

Politik Hukum Siber dalam Mewujudkan Keamanan Ruang Digital Nasional

Laely Wulandari ¹

¹Fakultas Hukum, Ilmu Sosial, dan Ilmu Politik Universitas Mataram, Indonesia

Email: laelywulandari01@gmail.com ¹

Abstrak

Penelitian ini bertujuan: (1) menganalisis arah dan konstruksi politik hukum siber di Indonesia dalam mewujudkan keamanan ruang digital nasional, dan (2) serta menilai kebijakan hukum siber yang ada dalam memberikan perlindungan hukum terhadap ancaman siber yang berkembang. Penelitian ini merupakan penelitian hukum normatif dengan pendekatan perundang-undangan, konseptual, dan analitis. Bahan hukum penelitian diperoleh dari bahan hukum primer, sekunder, dan tersier. Analisis dilakukan dengan menggunakan teori-teori hukum, asas-asas hukum, serta interpretasi hukum berupa interpretasi gramatikal, sistematis, dan teleologis. Seluruh bahan hukum diolah dengan penalaran hukum (legal reasoning) yang runut dan sistematis, dan penarikan kesimpulan dilakukan secara deduktif. Hasil penelitian menunjukkan bahwa arah politik hukum siber menekankan peran negara dalam mengatur, melindungi, dan mengamankan ruang digital nasional, dengan fokus pada keamanan sistem elektronik, perlindungan data, dan kepastian hukum. Regulasi yang ada telah membentuk kerangka perlindungan hukum normatif, tetapi penguatan harmonisasi antar perundang-undangan, keseragaman penafsiran, dan koordinasi kelembagaan tetap diperlukan agar perlindungan hukum dapat berfungsi secara optimal menghadapi dinamika ancaman siber.

Kata Kunci: Keamanan; Ruang Digital; Nasional; Politik Hukum; Siber.

Abstract

This study aims to: (1) analyze the direction and construction of cyber legal policy in Indonesia in realizing national digital space security, and (2) assess existing cyber legal policies in providing legal protection against developing cyber threats. This research is a normative legal research with a statutory, conceptual, and analytical approach. The legal material for this research is obtained from primary, secondary, and tertiary legal materials. The analysis is conducted using legal theories, legal principles, and legal interpretations in the form of grammatical, systematic, and teleological interpretations. All legal materials are processed using legal reasoning that is coherent and systematic, and conclusions are drawn deductively. The results of the study indicate that the direction of cyber legal policy emphasizes the role of the state in regulating, protecting, and securing the national digital space, with a focus on electronic system security, data protection, and legal certainty. Existing regulations have formed a normative legal protection framework, but strengthening harmonization between laws, uniformity of interpretation, and institutional coordination are still needed so that legal protection can function optimally in facing the dynamics of cyber threats.

Keywords: Security; Digital Space; National; Legal Politics; Cyber



RETORIKA: *Journal of Law, Social, and Humanities* is licensed under a [Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/).

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mengubah pola interaksi sosial, ekonomi, dan pemerintahan ke dalam ruang digital yang semakin kompleks. Transformasi digital mendorong peningkatan penggunaan sistem elektronik dalam transaksi bisnis, pelayanan publik, hingga aktivitas politik. Namun, di balik kemajuan tersebut, muncul berbagai ancaman siber seperti peretasan, pencurian data pribadi, penyebaran disinformasi, serta serangan terhadap infrastruktur digital strategis. Kondisi ini menunjukkan bahwa keamanan ruang digital nasional bukan hanya persoalan teknis, melainkan juga persoalan kebijakan hukum yang memerlukan perumusan politik hukum yang tepat, terarah, dan adaptif terhadap dinamika global.¹

Situasi tersebut menempatkan negara pada posisi yang menuntut peran aktif dalam membangun kerangka pengaturan yang mampu mengantisipasi risiko sekaligus menjamin perlindungan hak para pengguna ruang digital. Tanpa desain kebijakan hukum yang jelas, perkembangan teknologi berpotensi menimbulkan kekosongan norma, tumpang tindih pengaturan, serta ketidakpastian tanggung jawab ketika terjadi pelanggaran. Oleh karena itu, politik hukum siber diperlukan sebagai arah kebijakan dasar yang menentukan prioritas pengaturan, model perlindungan, serta batas kewenangan negara dalam mengelola dan mengamankan ruang digital. Keberadaan politik hukum yang terstruktur juga berfungsi sebagai pedoman dalam pembentukan dan penafsiran peraturan perundang-undangan di bidang siber agar tetap konsisten, terkoordinasi, dan responsif terhadap perkembangan ancaman yang terus berubah.²

Sebagai negara hukum, Indonesia telah membentuk berbagai regulasi untuk mengatur ruang siber, antara lain melalui UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, UU No. 1 Tahun 2024 tentang Perubahan Kedua atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, serta UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi.

¹ Muhammad Alfi, Ni Putu Yundari, and Ahnaf Tsaqif, "Analisis Risiko Keamanan Siber Dalam Transformasi Digital Pelayanan Publik Di Indonesia," *Jurnal Kajian Stratejik Ketahanan Nasional* 6, no. 2 (2023): 5.

