Law Research Review Quarterly
Vol. 11 Issue 3 (2025) 1169–1197
DOI:
Online **at**
Available online since:

Mengurai Paradigma Pemidanaan Dalam Konteks Kebijakan Kriminal Di Era Digital

Farida Dzalaqah, Indah Sri Utami

Faculty of Law, Universitas Negeri Semarang, Indonesia
First Author Email: dzdiana89@students.unnes.ac.id
First Author Email: indahsuji@mail.unnes.ac.id

Abstract

The development of technology and information has created new spaces that offer convenience in life. However, behind this ease lies a loophole exploited by individuals with malicious intent. This space is used as a means to commit criminal acts. Crime in the digital era represents a modern type of offense that requires a different legal approach compared to conventional crimes. The shifting characteristics and modus operandi of criminal acts in the digital era must be met with a reconstruction of positive law in Indonesia. This is crucial to ensure that these crimes can still be effectively handled, thereby maintaining state order.

KEYWORDS *Criminal Act, Digital, Characteristics, Reconstruction*

Submitted: ..... **Reviewed**: ..... **Revised**: ..... **Accepted**: .....
✉ Corresponding email: dzdiana89@students.unnes.ac.id

I. Pendahuluan

Proses digitalisasi yang terjadi selama dua dekade terakhir telah menciptakan perubahan signifikan dalam keseluruhan aspek kehidupan, hingga merambah pada sektor kehidupan bermasyarakat maupun pribadi, perekonomian, pendidikan hingga pemerintahan. Perubahan struktural yang terjadi menghadirkan cara baru berkomunikasi dengan sangat efisien dan cepat, namun atas perubahan tersebut menimbulkan munculnya ruang kosong yang rentan berpotensi untuk terjadi berbagai pelanggaran hukum[1]. Dalam menanggulangi percepatan teknologi, Indonesia melakukan langkah pemanfaatan teknologi yang telah di dorong dengan kebijakan nasional seperti *Roadmap Indonesia Digital 2021-2024* dan *Rencana Induk Transformasi Digital Nasional.* Namun, perlu diakui bahwa perkembangan teknologi yang secara massif belum dapat diimbangi dengan kesiapan regulasi yang ada, terutama dalam ranah hukum pidana.[2] Fenomena digitalisasi yang menghadirkan domain baru untuk terjadi tindak pidana digital atau *cyberspace* yang membutuhkan regulasi hukum komprehensif dan adaptif terhadap dinamika teknologi yang terus berkembang[3].

Data statisktik kejatan cyber berdasarkan data Badan Siber dan Sandi Negara (BSSN) mengatakan bahwa pada tahun 2013, terdapat peningkatan signifikan terhadap amgka kejahatan siber dengan total 1.2 miliar kejahatan pada berbagai sektor strategis nasional. Serta berdasarkan laporan dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) menunjukan kerugian ekonomi yang timbul akibat kejahatan siber di Indonesia mencapai angka RP 7,8 trilliun per tahun. Selain dari data yangtelah dijabarkan, komplesitas kejahatan pidana dalam era digital atau kejahatan siber yang saat ini terjadi semakin meningkat dan hadir dengan berbagai modus baru yang sebelumnya belum pernah ada dengan

---

[1] Barda Nawawi Arief, *Tindak pidana mayantara: perkembangan kajian cyber crime di Indonesia*. Jakarta: RajaGrafindo Persada, 2006.

[2] Nihitha Sallapalli, "Digital Transformation: Reshaping Industries Through Technology," *International Journal For Multidisciplinary Research* vol. 6, no. 6 (November 27, 2024): 31446. doi: https://doi.org/10.36948/ijfmr.2024.v06i06.31446.

[3] Ahmad M. Ramli, *Cyber law & HAKI: dalam sistem hukum Indonesia*, Cetakan ketiga. Bandung: Refika Aditama, 2010.

kesulitan yang tinggi. Modus yang kerap ditemu dalam kejahatan ciber yakni pelaku yang bersifat anonim, *deepfake, cryptojacking, ransomware* dan kejahatan yang memanfaatkan *artificial intelligence*[4].

Karakteristik kejahatan siber memiliki banyak perbedaan dengan kejahatan konvensional, selain dari kompleksitas dan modusnya, kejahatan siber juga memiliki kemudahan untuk dilakukan secara massal dengan kemampuan unruk melewatis batas ruang dan waktu hingga batas-batas yurikdisi suatu Negara sehingga sulit bila melakukan pendekatan kejahatan siber dengan pendakatan hukum pidana konvensional[5]. Indonesia telah memiliki regulasi untuk mengatasi kejahatan pidana yang terjadi pada era digitalisasi yakni 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 selain itu pengaturan terhadap kejahatan siber telah diatur dalam ketentuan KUHP 2023. Namun, hadirnya regulasi hukum positif mengenai kejahatan siber masih terdapat beberapa kekurangan maupun tantangan[6] dalam pengimplementasi hukum tersebut baik dari segi aparat penegak hukum hingga interprestasi pembuktian dalam persidangan.

Dalam kacamata hukum pidana, kejelasan norma menjadi salah satu tantangan dalam menghadapi kejahatan siber namun tidak hanya terfokus pada kejahatan norma, kapasitas suatu kelembagaan bertugas juga mengambil peran yang cukup fundamental sebagai jawaban untuk menangani kejahatan siber. Dalam penyelesaian kejahatan menurut hukum pidana dilakukan memlui berbagai proses yakni penyelidikan, penyidikan dan persidangan. Dalam proses penyelidikan dibutuhkan bukti permulaan terhadap suatu tindak pidana yang dalam kejahatan siber dibutuhkan keahlian forensic digital, infrastruktur teknologi

---

[4] Edmon Makarim, *Kompilasi hukum telematika*, Cet. 1. Jakarta: Divisi Buku Perguruan Tinggi, RajaGrafindo Persada, 2003.

[5] Vannya Anastasya and others, "Efektivitas Hukum Dan Kebijakan Publik Dalam Menghadapi Ancaman Siber Terhadap Keamanan Negara," *Unknown Journal*, no. 2 (2024): 1710–16.

