Jurnal RechtsVinding Media Pembinaan Hukum Nasional ISSN 2089-9009
Volume 14 Nomor 2, Agustus 2025

REDESAIN KEBIJAKAN HUKUM KEAMANAN DAN KETAHANAN SIBER: STUDI KASUS SERANGAN SIBER PADA PUSAT DATA NASIONAL TAHUN 2024

Redesigning Cyber Security and Resilience Policies: A Case Study of Cyber Attacks on the National Data Center in 2024

Habib Ferian Fajar
Fakultas Hukum Universitas Gadjah Mada
Bulaksumur, Daerah Istimewa Yogyakarta
e-mail: habibferianfajar@mail.ugm.ac.id

Afdhal Fadhila
Fakultas Hukum Universitas Andalas
e-mail: afdhalfdl@gmail.com

Muhammad Kevin Yades
Fakultas Hukum Universitas Andalas
e-mail: kevinyades2724@gmail.com

Abstrak

Keamanan dan ketahanan siber menjadi hal yang niscaya seiring dengan kian menjamurnya pemanfaatan internet dalam pelbagai aspek kehidupan. Belajar pada kasus serangan siber yang menargetkan Pusat Data Nasional Sementara (PDNS) tahun 2024 silam, terdapat banyak persoalan yang harus dibenahi oleh pemerintah Indonesia. Artikel ini menggunakan penelitian normatif melalui studi kepustakaan dalam pengumpulan data. Diketahui bahwa konstruksi hukum siber Indonesia masih menunjukkan kelemahan, seperti belum adanya undang-undang yang secara khusus dan komprehensif untuk melindungi ruang siber saat ini. Sehingga pemerintah masih mempertontonkan kegamangan dalam penanggulangan ancaman siber yang acapkali menghantui. Maka perlu adanya arah dan desain reformasi kebijakan hukum keamanan dan ketahanan siber yang secara garis besar harus meliputi lima aspek berikut: (1) pembentukan Undang-Undang Keamanan dan Ketahanan siber; (2) harmonisasi peraturan sektoral yang saling tumpang tindih agar tidak menciptakan dualisme otoritas dan konflik kewenangan; (3) penguatan mekanisme pengawasan demokratis terhadap lembaga-lembaga yang memiliki otoritas siber; (4) pelibatan masyarakat sipil multi *stakeholder* dalam setiap proses pengambilan kebijakan; dan (5) perlindungan terhadap hak-hak digital warga negara.
Kata Kunci: Pusat Data Nasional, Serangan Siber, Keamanan dan Ketahanan Siber.

Abstract

Cyber security and resilience are inevitable along with the increasing use of the internet in various aspects of life. Learning from the case of a cyber attack targeting the Temporary National Data Center (PDNS) in 2024, there are many problems that must be fixed by the Indonesian government. This article uses normative research through literature studies in data collection. It is known that Indonesia's construction of cyber law still shows weaknesses, such as the lack of a specific and comprehensive law to protect cyberspace at this time. So that the government is still showing uncertainty in dealing with cyber threats that often haunt them. Therefore, there needs to be a direction and design of cyber security and resilience law policy reform which in general must include the following five aspects. (1) Establishment of the Cyber Security and Resilience Law. (2) Harmonization of overlapping sectoral regulations so as not to create dualism of authority and conflict of authority. (3) Strengthening democratic supervision mechanisms for institutions that have cyber authority. (4) The involvement of multi-stakeholder civil society in every policy-making process. (5) Protection of citizens' digital rights.
Keywords: *National Data Center, Cyberattacks, Security and Cyber Resilience.*

A. Pendahuluan

Perkembangan teknologi informasi dan komunikasi telah melahirkan internet (*interconnected network*) yang secara langsung maupun tidak langsung menimbulkan perubahan di dalam masyarakat.[1] Digitalisasi menjadi salah satu aspek yang sangat terlihat sebagai dampak perubahan yang diakibatkan oleh perkembangan internet tersebut. Hampir semua lini bertransformasi dan mengambil peran dalam digitalisasi, sebagai bentuk inovasi agar terhindar dari ketertinggalan. Bahkan pemerintah Indonesia melalui Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintah Berbasis Elektronik (Perpres Nomor 95 Tahun 2018) serta diperkuat dengan Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Nasional (Perpres Nomor 39 Tahun 2019) dan Peraturan Presiden Nomor 82 Tahun 2023 tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional (Perpres Nomor 82 Tahun 2023) berkomitmen agar pelayanan pada publik dapat lebih mudah diakses dengan terintegrasinya jaringan internet dalam penyelenggaraan pemerintahan (*e-government*). Sehingga kondisi umat manusia saat ini dapat dikatakan telah berada dalam peradaban siber (*cyber civilization*).[2]