² Dian Indriyani, "Peran Regulasi Digital Dalam Perlindungan Hak Masyarakat Modern," *Jurnal Kajian Hukum* 1, no. 1 (2025): 24–29.

Meskipun demikian, perkembangan ancaman siber yang semakin kompleks menuntut evaluasi terhadap arah politik hukum siber nasional, khususnya dalam memastikan perlindungan hukum terhadap keamanan ruang digital dan kepastian hukum bagi masyarakat.

Kerangka regulasi yang ada menunjukkan bahwa negara telah menempatkan perlindungan sistem elektronik dan data pribadi sebagai bagian integral dari kebijakan hukum siber. UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, UU No. 1 Tahun 2024 tentang Perubahan Kedua atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatur larangan akses tanpa hak, manipulasi data, serta kewajiban menjaga integritas sistem elektronik, sedangkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menegaskan hak subjek data, kewajiban pengendali data, serta mekanisme sanksi bagi pelanggaran. Keterpaduan norma-norma ini membentuk fondasi hukum yang memungkinkan negara memberikan jaminan kepastian hukum, perlindungan hak, dan tanggung jawab para pihak yang terlibat dalam ruang digital. Namun, kompleksitas ancaman siber termasuk peretasan, kebocoran data, dan penyalahgunaan informasi menuntut agar regulasi tersebut dibaca secara terpadu, konsisten, dan diimplementasikan dengan koordinasi kelembagaan yang baik, sehingga perlindungan hukum tidak hanya bersifat deklaratif, tetapi benar-benar dapat menjamin keamanan dan stabilitas ruang digital nasional.³

Perkembangan ancaman siber yang semakin kompleks menuntut kajian mendalam terhadap kebijakan hukum siber di Indonesia, terutama terkait kemampuan regulasi untuk memberikan perlindungan hukum yang memadai. Meskipun berbagai peraturan telah diterapkan, termasuk UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, UU No. 1 Tahun 2024 tentang Perubahan Kedua atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan UU No. 27

³ Fadhila Rahman Najwa, "Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber Di Indonesia," *AL-BAHTS: Jurnal Ilmu Sosial, Politik, Dan Hukum* 1, no. 2 (2024): 8–16, <https://doi.org/https://doi.org/10.32520/albahts.v2i1.3044>.

Tahun 2022 tentang Perlindungan Data Pribadi UU PDP, risiko seperti peretasan, kebocoran data, dan penyalahgunaan informasi menimbulkan tantangan dalam penegakan hukum dan kepastian tanggung jawab. Kondisi ini menekankan perlunya analisis terhadap konstruksi politik hukum siber dan bentuk perlindungan hukum yang ada, agar tercipta kerangka regulasi yang selaras, terkoordinasi, dan mampu menjamin keamanan ruang digital nasional, perlindungan hak subjek hukum, serta kepastian hukum di era transformasi digital.⁴

Berdasarkan latar belakang tersebut, permasalahan dalam penelitian ini adalah: (1) bagaimana arah dan konstruksi politik hukum siber di Indonesia dalam mewujudkan keamanan ruang digital nasional; dan (2) Apakah kebijakan hukum siber yang berlaku telah memberikan perlindungan hukum yang memadai terhadap ancaman siber yang berkembang. Adapun tujuan penelitian ini adalah: (1) menganalisis arah politik hukum siber dalam sistem hukum nasional; dan (2) menilai kebijakan hukum siber yang berlaku dalam memberikan perlindungan hukum terhadap ancaman siber yang berkembang.

Landasan teori hukum yang digunakan dalam penelitian ini bertumpu pada teori politik hukum dan teori perlindungan hukum dalam kerangka negara hukum. Teori politik hukum digunakan untuk menganalisis arah, pilihan kebijakan, serta strategi pembentukan dan pengembangan regulasi di bidang siber sebagai bagian dari desain hukum nasional, sehingga dapat menjelaskan bagaimana negara menentukan prioritas pengaturan keamanan ruang digital. Melalui teori ini, regulasi siber dipahami bukan sekadar norma teknis, melainkan hasil keputusan kebijakan yang mencerminkan tujuan perlindungan kepentingan publik dan kedaulatan digital.⁵

Selain itu, teori perlindungan hukum digunakan untuk menilai kemampuan perangkat hukum yang ada dalam memberikan jaminan keamanan, kepastian, dan keadilan bagi seluruh subjek hukum di ruang digital, termasuk individu, pelaku usaha, maupun institusi negara. Hal ini menekankan bahwa hukum tidak hanya berfungsi

⁴ Rivan Hasan Laita, "Kritik Terhadap Lemahnya Penegakan Hukum Dalam Kasus Cybercrime Peretasan Platform Kripto Indodax 2024," *Juris Studia: Jurnal Kajian Hukum* 6, no. 2 (2025): 218–28, <https://doi.org/https://doi.org/10.55357/is.v6i2.888>.