[6] W. Widodo, *Sistem Pemidanaan Dalam Cyber Crime.* Aswaja Pressindo, 2021.

mutakhir, serta kemampuan analisis data elektronik yang harus dimiliki secara merata oleh seluruh aparat penegak hukum. Namun, penalaran dan pemahaman mengenai analisis terhadap bukti digital belum merata kepada seluruh aparat penegak hukum yang menimbulkan hambatan dalam upaya penegakan hukum yang efektif dan akuntanbel. Sebagai contoh pelacakan pelaku kejahatan siber yang bersifat anonim memerlukan usaha ekstra disbanding dengan kejahatan konvensional, tidak hanya terbatas anonim kejahatan siber yang telah melibatkan beberapa Negara juga kerap terhambat oleh keterbatasan kerjasama internasional serta kurangnya mekanisme mutual legal assistance yang responsive dan cepat.[7] Selain itu, penegakan hukum yang bersifat fragmentasi dan sektoral melemahkan proses koordinasi antar instansi terkait seperti pada kepolisian, kejaksaan dan kementerian komunikasi dan informatika serta badan instansi terkait lainya. Dalam keadaan seperti ini, subtansi hukum pidana menghadapi stagnasi dan menghadapi tantangan pada kelembagaan serta struktural. Sedangkan konstitusi telah menjamin warga Negara mendapatkan perlindungan terhadap rasa aman dan terhindar dari ancaman sebagaimana amanat dalam Pasal 28G ayat (1) Undang Undang Dasar Negara Republik Indonesia Tahun 1945. Ketidakmampuan Negara untuk dapat menghadirkan sistem hukum yang diandal dalam menangani kejahatan siber akan menimbulkan berkurangnya kepercayaan publik terhadap supremasi hukum dan keadilan.[8]

Artikel ini disusun memiliki tujuan untuk memberikan analisis konseptual dan yuridis terhadap kebijakan hukum yang ada di Indonesia dalam mengahadapi tindak pidana yang terjadi para era digital. Penelitian ini dilandaskan kepada paradigm hukum progresif dan berupaya mengidentifikasikan pengimplementasian regulasi dengan kesiapan sistem peradilan di Indonesia. Selain itu, penulisan artikel ini juga bertujuan untuk memberikan masukan melalui pendekatan alternative

---

[7] 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.

[8] Putri Diyah Ayu Anggraini et al., "Electronic Certificates in Indonesia: Enhancing Legal Certainty or Introducing New Challenges?," *Arkus* vol. 11, no. 1 (November 12, 2024): 686–98. doi: https://doi.org/10.37275/arkus.v11i1.659.

dalam perumusan kebijakan hukum pidana. Penelitian ini memiliki urgensi yang terletak pada ancaman keamanaan nasional dan ketertiban public yang terganggu oleh meningkatnya ekalasi cybercrime yang bilamana tidak diimbangi penanggulan dengan cepat dengan penggunaan hukum yang tepat akan menyebabkan sistem hukum Indonesia semakin tertinggal dalam era digital ini. Dengan penulisan artikel ini diharapkan dalam dapat menjadi landasan berpikir dan membantu dalam pemikiran terkait mengatasi kejahatan siber di Indonesia.

II. Metode Penelitian

Penelitian ini menggunakan pendekatan yuridis normatif yang menggunakan asas-asas hukum sebagai pondasi pembahasan[9], dengan terfokus kepada analisis hukum positif di Indonesia secara menyeluruh dan mendalam mengenai fenomena kejahatan digital yang terjadi pada era digital. Penelitian ini menggunakan pendekatan *library resarch* dan berfokus kepada pengumpulan dan analisis sata yang di dapat dari kajian ilmiah nasional dan internasional serta peraturan hukum terkait untuk menggambarkan fenomena yang diintegrasikan dengan peraturan hukum. Data terkait secara detail penulis dapatkan dari buku, jurnal akademik dan peraturan perundang-undangan. Data yang telah dikumpulkan mendukung analisis untuk mengkaji terkait rekontruksi hukum kejahatan siber.

III. Hasil dan Pembahasan

1. Karakteristik Kejahatan Siber dan Implikasinya terhadap Pendekatan Hukum Pidana

Tindak pidana telah mengalami pergeseran terhadap modus operandi para pelaku kejahatan dengan tingkat yang signikan. Dahulu kejahatan dilakukan secara konvensional yang diartikan bersifat fisik, seperti pencurian, perampokan, penculikan, penipuan konvensional. Namun, kini telah berubah kebentuk virtual melalui perangkat digital.

[9] Zainuddin Ali, *Metode Penelitian Hukum.* Jakarta: Sinar Grafika, 2018. 18.

Perubahan modus operandi ini menjadi gambaran suatu fenomena bahwa ruang siber telah menjadi lahan untuk melakukan tindak pidana yang dilakukan pelaku kejahatan dengan resiko rendah namun berdampak besar. Peningkatan penggunaan internet secara khusus di Indonesia menyebabkan meningkatnnya angka kejahatan yang terjadi melalui internet[10]. Pergeseran kriminalitas dari konvensional menjadi digital yang terjadi secara jelas dapat dilihat pada bentuk kejahatan seperti pencurian identitas, manipulasi transaksi keuangan melalui sistem keuangan, penyebaran konten illegal hingga penyusupan kedalam perangkat elektronik secara illegal. UndangUndang 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[11].

Perkembangan kriminalitas dalam era digital selain terkait modus juga terkait dengan perubahan strategi dan taktik pelaku kejahtan untuk menghindari pelacakan dan jeratan hukum. Terfokus pada perbuatan dalam mencari celah pada sistem informasi untuk mendapatkan keuntungan dan mengacaukan pelayan public secara virtual tanpa pertemuan antara pelaku dengan korban dengan rekayasa social pada celah sistem teknologi[12]. Kejahatan siber yang terjadi di Indonesia telah sampai kepada tahap serangkaian serangan yang ditujukan kepada instasi pemerintahan dan lembaga public, fenomena terjebut memiliki makna

---

[10] 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," *Unknown Journal*, 2024: 2–6.

