (2023): 614. https://doi.org/10.33087/wjh.v7i2.1244.

Silva, Ronaldo. “VIOLÊNCIA SEXUAL NA ERA DIGITAL : UM ESTUDO SOBRE A CRIMINALIZAÇÃO DO ESTUPRO VIRTUAL SEXUAL VIOLENCE IN THE DIGITAL AGE : A STUDY ON THE VIRTUAL RAPE CRIMINALIZATION Luiza Lopes-Flois a Criminalização Do Estupro Virtual Tem Ganhado Destaque , à Medida Que Os Reparação de Danos Pelas Vítimas . Por Sua Vez , o Embate Normativo Em Torno,” 2024, 269–97. https://doi.org/10.25110/rcjs.v27i1.2024-11341.

Skripchenko, Nina Yu. “The Use of Information and Telecommunication Networks for Criminal Purposes: Regulatory Accounting and Prospects for Expanding Criminal Law Authority.” *RUDN Journal of Law* 28, no. 1 (2024): 196–214. https://doi.org/10.22363/2313-2337-2024-28-1-196-214.

Sousa, Erik Richardson Faria e. “Legal and Technical Challenges in the Pursuit of Cybercriminals: An Analysis of the Difficulties Faced by the Authorities.” *Uniting Knowledge Integrated Scientific Research for Global Development*, 2023. https://doi.org/10.56238/uniknowindevolp-101.

Sudarta. “済無No Title No Title No Title” 16, no. 1 (2022): 1–23.

Sumartiningsih, Siti, Susanto Santiago Pararuk, and Ngestu Dwi Setyo Pambudi. “Mechanism for Protecting Personal Data Against Crimes in Cyber-Space (Cyber Crime).” *Journal of Development Research* 7, no. 1 (2023): 95–103. https://doi.org/10.28926/jdr.v7i1.278.

Temara, Sheetal. “The Dark Web and Cybercrime : Identifying Threats and Anticipating Emerging Trends” 6495, no. 10 (2024): 80–93.

Valentine, Virginia, Clara Sinta Septiani, and Jadiaman Parshusip. “Menghadapi Tantangan Dan Solusi Cybercrime Di Era Digital Facing Cybercrime Challenges And Solutions In The Digital Era” 1 (2024): 2–6.

WIDYA SETIABUDI SUMADINATA. “Cybercrime and Global Security Threats: A Challenge in International Law.” *Russian Law Journal* 11, no. 3 (2023): 438–44. https://doi.org/10.52783/rlj.v11i3.1112.

Кучер, В О. “ПРАВА ЛЮДИНИ ТА ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ ВІЙСЬКОВОЇ АГРЕСІЇ,” 2024, 125–30.