⁵ Soetardi Tri Cahyono, Wina Erni, and Taufik Hidayat, "Rekonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cyber Crime) Dalam Sistem Peradilan Pidana Indonesia: Rekonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cyber Crime) Dalam Sistem Peradilan Pidana Indonesia," *Dame Journal of Law* 1, no. 1 (2025): 111–33, <https://doi.org/https://doi.org/10.64344/djl.v1i1.6>.

sebagai aturan formal, tetapi juga sebagai instrumen perlindungan yang memastikan hak dan kewajiban setiap pihak dijalankan secara adil, serta risiko pelanggaran dapat diminimalkan melalui norma yang jelas dan mekanisme pertanggungjawaban yang tegas.⁶

Kebaruan penelitian ini terletak pada analisis yang mengintegrasikan konstruksi politik hukum siber dengan perlindungan hukum terhadap ancaman digital dalam satu kerangka pembahasan yang utuh. Kajian ini tidak hanya menguraikan ketentuan normatif dalam UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, UU No. 1 Tahun 2024 tentang Perubahan Kedua atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, serta UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadisecara terpisah, tetapi menempatkannya sebagai satu kesatuan sistem pengaturan hukum siber nasional. Dengan demikian, pembahasan menitikberatkan pada keterkaitan arah kebijakan hukum, struktur norma perlindungan, serta jaminan hak subjek hukum di ruang digital. Kontribusi utama kajian ini terletak pada perumusan gambaran yang lebih terpadu mengenai hubungan antara politik hukum siber dan perlindungan hukum, sehingga memberikan nilai tambah dalam pengembangan diskursus hukum siber nasional.

METODE

Metode penelitian yang digunakan dalam penelitian ini adalah penelitian hukum normatif, yaitu penelitian yang berfokus pada kajian terhadap norma, asas, dan sistem pengaturan hukum yang berkaitan dengan politik hukum siber dalam mewujudkan keamanan ruang digital nasional. Pendekatan penelitian yang digunakan meliputi pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan analitis (*analytical approach*), yang dilakukan dengan menelaah ketentuan regulasi, konsep politik hukum, serta konstruksi norma yang mengatur ruang siber dan keamanan digital.

⁶ Abd Syakur, "REKONSTRUKSI PERLINDUNGAN HUKUM KONSUMEN DALAM TRANSAKSI E-COMMERCE MELALUI KEBIJAKAN PEMERINTAH UNTUK Mendukung Ekonomi Digital Yang Berkeadilan" (UNIVERSITAS ISLAM SULTAN AGUNG, 2022).

Bahan hukum diperoleh dari tiga jenis sumber, yaitu bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Bahan hukum primer yang digunakan meliputi peraturan perundang-undangan yang berkaitan dengan ruang siber dan keamanan digital, antara lain Undang-Undang tentang Informasi dan Transaksi Elektronik beserta perubahannya, Undang-Undang tentang Perlindungan Data Pribadi, serta peraturan pelaksana dan regulasi terkait sistem dan keamanan elektronik. Bahan hukum sekunder terdiri dari buku, jurnal ilmiah, dan karya akademik di bidang hukum siber dan politik hukum, sedangkan bahan hukum tersier berupa kamus hukum dan ensiklopedia hukum.

Teknik analisis bahan hukum dilakukan melalui interpretasi gramatikal, interpretasi sistematis, dan interpretasi teleologis. Analisis juga menggunakan teori hukum dan asas-asas hukum yang relevan. Seluruh bahan hukum diolah dengan penalaran hukum (legal reasoning) yang runut dan sistematis, dan penarikan kesimpulan dilakukan secara deduktif.

HASIL DAN PEMBAHASAN

Arah dan Konstruksi Politik Hukum Siber di Indonesia dalam Mewujudkan Keamanan Ruang Digital Nasional

Pembahasan mengenai politik hukum siber tidak dapat dilepaskan dari perubahan karakter ruang interaksi masyarakat yang semakin bergeser ke ranah digital. Perkembangan teknologi informasi telah melahirkan bentuk aktivitas hukum baru, objek perlindungan baru, serta risiko pelanggaran yang berbeda dari ruang konvensional. Oleh karena itu, diperlukan kerangka kebijakan hukum yang mampu mengarahkan pembentukan norma, kelembagaan, dan mekanisme pengawasan secara terstruktur agar tata kelola ruang digital tetap berada dalam koridor negara hukum.

Arah dan konstruksi politik hukum siber di Indonesia menunjukkan bahwa negara menempatkan ruang digital sebagai wilayah strategis yang memerlukan pengaturan khusus demi menjamin keamanan dan kepastian hukum. Berdasarkan teori politik hukum, pembentukan regulasi siber merupakan wujud pilihan kebijakan negara dalam merespons perkembangan teknologi serta risiko kejahatan digital. Politik hukum tidak

hanya menentukan isi norma, tetapi juga orientasi perlindungan kepentingan umum dan stabilitas sistem digital nasional.⁷