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

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

bahwa kejahatan siber telah menjadi hal yang bersifat sistematik dan lintas sektor. Meski telah memiliki UU ITE sebagai dasar pengaturan kejahatan memalui ruang digital seperti pada Pasal 32 dan 33 mengnai sanksi atas akses illegal dan gangguan pada integritas data belum dapat seutuhnya mengatasi kejahatan siber, sebeb norma yang ada masih bersifat umum dan belum menyentuh aspek teknis seperti zero-day atau penggunaan algorimat kripto yang dikategorikan sebagai media melakukan tindak pidana. Noerma yang ada masih bersifat tradisional dan belum preventif. Kejahatan siber tidaklah bisa bila diselesaikan ketika hanya saat kejahatan terjadi. Dalam menghadapi kejahat siber haruslah memiliki norma yang mengatur tindakan preventif yakni tindakan sebelum kejahatan terjadi. Oleh karenanya dibuthkan peraturan yang bersifat preventif dan adaptif dengan berbasis teknologi yang mendalam guna dapat melancarkan upaya mencegah dan menanggulangi tindak pidana pada era digital yang termasuk kepada tindak pidana modern[13].

Transformasi pada bentuk-bentuk kejahatan pada era digital turut menggeser nilai pada tatanan struktur pelaku tindak pida yang bertindak sebagai aktor. Kejahatan konvensional sering melibatkan kelompok atau pertemuan secara konvensional yaitu tatap muka namun pada kejahatan siber tidak perlu adanya pertemuan secara langsung bahkan terhadap korban juga tidak perlu bertemu secraa langsung namun tetap dapat menimbulkan kerugian bagi korban. Cyberspace yang ada juga membuat kejahatan dapat terjadi tanpa perlu mengkhawatirkan batas waktu maupun geografis dengan makna segabai awal mula masa Kriminalitas global bisa terjadi antar Negara[14]. Tidak adanya halangan geografis aaupun batasan antar Negara pada kejahatan siber merupakan ttantangan yang bertabrakan dengan norma pada Pasal 2 KHUP yang membahas mengenai Asas Terotial yang mewajibkan seluruh warga Negara tunduk kepada KUHP namun pada tindak pidana era digital dapat dilakukan oleh warga Negara dari Negara lain namun tetap memberikan dampak merugikan Negara. Indonesia memang telah

---

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

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

melakukan ratifikasi beberapa konvensi internasional mengenai kejahatan lintas batas, salah satunya United Nations Convention against Transnational Organized Crime (UNTOC). Konvensi ini menjadi beberapa hal yang digunakan dalam berbagai undang-undang yang ada di Indonesia seperti pada masalah ekstradisi, tindakan antikorupsi, narkotika, tppu dan beberapa tindak pidana lintas Negara lainya[15]. Namun, pada implementasinya belum terdapat adaptasi subtansial secara menyeluruh dan terhamonisasi dalam peraturan perundang-undangan[16]. Selain itu pada kedaan di lapangan Asas Nasional Pasif maupun Asas Nasional Aktif masih memiliki kendala dalam pengimplementasianya yang disebabkan oleh rumitnya birokrasi antar negara[17]. Oleh karena itu, dalam perhatian terhadap cakupan kriminalitas global menjadi hal yang utama dalam rekonstruksi hukum tindak pidana dengan cakupan yuridis universal berbasis kepada kepentingan dan perlindungan internasional.

Identitas pelaku yang dapat disembunyikan melalui penggunaan jaringan proxy maupun enkrispi hingga darkweb menjadi hal yang mempersulit aparat penegak hukum untuk menemukan pelaku dalam kejahatan siber. Anonimitas sebagai karakteristik yang erat dengan kejahatan siber. Pelaku dalam melakukan kejahatanya dapat menggunakan bot maupun aplikasi yang dijalankan oleh computer tanpa perlu pengoprasian oleh manusia dalam waktu yang berkelanjutan namun tetap dapat menimbulkan kerugian bagi korban atau Negara.

---

[15] Ali Masyhar et al., "Legal Challenges of Combating International Cyberterrorism: The NCB Interpol Indonesia and Global Cooperation," *Legality : Jurnal Ilmiah Hukum* vol. 31, no. 2 (November 6, 2023): 344–66. doi: https://doi.org/10.22219/ljih.v31i2.29668.

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

[17] Roby Satya Nugraha et al., "The Transformation of Indonesia's Criminal Law System: Comprehensive Comparison between the Old and New Penal Codes," *Reformasi Hukum* vol. 29, no. 1 (April 27, 2025): 11. doi: https://doi.org/10.46257/jrh.v29i1.1169.

Dinamika ini yang menjadi tantangan bagi Indonesia yang belum terfasilitasi upaya penyelesaianya[18].

Karakteristik selanjutnya dari kejahatan siber adalah lintas yuridiksi yang menjadikan kejahatan sangat kompleks untuk diselsaikan dengan norma hukum yang masih bersifat territorial. Dalam konteks Indonesia prinsip territorial telah diatur dalam Pasal 2 dan Pasal 3KUHP mengatur Asas Wilayah atau Teritorialitas yang menyebutkan bahwa hukum pidana dapat berbentuk Tindak Pidana Berbasis Teknologi Informasi atau Tindak Pidana Lainya Yang Dampaknya Dialami atau Terjadi di Wilayah NKRI yang mana asas ini mencakup kepada perbuatan tindak pidana yang di lakukan oleh WNI menggunakan teknologi informasi yang berpotensi merugikan Negara baik dilakukan di dalam maupun di luar negeri., Asas Perlindungan Nasional Pasif yang betujuan memberikan perlindungan bagi warga Negara Indoensia dari tindak pidana serta Asas Universal yaitu asas yang merujuk pada prinsip universalitas dalam hukum pidana internasional atas suatu tindak pidana kejahatan manusia dan membirikan dampak lintas negara[19]. Dalam kejahatan siber dengan sistamitak yang rumit dapat dilakukan pada negara yang berbeda yang berbeda dengan korban menybebkan hadirnya beberapa yurisdiksi yang berbeda yang memperumit proses penyelesaian perkara[20]. UU ITE mengatur secara eksplisit mengenai kerjasama international yang dilakukan melalui Mutual Legal Assistanse (MLA) namun prosedur dalam MLA cukup lambat dan tidak reponsif, sehingga tidaklah cukup untuk menangani tindak pidana modern yang terjadi

---

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

[19] Nirmal Kanti Chakrabarti and Dr. Arpita Mitra, "Universal Criminal Jurisdiction and International Cooperation as Legislative Policy to Combat Terrorism: A Comparative Study of Domestic Legislations of Different Nations," *Journal of Advanced Research in Dynamical and Control Systems* vol. 12, no. 05-SPECIAL ISSUE (May 30, 2020): 1248–53. doi: https://doi.org/10.5373/JARDCS/V12SP5/20201882.