Ancaman siber atau ancaman dalam dunia maya secara garis besar dapat diklasifikasikan pada istilah *cyber attack* (serangan siber), *cyber warfare* (perang siber), dan *cyber crime* (kejahatan siber). Kendati ketiga istilah tersebut saling berkelindan, namun Oona A. Hathway, *et.all* memberikan batasan dan perbedaan satu sama lain. Menurutnya serangan siber dapat dilakukan oleh aktor negara atau non-negara, melibatkan tindakan aktif, bertujuan untuk melemahkan atau merusak fungsi jaringan komputer, dan harus memiliki tujuan politik atau keamanan nasional. Sedangkan kejahatan siber tidak perlu merusak jaringan komputer targetnya (meskipun dalam beberapa kasus juga bisa merusak), dan sebagian besar tidak memiliki tujuan politik atau keamanan nasional. Pelaku kejahatan siber biasanya adalah individu, bukan negara. Walaupun beberapa serangan siber juga merupakan kejahatan siber dan tidak semua kejahatan siber adalah serangan siber. Di sisi lain, perang siber selalu memenuhi syarat-syarat serangan siber, namun tidak semua serangan siber adalah perang siber. Hanya serangan siber yang berdampak setara dengan serangan bersenjata konvensional atau yang terjadi dalam konteks konflik bersenjata yang dapat dikategorikan sebagai perang siber.[3]

Indonesia merupakan negara yang kerap dihadapkan dengan ancaman serangan siber. Sepanjang tahun 2024 saja, sebagaimana yang dilaporkan oleh Badan Siber dan Sandi Negara (BSSN), terdapat 330.527.636 total trafik anomali serangan siber. Aktivitas anomali trafik ini dapat berdampak pada penurunan performa perangkat dan jaringan, pencurian data sensitif, hingga perusakan reputasi dan penurunan kepercayaan terhadap suatu organisasi. Berikut tabel sepuluh trafik anomali teratas.[4]

1 Catur Nugroho, *Cyber Society Teknologi, Media Baru, dan Distrupsi Informasi* (Jakarta: Kencana, 2020), hlm. 121.
2 Wasyihun Sema Admass, Yirga Yayeh Munaye, and Abebe Abeshu Diro, "Cyber Security: State of The Art, Challenges and Future Directions," *Cyber Security and Applications* 2, (2024): 1.
3 Oona A. Hathaway, et.all, " The Law of Cyber Attack," *California Law Review* 100, no. 817 (2012): 834-836.
4 BSSN, *Lanskap Keamanan Siber Indonesia 2024* (Jakarta: BSSN, 2024), hlm.16-17.

Tabel. 1 Top 10 Trafik Anomali Serangan Siber Tahun 2024

No.	Jenis Trafik Anomali	Jumlah
1.	Mirai Botnet	81.286.596
2.	Generic Trojan RAT	30.914.047
3.	PhishingSite	26.771.610
4.	MyloBot Botnet	23.510.819
5.	Discover the communication behavior of the VPN tool wireguard	16.481.931
6.	The remote connection tool zerotier is actice	15.209.912
7.	Discover the communication behavior of VPN tool OpenVPN	14.472.619
8.	Remcos RAT activity	12.731.831
9.	Discover client mining behavior (login to mining pool	7.364.936
10.	Netcore backdoor vulnerability exploitation	7.06.156

Sumber: Diolah dari Lanskap Keamanan Siber Indonesia 2024

Akan tetapi, berdasarkan hasil pemantauan *Cyber Threat Intelligence* (CTI) terdapat sebanyak 593 dugaan insiden siber seperti kebocoran data, *ransomware*, *web defacement*, indikasi serangan DDoS (*Distributed Denial of Service*), dan pemantauan proaktif dugaan insiden siber. Sektor administrasi pemerintahan menempati urutan pertama dengan 352 dugaan insiden siber dari 593 dugaan yang tercatat.[5]