Penempatan ruang digital sebagai wilayah strategis tercermin dari intensitas pembentukan regulasi dan penguatan kelembagaan yang berkaitan dengan tata kelola sistem elektronik, perlindungan data, serta penanggulangan kejahatan siber. Negara tidak lagi memandang ruang digital sekadar sebagai sarana komunikasi, tetapi sebagai bagian dari infrastruktur nasional yang berkaitan langsung dengan kepentingan ekonomi, keamanan, dan kedaulatan. Setiap perkembangan aktivitas masyarakat yang menimbulkan konsekuensi hukum harus direspons melalui pengaturan yang memberikan kepastian dan perlindungan. Oleh karena itu, konstruksi politik hukum siber diarahkan pada pembentukan norma yang mampu menjaga keseimbangan antara kebebasan pemanfaatan teknologi dan kewajiban untuk mencegah penyalahgunaan. Dengan demikian, regulasi siber menjadi instrumen strategis yang tidak hanya bersifat represif terhadap pelanggaran, tetapi juga preventif dalam membangun sistem keamanan digital nasional yang terintegrasi.⁸

Konstruksi politik hukum siber tersebut tercermin dalam pengaturan UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang membentuk kerangka dasar pengaturan aktivitas elektronik dan larangan perbuatan melawan hukum di ruang siber. Melalui interpretasi gramatikal terhadap Pasal 3 UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, makna setiap asas dipahami berdasarkan rumusan bahasanya sebagai dasar normatif penyelenggaraan sistem informasi elektronik yang menegaskan bahwa pemanfaatan teknologi harus diadakan dalam kerangka keamanan hukum, memberikan manfaat bagi masyarakat, dilaksanakan dengan kehati-hatian, didasarkan pada itikad baik, serta memberikan kebebasan bagi pihak-pihak untuk memilih teknologi yang digunakan sepanjang tidak melihat dengan peraturan-undangan, sehingga asas-asas tersebut berfungsi sebagai pedoman normatif bagi implementasi

⁷ Widarto Widarto, "Rekonstruksi Politik Hukum Pemberantasan Tindak Pidana Cyber Crime Terkait Penyalahgunaan Narkotika Yang Berbasis Nilai Keadilan" (UNIVERSITAS ISLAM SULTAN AGUNG, 2021).

⁸ Zahra Pitaloka Islami, "Tantangan Penegakan Hukum Di Era Globalisasi Digital: Strategi Nasional Menghadapi Kejahatan Siber Lintas Batas," *AKSIOMA: Jurnal Sains Ekonomi Dan Edukasi* 2, no. 12 (2025): 2579–91, <https://doi.org/https://doi.org/10.62335/aksioma.v2i12.1985>.

sistem elektronik sekaligus sebagai dasar terhadap penggunaan teknologi informasi agar tetap dalam koridor hukum.⁹

Selanjutnya, melalui interpretasi teleologis terhadap pasal yang sama, asas-asas tersebut dimaknai sebagai penunjuk tujuan pembentuk undang-undang untuk mewujudkan perlindungan dan pengamanan ekosistem digital sebagai arah kebijakan hukum siber nasional, sehingga pemanfaatan informasi tidak hanya diarahkan pada pengembangan inovasi dan efisiensi dalam aktivitas elektronik, tetapi juga pada pembentukan tata kelola sistem elektronik yang menjamin keamanan, kerahasiaan, serta perlindungan terhadap hak dan kepentingan para pihak dalam penyelenggaraan sistem elektronik dan transaksi yang dilakukan dalam ruang digital.¹⁰

Dalam kerangka interpretasi sistematis, ketentuan Pasal 30 UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengenai larangan akses tanpa hak terhadap sistem elektronik tidak dapat dipahami secara terpisah, melainkan harus dibaca dalam keterkaitannya dengan Pasal 32 UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Pasal 20, Pasal 21, Pasal 65, dan Pasal 67 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi,. Dengan menempatkan norma-norma tersebut dalam satu kesatuan sistem pengaturan siber, terlihat bahwa perlindungan hukum tidak hanya diarahkan pada aspek akses sistem, tetapi juga pada integritas, kerahasiaan, dan keamanan data secara menyeluruh. Hal ini menunjukkan bahwa konstruksi hukum siber nasional berorientasi pada perlindungan sistem dan data sebagai unsur utama keamanan ruang digital, selaras dengan asas kepastian hukum dan asas perlindungan hukum dalam negara hukum.¹¹

Keterpaduan pengaturan ini menunjukkan bahwa pembentuk undang-undang menempatkan perlindungan sistem dan perlindungan data dalam satu desain kebijakan hukum yang saling melengkapi. Hal tersebut sejalan dengan asas perlindungan hukum

⁹ Nanung Nugroho Indaryanto, "Rekonstruksi Regulasi Penegakan Hukum Tindak Pidana Penghinaan Dan Pencemaran Nama Baik Melalui Media Sosial Berbasis Nilai Keadilan" (UNIVERSITAS ISLAM SULTAN AGUNG, 2022).

¹⁰ Sumiaty Adelina Hutabarat et al., *CYBER-LAW: Quo Vadis Regulasi UU ITE Dalam Revolusi Industri 4.0 Menuju Era Society 5.0* (PT. Sonpedia Publishing Indonesia, 2023).