[20] 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* vol. 45, no. 1 (2023): 1–17.

secara dinamis dan cepat. Oleh karena itu dibutuhkan perumusan baru yang menggunakan pendekatan beberapa yurisdiksi dan perjanjian antara Negara yang fleksibel antar Negara dalam pertukaran informasi dan penyidikan bersama (*joint cybercrime investigation*)[21].

Selain itu tindak pidana pada era digital memiliki kecapatan penyebaran yang sangat cepat dengan serangan yang stabil dengan menyerang banyak sistem secara bersamaan. Salah satu contoh dapat dilihat pada serangan Distributed Denial of Service (DDoS) yang melumpuhkan sistem layanan public ataupun pengiriman malware yang melumpuhkan sistem pelayanan publik. Tindak pidana yang dilakukan dengan waktu yang cepat dan luasnya ruang tindak pidana siber tidaklah bisa dihadapi dengan undang-undang yang bersifat reaktif. Pengaruran mengenai gangguan sistem informasi memang telah diatur dalam Pasal 33 UU ITE namun secara tidak eksplisit belum menyesuaikan dengan gangguan DDOS atau worms serta belum bersifat preventif guna mencegah terjadi tindak pidana. Sifat preventif seperti pendeteksi dini sistem artificial intelligience dan algoritma prediktif harus di selaraskan dengan hukum pidana agar dapat memberi manfaat maksimal pencegahan kejahatan siber[22].

Norma hukum pidana yang bersifat statis,territorial dan hierarkis tidak lagi memadai untuk mnanggapi dinamika tindak pidana pada era digital, saat ini untuk melakukan rekonstruksi hukum memerlukan perhatikan pada hukum yang dapat responsive menghadapi serangan kejahatan siber. Indonesia memiliki KUHP sebagai *lex generalis* yang mengatur asas asas pidana dan delik delik kejahatan siber terdapat dalam dengan UU ITE sebagai *lex specialis* seba dalam menghadapi kejahatan siber, keduanya saling berhubungan dan menjadikan ketentuan yang komprehensif. Terkait rekonstruksi hukum pidana yang dibutuhkan

---

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

[22] Erik Richardson Faria e Sousa, "Legal and Technical Challenges in the Pursuit of Cybercriminals: An Analysis of the Difficulties Faced by the Authorities," 2023. doi: https://doi.org/10.56238/uniknowindevolp-101.

oleh Indonesia melihat pada karakteristik kejahatan siber adalah integrasi hukum nasional mengenai siber secara sistematis dan parsial guna menjawab kejahatan siber yang bersifat kompleks diranah digital[23].

Permasalahan tindak pidana era digital tentunya tidak akan terlepas dari pondasi hukum pidana seperti asas legalitas (*nulla poena sine legi*) yang mana tiada pidana tanpa aturan pidana yang telah mengatur sebelum tindak pidana terjadi. Pengaturan norma hukum sebagai bentuk asas legalitas yang rigid adalah hal penting agar tindakan kejahatan siber telah diakui sebagai tindak pidana sehingga tidak ada pelaku kejahatan siber yang lepas dari tanggung jawab pemidanaan. Prinsip adaptive legality dalam rekonstruksi hukum pidana siber sangatlah dibutuhkan untuk menjerat berbagai tindak pidana siber karena pada prinsip ini menerapkan delik terbuka yang dapat mengakomodir perbuatan yang belum diatur dalam peraturan namun dianggap sebagai kejahatan dan dapat dipertanggungjawabkan oleh ahli maupun aparat penegak hukum, selain itu pembaharuan hukum pidana perlu mengadopsi prinsip *extraterritorial jurisdiction* yang mana prinsip ini memiliki arti untuk tetap dapat melakukan penuntutan kepada pelaku kejahatan siber yang berada diluar negeri karena yurisdiksi tidak tefokus pada batas Negara[24].

2. Perubahan Paradigma: Rekonstruksi Hukum Pidana sebagai Respons terhadap Tantangan Kejahatan Siber

Dalam kriminologi terdapat Teori anomi yang memiliki makna bila terjadi suatu perubahan dalam kondisi sosial secara cepat dan ekstrem akan menyebabkan perubahan yang signifikan terhadap kelompok masyarakat dalam jumlah bersar, perubahan tersebut akan membuat nilai atau norma yang ada akan menjadi kabur bahkan lenyap. Norma yang pengkaburan itu menyebabkan ketidakpastian hukum yang mendorong

---

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

[24] 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 ."

terjadi prilaku yang melanggar norma[25]. Dalam kejahatan siber memiliki penyebab yang berbeda pada setiap kasusnya begitupula dengan motivasi pelaku yang tidak sama. Dalam kriminologi terdapat 4 teori dalam mengkaji kejahatan siber[26]:

1. Teori Anomi dalam kejahatan siber terjadi karena tidak adanya norma dalam masyarakat, hukum yang tidak dapat mengakomodir terjadi karena adanya kesenjangan karakteristik antara kejahatan konvensional dan kejahatan siber yang mana peraturan hukum yang ada saat ini belum dapat mengakomodir karakteristik kejahatan siber[27];
2. Teori Asosiasi Diferensial menyatakan kejahatan terjadi diakibatkan pelaku telah mempelajari komunikasi dan tindakan pihak lain dalam pekerjaan yang sama;
3. Teori Kontrol Sosial menyatakan pelaku melakukan kejahatan karena ikatan sosial dalam diri melemah;
4. Teori Netralisasi adalah prilaku diri yang mulai menetralisasikan norma dan semakin lama akan melakukan penyimpangan terhadap norma.