Salah satu insiden serangan siber yang menarik perhatian publik terhadap administrasi pemerintahan di tahun 2024 tersebut, adalah serangan pada Pusat Data Nasional Sementara 2 (PDNS 2) yang berlokasi di Surabaya. Pusat Data Nasional (PDN) berdasarkan Perpres Nomor 95 Tahun 2018 dikelola oleh Kementerian Komunikasi dan Informatika (Kemenkominfo) yang sekarang bertransformasi menjadi Kementerian Komunikasi dan Digital (Komdigi), mendapatkan serangan *ransomware* sejak tanggal 20 Juni 2024. Setidaknya serangan ini berdampak pada 239 instansi baik di tingkat pusat maupun daerah, yang mengunci hingga tidak bisa diaksesnya layanan pada instansi terdampak. Peretas meminta tebusan sebesar $8 Juta atau setara Rp.131,6 miliar, atas serangan *ransomware* bernama *Brain Cipher Ransomware* (*ransomware lockbit* 3.0) yang mereka gunakan.[6] Ketua Indonesia *Cyber Security Forum* Ardi Sutedja pada Kompas menyatakan, gangguan pada PDN merupakan bencana siber berskala nasional karena data hasil peretasan berpotensi dimanfaatkan berbagai pihak termasuk negara lain dengan kepentingan yang beragam. Lebih lanjut Ardi menyebutkan, bahwa peretasan terhadap

[5] *Ibid*, hlm. 33.
[6] Tempo, "Kronologi Pusat Data Nasional Jebol Hingga Desakan Menkominfo Budi Arie Mundur dari Jabatannya." https://www.tempo.co/politik/kronologi-pusat-data-nasional-jebol-hingga-desakan-menkominfo-budi-arie-mundur-dari-jabatannya-44552 (diakses 5 Mei 2025).

PDN bukan peretasan biasa tetapi menyangkut kelemahan manajerial, sistem teknologi, bahkan bisa jadi dalam pengadaan teknologinya.[7] Tentu saja yang mengalami kerugian dari peristiwa ini tidak hanya pemerintah, namun juga warga negara. Sebab data-data pribadi warga negara yang juga terdata pada PDN berpotensi disalahgunakan oleh peretas. Buruknya koordinasi antara Kemenkominfo dan BSSN, dan ketiadaan cadangan data (*data backup*) pada PDNS semakin memperumit keadaan.

Melihat begitu mudahnya peretasan yang terjadi pada objek vitas strategis nasional tersebut, menjadi bukti betapa lemahnya keamanan siber nasional. Tidak heran *National Cyber Security Index* (NCSI) pada tahun 2023 hanya memberikan skor 63.64 untuk ketahanan siber Indonesia, dengan menduduki peringkat ke-49 dari 176 negara yang disurvei. Skor tersebut masih tergolong rendah, terlebih jika dibandingkan dengan beberapa negara tetangga di ASEAN. Seperti Malaysia di peringkat 22 (skor 79.22), Singapura di peringkat 31 (skor 71.43), dan Thailand di peringkat 45 (skor 64.94).[8] Keamanan siber (*cyber security*) merupakan bagian yang tidak terpisahkan dari keamanan nasional dari suatu negara.[9] Tantangan keamanan siber bukanlah perkara teknis semata, namun jauh lebih kompleks. Hal tersebut dapat diilustrasikan dalam kalimat berikut:[10]

> "The challenge of cyber security is not merely a technical one. It is a political, economic, social, organizational, and behavioral challenge in a technically fluid environment. The consequences of interconnectedness and the condition of constant contact that flows from it require a framework that can position a State comprehensively."

Sehingga belajar dari serangan pada PDNS tahun kemarin, Indonesia perlu untuk berbenah dan mereformasi arah kebijakan keamanan dan ketahanan siber ke depannya.

Potret regulasi yang dimiliki oleh Indonesia saat ini, juga belum mampu menciptakan iklim keamanan siber secara utuh. Misalnya regulasi di level undang-undang, terdapat Undang-Undang Nomor 11 Tahun 2018 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), masing-masing masih memiliki kelemahan untuk dijadikan rujukan dalam menjawab tantangan keamanan dan ketahanan siber. Seperti kedua beleid tersebut masih bersifat *individual centric* dalam memberikan perlindungan atas serangan siber.

---

7 Kompas.id, "Bencana Nasional Serangan ke Pusat Data Nsional Bisa Buka Perang Siber dan Ancaman Negara." https://www.kompas.id/baca/polhuk/2024/06/26/bencana-nasional-akibat-serangan-ke-pusat-data-nasional (diakses 5 Mei 2025). Pasca serangan *ransomware* tersebut Kejaksaan mengendus terdapat indikasi dugaan tindak pidana korupsi dalam Pengadaan barang/jasa pada pengelolaan PDN. Lihat dalam Tempo, "Kejaksaan Usut Dugaan Korupsi Pusat Data Nasional Usai Serangan Ransomware Juni 2024," https://www.tempo.co/hukum/kejaksaan-usut-dugaan-korupsi-pusat-data-nasional-usai-serangan-ransomware-juni-2024--1220952 (diakses 5 Mei 2025).