¹¹ Teguh Ferdinan Sembiring, "ASPEK PERLINDUNGAN YURIDIS KORBAN PERUNDUNGAN SIBER DALAM PERSPEKTIF UNDANG UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK: KAJIAN DARI SUDUT PANDANG HUKUM DAN SOSIAL" (Magister Hukum, Universitas Islam Sumatera Utara, 2026).

dan asas tanggung jawab, di mana setiap pihak yang menguasai atau memproses data dibebani kewajiban hukum yang jelas untuk menjaga keamanan dan kerahasiaannya. Dengan demikian, keamanan ruang digital dibangun melalui kombinasi norma pencegahan, pembatasan, dan pertanggungjawaban dalam satu struktur regulasi yang terpadu.¹²

Dengan demikian, keseluruhan pengaturan mengenai akses sistem elektronik, integritas data, dan kewajiban pengendali data menunjukkan bahwa konstruksi politik hukum siber nasional telah dirancang secara terpadu untuk menopang keamanan ruang digital. Kesatuan norma larangan, kewajiban, dan sanksi membentuk kerangka perlindungan yang tidak hanya bersifat represif, tetapi juga preventif. Oleh karena itu, konsistensi penafsiran dan penerapan norma menjadi faktor kunci agar tujuan perlindungan dan kepastian hukum di ruang digital dapat terwujud secara efektif

Perlindungan Hukum terhadap Ancaman Siber dalam Kerangka Kebijakan Hukum Nasional

Meningkatnya intensitas serangan siber, kebocoran data, dan penyalahgunaan informasi pribadi menunjukkan bahwa ancaman di ruang digital berkembang lebih cepat dibandingkan pola pengaturannya. Kondisi tersebut menuntut kebijakan hukum yang tidak hanya menyediakan larangan dan sanksi, tetapi juga menjamin perlindungan hak serta kepastian mekanisme pertanggungjawaban. Dalam kerangka negara hukum, respons regulatif terhadap risiko digital menjadi ukuran sejauh mana hukum mampu berfungsi sebagai instrumen perlindungan dan pengendalian.

Kemampuan kebijakan hukum dalam merespons perkembangan ancaman siber dapat dianalisis melalui teori perlindungan hukum dan asas efektivitas hukum. Kedua kerangka tersebut digunakan untuk menilai sejauh mana norma yang dibentuk mampu memberikan jaminan perlindungan hak, kepastian hukum, serta daya guna dalam penerapannya. Secara normatif, negara telah melakukan penguatan rezim hukum siber melalui pembentukan UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi sebagai bentuk respons regulatif terhadap meningkatnya risiko kebocoran dan penyalahgunaan

¹² Muhammad Putra Syawal Al Mahdi and Irwan Triadi, "DARI RECTSVACCUM MENUJU KEPASTIAN HUKUM: PEMBENTUKAN LEMBAGA PERLINDUNGAN DATA PRIBADI SEBAGAI PENEMUAN HUKUM DI ERA DIGITAL," *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial* 12, no. 11 (2025): 4416–30, <https://doi.org/https://doi.org/10.31604/jips.v12i11.2025.4416-4430>.

data pribadi di ruang digital. Regulasi ini menjadi landasan hukum khusus yang mengatur hak subjek data, kewajiban pengendali data, serta mekanisme pertanggungjawaban atas pelanggaran perlindungan data.¹³

Perkembangan ancaman tersebut memperlihatkan bahwa risiko digital tidak lagi bersifat sporadis, melainkan sistemik dan berdampak luas terhadap kepentingan individu, pelaku usaha, maupun negara. Kebocoran data pribadi, peretasan sistem elektronik, dan penyalahgunaan informasi strategis berpotensi menimbulkan kerugian ekonomi, gangguan layanan publik, hingga penurunan kepercayaan masyarakat terhadap sistem digital. Oleh karena itu, kebijakan hukum dituntut untuk membangun kerangka perlindungan yang komprehensif, mencakup kejelasan hak dan kewajiban para pihak, mekanisme pengawasan, serta sistem sanksi yang proporsional. Dalam konteks tersebut, efektivitas hukum tidak hanya diukur dari keberadaan norma tertulis, tetapi juga dari kemampuannya menciptakan kepastian, mencegah pelanggaran, dan memberikan jaminan pemulihan ketika terjadi penyimpangan di ruang digital.¹⁴

Melalui interpretasi teleologis terhadap Pasal 3 UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, tujuan norma dipahami sebagai dasar pembentukan perlindungan preventif dan tata kelola data yang akuntabel. Pemaknaan tersebut menegaskan bahwa perlindungan data pribadi diarahkan untuk menjamin perlindungan terhadap hak privasi setiap subjek data serta mendorong penyelenggara sistem elektronik dan pengontrol data untuk menjalankan pemrosesan data secara bertanggung jawab, transparan, dan proporsional. Dengan demikian, norma ini berfungsi sebagai landasan normatif bagi pembentukan sistem pengelolaan data yang tidak hanya bertumpu pada kepatuhan administratif, tetapi juga pada perlindungan hak asasi dan kepastian hukum.¹⁵

Selanjutnya, interpretasi sistematis dilakukan dengan menghubungkan Pasal 3, Pasal 65, dan Pasal 67 UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi yang memuat tujuan, larangan perolehan dan penggunaan data secara melawan hukum, serta

¹³ Aisyah Azzahra et al., “Analisis Asas Pembentukan UU Perlindungan Data Pribadi Dalam Menjamin Hak Privasi Warga Negara,” *IKRA-ITH HUMANIORA: Jurnal Sosial Dan Humaniora* 9, no. 3 (2025): 1235–46, <https://doi.org/https://doi.org/10.37817/ikraith-humaniora.v9i3>.