Ketika dunia telah terintegrasi, kejahatan akan ikut terintergrasi tanpa terbatas pada yurisdiksi setiap Negara menimbulkan berbagai kejahatan kemanusiaan hingga kejahatan dunia maya[28]. Perubahan keadaan menyebabkan turut terjadi perubahan paradigma hukum pidana dalam mengahadi kejahatan siber yang bersifat dinamis. Paradigma hukum yang awalnya identik dengan sifatnya yang statistik,

---

[25] Dijk, J.J.M. Van, *Artuele Criminologie*, trans. Sumitro. Surakarta: Universitas Sebelas Maret Press, 1996.

[26] Hardianto Djanggih and Nurul Qamar, "Penerapan Teori-Teori Kriminologi Dalam Penanggulangan Kejahatan Siber (Cyber Crime)," *Pandecta: Research Law Journal* vol. 13, no. 1 (August 2, 2018): 10–23. doi: https://doi.org/10.15294/pandecta.v13i1.14020.

[27] Agus Raharjo, *Cybercrime: pemahaman dan upaya pencegahan kejahatan berteknologi*, Cetakan ke-1, tahun 2002. Bandung: Citra Aditya Bakti, 2002, 220.

[28] Mateja Čehulić, "Perspectives of Legal Culture: A Systematic Literature Review," *Revija Za Sociologiju* vol. 51, no. 2 (August 31, 2021): 257–82. doi: https://doi.org/10.5613/rzs.51.2.4.

reaktif dan menekankan pada delik materil sudah tidak dapat mengimbangi kejahatan siber. Pada beberapa kejahatan memang diterapkan delik formil dan hal ini juga berlaku kepada kejahatan siber, karena bila hanya menitik beratkan pada akibat yang ditimbulkan akibat tindak pidana maka akan semakin lama pelaku kejahatan siber akan diadili. Oleh karena itu, paradigma baru adalah hukum yang preventif dimana tidak hanya mengatur mengenai delik perbuatan namun juga upaya preventif oleh pejabat yang memiliki tugas menjaga kemaanan sistem dengan menggunakan aplikasi atau perangkat pelindung. Dalam hal ini pemerintah harus melengkapi dengan regulasi yang terang serta teknologi yang memadai[29].

Selain langkah preventif, paradigma hukum pidana modern juga harus melibatkan berbagai elemen masyarakat dalam melakukan pencegahan dan penanggulangan kejahatan siber sehingga menempatkan warga negara, institusi pendidikan, sektor swasta, hingga komunitas digital sebagai bagian dari sistem pertahanan 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 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. Adanya kolaborasi antara aparat penegak hukum dengan bergbagai elemen masyarakat diharapkan dapat meningkatkan kepercayaan publik terhadap kasus-kasus kontroversial dibidang ITE[30].

Paradigma hukum pidana modern juga menuntut reformulasi terhadap tujuan pemidanaan itu sendiri. Sebagai contoh apabila suatu

---

[29] Soetardi Tri Cahyono, Wina Erni, and Taufik Hidayat, "Reconstruction of Criminal Law Against Cybercrime in The Indonesian Criminal Justice System: Rekonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cyber Crime) Dalam Sistem Peradilan Pidana Indonesia," *Dame Journal of Law* vol. 1, no. 1 (n.d.): 8.

[30] 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 ."

kejahatan siber dilakukan oleh oleh pelaku non-profesional atau dilakukan tanpa adanya motif ekonomi, maka pembalasan tidak selalu efektif untuk memberikan efek jera terhadap pelaku kejahatan siber sehingga pemidanaan harus difokuskan pada pemulihan kerugian korban serta jaminan agar pelaku tidak melakukan pengulangan[31]. Ujaran kebencian dan penyeberan berita bohong di dunia maya, misalnya dapat dilakukan pendekatan rehabilitasi dan edukasi dibanding dengan pemenjaraan sehingga sistem hukum dapat menjadi lebih humanis dan efektif.

Bertolak dari kebutuhan zaman di era digital, rekonstruksi hukum pidana baik secara teoritis maupun normatif dalam konteks kejahatan siber dalam hal perubahan atau amandemen terhadap norma-norma yang sudah ada merupakan sebuah pendekatan progresif, maka rekonstruksi hukum pidana digital khususnya kejahatan siber harus diawali dari pemahaman bahwa kejahatan siber memiliki karakteristik tersendiri yang tidak dijawab oleh pendekatan hukum konvensional yang represif dan terfragmentasi[32].

Pembaharuan hukum pidana dalam hal ini menjadi sangat penting dengan terjadinya berbagai kejahatan di dunia digital yang semakin kompleks baik dari modus operandinya yang makin beragam, dapat dilakukan secara lintas yurisdiksi, dan dapat mengancam stabilitas negara hingga integritas sistem demokrasi. Kitab Undang-Undang Hukum Pidana (KUHP) dan UndangUndang Informasi dan Transaksi Elektronik (UU ITE) belum mampu untuk mengakomodir kejahatan siber karena kedua peraturan tersebut lahir dari paradigma pra-digital, sehingga tidak memadai untuk menjawab tantangan zaman digital yang

---

[31] Azam and others, "Cybercrime Unmasked: Investigating Cases and Digital Evidence."

[32] Saifullah and others, "The Evaluation of the Indonesian Fintech Law From the Perspective of Regulatory Technology Paradigms To Mitigate Illegal Fintech," *Jurisdictie: Jurnal Hukum Dan Syariah* 14 (2023). doi: https://doi.org/10.18860/j.v14i2.24025.

disruptif sehingga dinilai masih memiliki banyak celah atau kekosongan normatif [33].

Rekonstruksi hukum dalam ranah digital meliputi tiga aspek krusial: rekonseptualisasi delik digital, pembaruan struktur norma pidana, dan adaptasi prinsip hukum pidana dalam konteks siber. Secara konseptual, esensial untuk mendefinisikan ulang kejahatan siber agar mampu mengakomodasi modus operandi baru seperti manipulasi algoritma, deepfake, pencurian data biometrik, dan pemanfaatan kecerdasan buatan untuk tujuan kriminal. Reformulasi norma-norma pidana juga mesti mematuhi prinsip *lex certa* (kepastian hukum) dan *lex scripta* (hukum tertulis) demi mencegah ambiguitas hukum dan pelanggaran prinsip non-retroaktif. Lebih lanjut, pendekatan normatif dalam rekonstruksi hukum pidana digital wajib mempertimbangkan 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. Dengan demikian, paradigma rekonstruksi harus bersifat responsif, inklusif, dan berlandaskan keadilan. Hal ini menuntut partisipasi beragam pemangku kepentingan, termasuk akademisi, praktisi hukum, lembaga negara, dan masyarakat sipil, dalam proses legislasi serta perumusan kebijakan.

Dengan demikian, rekonstruksi hukum pidana sebagai respons terhadap kejahatan siber mesti dilakukan secara holistik, bukan parsial[34]. Ini menuntut pendekatan sistemik yang mengintegrasikan pembaruan substansi hukum, penguatan struktur penegakan hukum, serta internalisasi nilai-nilai keadilan dan konstitusionalitas. Dalam konteks ini, rekonstruksi hukum pidana tidak sekadar dimaknai sebagai pembaruan teknis, melainkan sebagai upaya transformatif untuk

---

[33] 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* vol. 7, no. 2 (2023): 614. doi: https://doi.org/10.33087/wjh.v7i2.1244.

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

membangun sistem hukum yang adaptif, adil, dan berkelanjutan di tengah tantangan era digital.

Modernisasi hukum ke arah yang tanggap terhadap dinamika zaman agar terciptanya ruang aman bagi warga negara di ruang digital merupakan hak konstitusional mereka. Pembaharuan terhadap UU ITE terhadap beberapa Pasal yang menimbulkan multi tafsir dan implementasi yang tidak proporsional[35], seperti dalam Pasal 27 ayat (3) dan Pasal 28 ayat (2) tentang pencemaran nama baik dan ujaran kebencian. Meskipun revisi Revisi KUHP yang tertuang dalam Undang-Undang Nomor 1 Tahun 2023 telah memperkenalkan beberapa ketentuan baru mengenai kejahatan siber, akan tetapi peraturan belum mengatur secara khusus terkait kejahatan siber sehingga reformulasi tersebut perlu diarahkan kepada penyusunan undang-undang khusus yang berfungsi sebagai Cyber Penal Code, sebagai lex specialis dalam menanggulangi kejahatan dunia maya[36]. Konvensi Budapest tentang Cybercrime 2001 dapat dijadikan rujukan untuk menyusun rancangan tersebut, terutama dalam pengaturan terkait illegal access, data interference, dan system interference yang masih lemah dalam legislasi nasional.

Pendekatan risk-based regulation dapat menjadi langkah strategis lain dalam kerangka legislasi pidana sehingga hukum hadir sebelum terjadinya kejahatan dan dapat merespon maupun mengidentifikasi kejahatan digital secara preventif. Oleh karena itu, prinsip kehati-hatian dan perlindungan data pribadi yang tertuang seperti dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) pada Pasal 65-73 harus diintegrasikan secara lebih efektif ke dalam sistem pemidanaan. Meskipun UU PDP sudah mengatur sanksi pidana

---

[35] 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* vol. 2, no. 1 (2024): 1–8. doi: https://doi.org/10.61306/ijsl.v2i1.68.

[36] 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. doi: https://doi.org/10.35707/dostresmil/25385.

untuk penyalahgunaan data, akan tetapi tidak koordinasi dengan hukum pidana umum yang masih belum optimal[37].

Selain itu, legislasi harus memastikan sinkronisasi antara hukum pidana dengan regulasi administratif, perdata, dan konstitusional. Banyak pelanggaran siber bersifat lintas domain hukum seperti, kebocoran data atau manipulasi algoritma yang memengaruhi hak ekonomi, kebebasan sipil, dan integritas digital masyarakat. Maka, substansi hukum pidana perlu diperbarui menuju sistem hukum yang interdisipliner untuk menghadapi realitas digital yang kompleks. Pasal 28G ayat (1) dan Pasal 28H ayat (4) UUD 1945, yang menjamin hak atas rasa aman dan perlindungan data pribadi, menjadi fondasi hukum normatif yang tak tergantikan[38].

Bahwa reformulasi norma pidana harus menjunjung tinggi *prinsip legal clarity, necessity, dan proportionality* sebagaimana dijamin oleh UUD 1945 Pasal 28J ayat (2) dan Pasal 19 ayat (3) Kovenan Internasional tentang Hak Sipil dan Politik (ICCPR). Hukum pidana tidak boleh menjadi instrumen represif yang melanggar kebebasan berekspresi, sebaliknya harus menjadi alat pelindung keadilan, kebenaran, dan integritas digital dalam masyarakat[39].

Dengan dari berbagai regulasi, serta dengan keberanian politik dan visi keadilan digital yang progresif, maka arah dan strategi

---

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

[38] 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* vol. 28, no. 1 (2024): 196–214. doi: https://doi.org/10.22363/2313-2337-2024-28-1-196-214.

[39] 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," *Unknown Journal*, 2024, 269–97. doi: https://doi.org/10.25110/rcjs.v27i1.2024-11341.

pembaruan substansi hukum pidana dapat mewujudkan sistem restoratif dan transformatif. Pembaharuan yang konkret merupakan tanggung jawab negara dalam memberikan jaminan hukum atas kehidupan digital yang adil, aman, dan beradab di era digital.

Kompleksitas dalam pengakkan hukum kejahatan siber seperti teknis, kelembagaan dan koordinasi antar intansi tidak mampu diakomodir oleh paradigma hukum yang konvensional sehingga diperlukan pembaharuan secara menyeluruh terhadap prosedur, struktur dan teknologi guna menjawab tantangan dan dinamika kejahatan digital yang semakin canggih dan dinamis. Pembentukan unit khusus *cyber crime* dakam tubuh aparat penegak hukum seperti, kepolisian, kejaksaan dan lembaga peradilan dengan penguatan di bagian digital forensik sebagai fondasi penguatan yang utama dan bekerja dengan standar interoperabilitas data, kecepatan penanganan, serta akurasi bukti digital.