¹⁴ Sidar Saputri, “KEPASTIAN HUKUM PIDANA TERHADAP KEBOCORAN DATA PRIBADI PADA MARKETPLACE” (Universitas Islam Negri Palopo, 2025).

¹⁵ Sidi Ahyar Wiraguna and Megawati Barthos, *Hukum Privasi Dan Pelindungan Data Pribadi Di Indonesia* (CV WIDINA MEDIA UTAMA, 2025).

sanksinya dengan Pasal 30 dan Pasal 32 UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengenai larangan akses tanpa hak dan manipulasi data elektronik. Pembacaan norma secara terpadu tersebut menunjukkan bahwa perlindungan data pribadi dan keamanan sistem elektronik merupakan satu kesatuan rezim hukum siber yang ditujukan untuk menjamin integritas, kerahasiaan, dan pertanggungjawaban dalam penyelenggaraan ruang digital.¹⁶

Dengan membaca ketentuan-ketentuan tersebut secara terpadu, terlihat bahwa sistem hukum tidak hanya menindak perbuatan setelah terjadinya pelanggaran, tetapi juga membentuk standar kepatuhan dan tanggung jawab sejak tahap pengumpulan hingga pemanfaatan data. Konstruksi normatif yang saling terhubung ini memperkuat argumentasi bahwa perlindungan hukum di ruang digital bersifat komprehensif, mencakup aspek pencegahan, pengawasan, dan penegakan sanksi dalam satu kerangka regulasi yang terintegrasi.¹⁷

Ditinjau berdasarkan teori perlindungan hukum, kebijakan hukum yang ada telah membentuk landasan normatif untuk memberikan jaminan perlindungan terhadap kepentingan hukum masyarakat di ruang digital, terutama melalui pengaturan hak, kewajiban, dan mekanisme sanksi. Dalam kerangka asas kepastian hukum dan asas proporsionalitas, norma yang tersedia sudah menunjukkan adanya keseimbangan antara perlindungan kepentingan korban, tanggung jawab pelaku, dan kewenangan negara dalam melakukan penegakan hukum. Namun demikian, tingkat perlindungan yang efektif tidak hanya ditentukan oleh keberadaan norma, melainkan juga oleh kualitas implementasinya. Tanpa harmonisasi antarregulasi, koordinasi kelembagaan yang konsisten, serta keseragaman penafsiran dalam praktik penegakan hukum, daya jangkau perlindungan hukum berpotensi menjadi terbatas. Oleh karena itu, kebijakan hukum siber dapat dinilai memadai secara konseptual, tetapi tetap memerlukan penguatan pada aspek

¹⁶ Mushliasak Lubis, "TANGGUNGJAWAB HUKUM PENYEDIA LAYANAN TEKNOLOGI KEUANGAN (FINANCIAL TECHNOLOGY/FINTECH) ATAS PELANGGARAN DATA PRIVASI PENGGUNA" (Magister Hukum, Universitas Islam Sumatera Utara, 2025).

¹⁷ H Uu Nurul Huda et al., *Data Pribadi, Hak Warga, Dan Negara Hukum: Menjaga Privasi Di Tengah Ancaman Digital* (Penerbit Widina, 2024).

struktural dan operasional agar fungsi perlindungan hukum terhadap ancaman siber yang terus berkembang dapat terwujud secara optimal.¹⁸

Penguatan tersebut menjadi relevan mengingat karakter ancaman siber yang bersifat dinamis, lintas yurisdiksi, dan memanfaatkan celah teknologis yang terus berkembang. Dalam konteks ini, perlindungan hukum tidak dapat dipahami semata-mata sebagai keberadaan norma tertulis, melainkan sebagai suatu sistem yang bekerja secara terpadu antara pengaturan substantif, mekanisme pengawasan, dan penegakan sanksi. Ketiadaan sinkronisasi antarperaturan atau perbedaan penafsiran dalam praktik berpotensi menimbulkan ketidakpastian hukum dan melemahkan posisi subjek hukum yang seharusnya dilindungi. Oleh karena itu, konsolidasi regulasi, peningkatan kapasitas kelembagaan, serta pembentukan standar penegakan yang konsisten menjadi bagian integral dari upaya memastikan bahwa perlindungan hukum di ruang digital tidak hanya bersifat deklaratif, tetapi benar-benar mampu menjamin keamanan, kepastian, dan keadilan bagi masyarakat.¹⁹

Dengan demikian, penguatan perlindungan hukum di bidang siber harus ditempatkan sebagai agenda berkelanjutan dalam kebijakan hukum nasional, melalui penyelarasan norma, konsistensi penafsiran, dan penguatan kapasitas penegakan hukum. Langkah tersebut diperlukan agar kerangka regulasi yang telah dibentuk tidak hanya memberikan kepastian secara normatif, tetapi juga mampu berfungsi secara nyata dalam melindungi kepentingan hukum masyarakat serta menjaga keamanan ruang digital nasional di tengah perkembangan ancaman yang semakin kompleks.