Angin segar hadir dalam proses pengadilan di Indonesia melalui Peraturan Mahkamah Agung Nomor 1 tahun 2019 Tentang Adminstrasi Perkara dan Persidangan di Pengadilan secara elektronik mengggunakan implementasi *electronic evidence* (e-evidence) menjadi krusial pada proses peradilan. Dalam proses pengadilan penting adanya pembentukan regulasi yang berisikan khusus atas tata cara pengumpulan, autentifikasi, penyimpanan dan presentasi alat bukti digital sebagai alat bukti dalam persidangan dalam keadaan mendesak, hal ini selaras dengan Pasal 5 UU ITE yang menjelaskan bahwa alat bukti elektronik dapat digunakan sebagai alat bukti yang sah dalam persidangan. Namun, dalam praktiknya belum semua apparat penegak hukum memahami secara mendalam mengenai mekanisme *chain of custody* dan validitas forensik digital dalam pengaplikasian pada proses pembuktian[40].

[40] 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* vol. 6, no. 3 (2022): 172–85. doi: https://doi.org/10.52468/2542-1514.2022.6(3).172-185.

Langkah selanjutnya yang harus diaplikasikan dalam proses pengadilan perkara kejahatan siber adalah menggunakan teknologi yang sama seperti para pelaku sepertinya salah satunya adalah penggunaan teknologi kecerdasan buatan seperti *AI-assisted justice*. Penggunaan teknologi kecerdasan buatan dalam proses adjudikasi dapat mendukung percepatan penyesaian kasus bila dimanfaatkan dengan benar karena dapat memberikan bantuan analisis pola kejahatan dan meningkatkan akurasi pengambilan Keputusan. Mekanisme ini telah diadaptasi oleh beberapa negara seperti china yang menggunakan 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[41].

Sinergi antar Lembaga juga menjadi Langkah selanjutnya dalam rekonstruksi system penegakan hukum termasuk Badan Siber dan Sandi Negara (BSSN), Kementerian Komunikasi dan Informatika (Kominfo), serta lembaga perlindungan data seperti Komisi Informasi dan Komnas HAM. Pembagiaan koordinsai yang jelas, kewenangan, pembagian tugas tanpa tindih melalui regulasi sistematis yang terang dan penggunaan palform terpadu dalam Upaya pelaporan dan pelacakan pelaku kejahatan siber akan membentuk sinergi antar Lembaga yang kuat dan terorgansiri. 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[42].

Amanat konstitusi melalui Pasal 28D ayat (1) UUD 1945 menegaskan bahwa setiap orang berhak atas pengakuan, jaminan,

---

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

[42] 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. doi: https://doi.org/10.32782/2524-0374/2023-2/116.

perlindungan dan kepastian hukum yang adil serta perlakuan yang sama di hadapan hukum. Oleh Karena itu rekonstruksi hukum dalam penegakan hukum menghadapi kejahat siber haruslah memiliki prinsip keadilan substansi dengan makna bahwa proses hukum tidak boleh menjadi alat represi yang melanggar hak warga negara, tetapi harus menjamin adanya perlindungan, kepastian, dan keadilan. Hal ini juga mengartikan bahwa seusia dengan konstitusi bhawa system rekonstruksi digunakan sebagai bukti untuk menciptakan perlindungan dan mengembalikan kepercayaan public terhadap Lembaga hukum terutama dalam proses penanganan kejahatan siber yang bersifat kompleks dan sensitif[43].

Negara perlu melakukan pengembangan danmerusmuskan regulasi yang strategis dan dapat beradaptasi selama jangka waktu yang Panjang, karena dalam menyikapi kompleksitas dan dinamika kejahatan siber yang terus berkembang dari waktu ke waktu. Regulasi jangka Panjang adalah hal yang penting karena tidak hanya bersifat reaktif namun juga dapat bersifat adaptif, inklusif fan antisipatif terhadapperkembangan teknologi. Syogyanya dalam reformasi hukum tidak hanya terfokus kepada subtansi hukum namun juga perhatian pada tata Kelola, reformasi kelembagaan hingga penguatan kesadaran digital masyarakat[44].

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

---

[43] Hui Li and others, "A Technical Solution for the Rule of Law, Peace, Security, and Evolvability of Global Cyberspace – Solve the Three Genetic Defects of IP Network," 2024.

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

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[45].

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[46].

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)[47].

Pada aspek kelembagaan, penting untuk dibentuk unit khusus penegakan hukum siber di setiap tingkatan penegak hukum, mulai dari

---

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

[46] Thing and Lim.

[47] 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," n.d.

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)[48]. 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[49].

Akhirnya, dalam mengawal keseluruhan proses rekonstruksi hukum pidana digital, diperlukan kebijakan pendidikan literasi digital dan etika hukum siber bagi masyarakat luas, 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[50]. 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.

---

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

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

[50] 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* vol. 7, no. 1 (2023): 95–103. doi: https://doi.org/10.28926/jdr.v7i1.278.

IV. Kesimpulan

Perubahan paradigma hukum pidana terhadap kejahatan siber dipengaruhi oleh karakteristik kejahatan siber yang berbeda dari kejahatan konvensional yakni bersifat cepat dan dinamis, sehingga paradigma hukum pidana yang baru haruslah bersifat responsif dan preventif. Dalam mewujudkan hukum pidana yang preventif, pemerintah perlu memfasilitasi teknologi yang memadi dan sumber daya manusia yang memahami lebih mendalam tentang teknologi seperti proxy, script dan perangkat keamanan dalam sistem untuk senantiasa menjadi pehalang terjadinya serangan siber. Selain terhadap teknologi, pemerintah juga dapat mengajak masyarakat untuk menjadi pengawas kejahatan siber dalam dunia maya maupun sistem pelayanan publik dengan sebelumnya memberikan edukasi mengenai hukum dan kejahatan siber.

Kejahatan siber dapat terjadi antar lintas yurisdiksi, oleh karena itu pemerintah perlu melakukan rekonstruksi hukum yang meningkatkan hubungan bilateral antar negara dan percepetan proses perkara antara negara seperti penyidikan bersama guna mempercepat proses penanganan perkara. Regulasi yang dibuat juga harus bersifat terbuka namun tetap terfokus pada kerugian yang timbul akibat tindak pidana di era digital. Pelaku kejahatan siber juga harus diberikan sanksi yang membuatnya jera tidak hanya berfokus kepada penjara maupun ganti rugi.

Daftar Pustaka

Ali, Zainuddin. *Metode Penelitian Hukum*. Jakarta: Sinar Grafika, 2018.

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

Anastasya, Vannya and others. "Efektivitas Hukum Dan Kebijakan Publik Dalam Menghadapi Ancaman Siber Terhadap Keamanan Negara." *Unknown Journal*, no. 2 (2024): 1710–16.