SIMPULAN

Arah dan konstruksi politik hukum siber di Indonesia menunjukkan orientasi pada penguatan peran negara dalam mengatur, melindungi, dan mengamankan ruang digital nasional melalui pembentukan dan pengembangan regulasi di bidang teknologi informasi dan data. Politik hukum siber dibangun dengan menempatkan keamanan sistem

¹⁸ Khwarizmi Maulana Simatupang, "Tinjauan Yuridis Perlindungan Hak Cipta Dalam Ranah Digital," *Jurnal Ilmiah Kebijakan Hukum* 15, no. 1 (2021): 67–80, <https://doi.org/DOI: http://dx.doi.org/10.30641/kebijakan.2021.V15.67-80>.

¹⁹ S H Budiyo, *Pengantar Cybercrime Dalam Sistem Hukum Pidana Di Indonesia* (Sada Kurnia Pustaka, 2025).

elektronik, perlindungan data, dan kepastian hukum sebagai fondasi utama. Konstruksi normatifnya menegaskan asas kepastian hukum, kehati-hatian, dan perlindungan kepentingan umum, serta memperlihatkan pendekatan preventif dan represif terhadap penyalahgunaan ruang digital. Dengan demikian, politik hukum siber telah diarahkan sebagai instrumen strategis untuk menjaga stabilitas dan keamanan ekosistem digital nasional.

Kebijakan hukum yang ada pada dasarnya telah membentuk kerangka perlindungan hukum terhadap ancaman siber yang berkembang, karena tersedia perangkat regulasi yang mengatur larangan, kewajiban, serta sanksi atas pelanggaran di ruang digital, termasuk perlindungan data pribadi dan keamanan sistem elektronik. Secara normatif, pengaturan tersebut telah mencerminkan upaya negara dalam memberikan jaminan kepastian hukum, perlindungan hak, dan mekanisme pertanggungjawaban. Namun demikian, kualitas perlindungan hukum tidak hanya ditentukan oleh keberadaan norma, melainkan juga oleh konsistensi harmonisasi antarregulasi, keseragaman penafsiran, serta dukungan kelembagaan dalam penegakannya. Dengan demikian, kerangka perlindungan hukum terhadap ancaman siber telah terbentuk secara konseptual, tetapi penguatan pada aspek implementasi dan koordinasi tetap menjadi prasyarat agar perlindungan tersebut dapat berfungsi secara optimal dalam menghadapi dinamika ancaman digital.

UCAPAN TERIMA KASIH

Penulis menyampaikan apresiasi dan terima kasih kepada semua pihak yang telah memberikan dukungan dalam proses penyusunan artikel ini. Ucapan terima kasih disampaikan kepada pimpinan institusi dan rekan-rekan akademisi yang telah memberikan masukan konstruktif, dukungan moral, serta ruang diskusi ilmiah yang memperkaya substansi penelitian ini. Semoga artikel ini dapat memberikan kontribusi bagi pengembangan ilmu hukum, khususnya dalam bidang hukum siber dan kebijakan hukum digital di Indonesia, serta menjadi referensi bagi penguatan keamanan ruang digital nasional.

DAFTAR PUSTAKA

Alfi, Muhammad, Ni Putu Yundari, and Ahnaf Tsaqif. "Analisis Risiko Keamanan Siber Dalam Transformasi Digital Pelayanan Publik Di Indonesia." *Jurnal Kajian*

- Strategik Ketahanan Nasional* 6, no. 2 (2023): 5.
- Azzahra, Aisyah, Anisa Mutiara Rizky, Nur Wahid Muharrom, Ronaan Maulana Basuki, Devina Angelica, and Kuswan Hadji. "Analisis Asas Pembentukan UU Perlindungan Data Pribadi Dalam Menjamin Hak Privasi Warga Negara." *IKRA-ITH HUMANIORA: Jurnal Sosial Dan Humaniora* 9, no. 3 (2025): 1235–46. <https://doi.org/https://doi.org/10.37817/ikraith-humaniora.v9i3>.
- Budiyanto, S H. *Pengantar Cybercrime Dalam Sistem Hukum Pidana Di Indonesia*. Sada Kurnia Pustaka, 2025.
- Cahyono, Soetardi Tri, Wina Erni, and Taufik Hidayat. "Rekonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cyber Crime) Dalam Sistem Peradilan Pidana Indonesia: Rekonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cyber Crime) Dalam Sistem Peradilan Pidana Indonesia." *Dame Journal of Law* 1, no. 1 (2025): 111–33. <https://doi.org/https://doi.org/10.64344/djl.v1i1.6>.
- Huda, H Uu Nurul, M H SH, H Tatang Astaruddin, M Si SH, Muhammad Irsan Nasution, M H SH, S H Alwi Al Haddad, Dian Rachmat Gumelar, and M H SH. *Data Pribadi, Hak Warga, Dan Negara Hukum: Menjaga Privasi Di Tengah Ancaman Digital*. Penerbit Widina, 2024.
- Hutabarat, Sumiaty Adelina, Selvia Junita Praja, Didik Suhariyanto, Saptaning Ruju Paminto, Dora Kusumastuti, Rahma Melisha Fajrina, Immi Ira Monalisa Saragih, Eko Budihartono, and Muhamad Abas. *CYBER-LAW: Quo Vadis Regulasi UU ITE Dalam Revolusi Industri 4.0 Menuju Era Society 5.0*. PT. Sonpedia Publishing Indonesia, 2023.
- Indaryanto, Nanung Nugroho. "Rekonstruksi Regulasi Penegakan Hukum Tindak Pidana Penghinaan Dan Pencemaran Nama Baik Melalui Media Sosial Berbasis Nilai Keadilan." UNIVERSITAS ISLAM SULTAN AGUNG, 2022.
- Indriyani, Dian. "Peran Regulasi Digital Dalam Perlindungan Hak Masyarakat Modern." *Jurnal Kajian Hukum* 1, no. 1 (2025): 24–29.
- Islami, Zahra Pitaloka. "Tantangan Penegakan Hukum Di Era Globalisasi Digital: Strategi Nasional Menghadapi Kejahatan Siber Lintas Batas." *AKSIOMA: Jurnal Sains Ekonomi Dan Edukasi* 2, no. 12 (2025): 2579–91. <https://doi.org/https://doi.org/10.62335/aksioma.v2i12.1985>.
- Laita, Rivan Hasan. "Kritik Terhadap Lemahnya Penegakan Hukum Dalam Kasus Cybercrime Peretasan Platform Kripto Indodax 2024." *Iuris Studia: Jurnal Kajian Hukum* 6, no. 2 (2025): 218–28. <https://doi.org/https://doi.org/10.55357/is.v6i2.888>.
- Lubis, Mushliasak. "TANGGUNGJAWAB HUKUM PENYEDIA LAYANAN TEKNOLOGI KEUANGAN (FINANCIAL TECHNOLOGY/FINTECH) ATAS PELANGGARAN DATA PRIVASI PENGGUNA." Magister Hukum, Universitas Islam Sumatera Utara, 2025.
- Mahdi, Muhammad Putra Syawal Al, and Irwan Triadi. "DARI RECTSVACCUM MENUJU KEPASTIAN HUKUM: PEMBENTUKAN LEMBAGA PERLINDUNGAN DATA PRIBADI SEBAGAI PENEMUAN HUKUM DI ERA DIGITAL." *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial* 12, no. 11 (2025): 4416–30. <https://doi.org/https://doi.org/10.31604/jips.v12i11.2025.4416-4430>.
- Najwa, Fadhila Rahman. "Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber Di Indonesia." *AL-BAHTS: Jurnal Ilmu Sosial*,

- Politik, Dan Hukum* 1, no. 2 (2024): 8–16.
<https://doi.org/https://doi.org/10.32520/albahts.v2i1.3044>.
- Saputri, Sidar. “KEPASTIAN HUKUM PIDANA TERHADAP KEBOCORAN DATA PRIBADI PADA MARKETPLACE.” Universitas Islam Negri Palopo, 2025.
- Sembiring, Teguh Ferdinan. “ASPEK PERLINDUNGAN YURIDIS KORBAN PERUNDUNGAN SIBER DALAM PERSPEKTIF UNDANG UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK: KAJIAN DARI SUDUT PANDANG HUKUM DAN SOSIAL.” Magister Hukum, Universitas Islam Sumatera Utara, 2026.
- Simatupang, Khwarizmi Maulana. “Tinjauan Yuridis Perlindungan Hak Cipta Dalam Ranah Digital.” *Jurnal Ilmiah Kebijakan Hukum* 15, no. 1 (2021): 67–80.
<https://doi.org/DOI: http://dx.doi.org/10.30641/kebijakan.2021.V15.67-80>.
- Syakur, Abd. “REKONSTRUKSI PERLINDUNGAN HUKUM KONSUMEN DALAM TRANSAKSI E-COMMERCE MELALUI KEBIJAKAN PEMERINTAH UNTUK Mendukung Ekonomi Digital Yang Berkeadilan.” UNIVERSITAS ISLAM SULTAN AGUNG, 2022.
- Widarto, Widarto. “Rekonstruksi Politik Hukum Pemberantasan Tindak Pidana Cyber Crime Terkait Penyalahgunaan Narkotika Yang Berbasis Nilai Keadilan.” UNIVERSITAS ISLAM SULTAN AGUNG, 2021.
- Wiraguna, Sidi Ahyar, and Megawati Barthos. *Hukum Privasi Dan Pelindungan Data Pribadi Di Indonesia*. CV WIDINA MEDIA UTAMA, 2025.