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

Arief, Barda Nawawi. *Tindak pidana mayantara: perkembangan kajian cyber crime di Indonesia*. Jakarta: RajaGrafindo Persada, 2006.

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

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

Cahyono, Soetardi Tri, Wina Erni, and Taufik Hidayat. "Reconstruction of Criminal Law Against Cybercrime in The Indonesian Criminal Justice System: Rekonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cyber Crime) Dalam Sistem Peradilan Pidana Indonesia." *Dame Journal of Law* vol. 1, no. 1 (n.d.): 1–23.

Čehulić, Mateja. "Perspectives of Legal Culture: A Systematic Literature Review." *Revija Za Sociologiju* vol. 51, no. 2 (August 31, 2021): 257–82. doi: https://doi.org/10.5613/rzs.51.2.4.

Chakrabarti, Nirmal Kanti, and Dr. Arpita Mitra. "Universal Criminal Jurisdiction and International Cooperation as Legislative Policy to Combat Terrorism: A Comparative Study of Domestic Legislations of Different Nations." *Journal of Advanced Research in Dynamical and Control Systems* vol. 12, no. 05-SPECIAL ISSUE (May 30, 2020): 1248–53. doi: https://doi.org/10.5373/JARDCS/V12SP5/20201882.

Delerue, François, and Monica Kaminska. "Governing Cyber Crises: Policy Lessons from a Comparative Analysis." *Policy Design and*

Practice vol. 6, no. 2 (2023): 127–30. doi: https://doi.org/10.1080/25741292.2023.2213061.

Dijk, J.J.M. Van. *Artuele Criminologie*. Translated by Sumitro. Surakarta: Universitas Sebelas Maret Press, 1996.

Diyah Ayu Anggraini, Putri, Aqhina Aurora Dzikrah, Aprilia Niravita, Muhammad Adymas Hikal Fikri, and Harry Nugroho. "Electronic Certificates in Indonesia: Enhancing Legal Certainty or Introducing New Challenges?" *Arkus* vol. 11, no. 1 (November 12, 2024): 686–98. doi: https://doi.org/10.37275/arkus.v11i1.659.

Djanggih, Hardianto, and Nurul Qamar. "Penerapan Teori-Teori Kriminologi Dalam Penanggulangan Kejahatan Siber (Cyber Crime)." *Pandecta: Research Law Journal* vol. 13, no. 1 (August 2, 2018): 10–23. doi: https://doi.org/10.15294/pandecta.v13i1.14020.

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

Li, Hui and others. "A Technical Solution for the Rule of Law, Peace, Security, and Evolvability of Global Cyberspace – Solve the Three Genetic Defects of IP Network," 2024.

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

Makarim, Edmon. *Kompilasi hukum telematika*. Cet. 1. Jakarta: Divisi Buku Perguruan Tinggi, RajaGrafindo Persada, 2003.

Masyhar, Ali, Indah Sri Utari, Usman Usman, and Ahmad Zaharuddin Sani Ahmad Sabri. "Legal Challenges of Combating International Cyberterrorism: The NCB Interpol Indonesia and Global Cooperation." *Legality : Jurnal Ilmiah Hukum* vol. 31, no. 2

(November 6, 2023): 344–66. doi: https://doi.org/10.22219/ljih.v31i2.29668.

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* vol. 6, no. 3 (2022): 172–85. doi: https://doi.org/10.52468/2542-1514.2022.6(3).172-185.

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

Nugraha, Roby Satya, Edi Rohaedi, Nandang Kusnadi, and Abid Abid. "The Transformation of Indonesia's Criminal Law System: Comprehensive Comparison between the Old and New Penal Codes." *Reformasi Hukum* vol. 29, no. 1 (April 27, 2025): 1–21. doi: https://doi.org/10.46257/jrh.v29i1.1169.

Nurkhasanah, Kharisma Ika, and Zydane Maheswara Prasetyo. "Law Enforcement of State Jurisdiction in Hacking Crimes." *Indonesian Journal of Applied and Industrial Sciences (ESA)* vol. 3, no. 3 (May 31, 2024): 319–28. doi: 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* vol. 6, no. 4 (2024): 2089–98. doi: https://doi.org/10.47476/reslaj.v6i4.2067.

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* vol. 45, no. 1 (2023): 1–17.

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. doi: https://doi.org/10.32782/2524-0374/2023-2/116.

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

Raharjo, Agus. *Cybercrime: pemahaman dan upaya pencegahan kejahatan berteknologi*. Cetakan ke-1, Tahun 2002. Bandung: Citra Aditya Bakti, 2002.

Ramli, Ahmad M. *Cyber law & HAKI: dalam sistem hukum Indonesia*. Cetakan ketiga. Bandung: Refika Aditama, 2010.

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. doi: https://doi.org/10.35707/dostresmil/25385.

Saifullah and others. "The Evaluation of the Indonesian Fintech Law From the Perspective of Regulatory Technology Paradigms To Mitigate Illegal Fintech." *Jurisdictie: Jurnal Hukum Dan Syariah* 14 (2023). doi: https://doi.org/10.18860/j.v14i2.24025.

Sallapalli, Nihitha. "Digital Transformation: Reshaping Industries Through Technology." *International Journal For Multidisciplinary Research* vol. 6, no. 6 (November 27, 2024): 31446. doi: https://doi.org/10.36948/ijfmr.2024.v06i06.31446.

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

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.

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 vol. 7, no. 2 (2023): 614. doi: 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." *Unknown Journal*, 2024, 269–97. doi: 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* vol. 28, no. 1 (2024): 196–214. doi: 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," 2023. doi: https://doi.org/10.56238/uniknowindevolp-101.

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

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* vol. 7, no. 1 (2023): 95–103. doi: https://doi.org/10.28926/jdr.v7i1.278.

Temara, Sheetal. "The Dark Web and Cybercrime : Identifying Threats and Anticipating Emerging Trends." *Unknown Journal*, no. 10 (2024): 80–93.

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

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." *Unknown Journal*, 2024, 2–6.

Widodo, W. *Sistem Pemidanaan Dalam Cyber Crime*. Aswaja Pressindo, 2021.