8 NCSI, "National Cyber Security Index," https://ncsi.ega.ee/ncsi-index/?order=rank&archive=1 (diakses 5 Mei 2025).

9 Lawrance J. Trautman, "Cybersecurity What About U.S Policy?" *Journal of Law, Technology & Policy* 2015, no. 341 (2015): 359.

10 Michael P. Fischerkeller, Emily O. Goldman, dan Richard J. Harknett, *Cyber Persistence Theory Redefining National Security in Cyberscpace* (New York: Oxford University Press, 2022), hlm. 156.

Maka salah satu perwujudan reformasi kebijakan keamanan dan ketahanan siber Indonesia, adalah dengan segera mengesahkan RUU tentang Keamanan dan Ketahanan Siber yang telah muncul kepermukaan sejak tahun 2019 silam. Harapannya RUU ini mampu menjawab persoalan keamanan dan ketahanan siber dewasa ini, sehingga asas *meaningful participation* dalam proses pembentukan undang-undang dimaksud menjadi keniscayaan. Pasalnya RUU *a quo* masuk dalam daftar Program Legislasi Nasional (Prolegnas) Prioritas 2025.[11] Keamanan siber menjadi contoh menarik mengapa perlu mengadopsi perspektif yang lebih kompleks dan interaktif untuk memahami hubungan dinamis antara aktor manusia dan teknologi.[12] Berangkat dari latar belakang tersebut, Penulis sepakat untuk mengusung dua rumusan masalah. Pertama, bagaimana konstruksi hukum serta potret aktual keamanan dan ketahanan siber Indonesia? Kedua, bagaimana arah dan desain reformasi kebijakan hukum keamanan dan ketahanan siber mendatang?

B. Metode Penelitian

Penelitian ini menggunakan metode penelitian normatif, yakni merupakan suatu upaya dalam menemukan aturan-aturan hukum, prinsip-prinsip hukum, maupun doktrin-doktrin hukum guna menjawab permasalahan-permasalahan hukum yang dihadapi.[13] Penelitian hukum normatif juga dilakukan untuk menciptakan argumentasi, teori, serta konsep hukum yang baru sebagai suatu preskripsi untuk menyelesaikan masalah-masalah hukum yang dihadapi.[14]

Pendekatan yang dilakukan dalam penelitian ini adalah pendekatan perundang-undangan (*statue approach*), yaitu pendekatan yang digunakan untuk menganalisis ketentuan-ketentuan hukum terkait keamanan siber, dengan analisis difokuskan kepada relevansi serta efektivitas pengaturan tersebut dalam memecahkan permasalahan keamanan siber saat ini.[15] Pendekatan selanjutnya yang digunakan dalam penelitian ini adalah pendekatan perbandingan (*comparative approach).* Pendekatan ini bertujuan untuk membandingkan ketentuan-ketentuan di bidang keamanan siber pada beberapa negara, yang kemudian melalui pendekatan ini akan teridentifikasikan kesamaan, perbedaan dan peluang untuk mengadopsikannya ke dalam hukum Indonesia.[16] Terakhir, penelitian ini juga menggunakan pendekatan konseptual (*conceptual approach),* yakni pendekatan yang menggunakan pandangan teoritik dalam hal mengkonsepsikan suatu permasalahan hukum yang sebelumnya tidak diatur dalam peraturan hukum yang berlaku saat ini.[17]

---

11 Hukumonline, "Ini 41 RUU yang Masuk Prolgenas Prioritas 2025," https://www.hukumonline.com/berita/a/ini-41-ruu-yang-masuk-prolegnas-prioritas-2025-lt673c52dc1bcb0/?page=2 (diakses 5 Mei 2025)

12 Myriam Dunn Cavelty, *The Politics of Cyber-Security* (New York: Routledge, 2025), hlm. 6.

13 Peter Mahmud Marzuki (Peter Mahmud I), *Penelitian Hukum*: Edisi Revisi, (Jakarta: Kencana Prenada Media Group, 2005), hlm. 47.

14 *Ibid.,* 35.

15 Muhaimin, *Metode Penelitian Hukum,* (Mataram: Mataram University Pers, 2020), hlm. 56.

16 Ahmad Irwan Hamzani dkk, "Legal Research Method: Theoretical and Implementative Review", *International Journal of Membrane Science and Technology* 10, no. 2 (2023): 3610-3619.

17 Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif : Suatu Tinjauan Singkat,* ed. 17, (Jakarta : Rajawali Pers, 2015), hlm. 92.

Penelitian ini menggunakan metode pengumpulan data dengan studi kepustakaan, yang kemudian data-data tersebut dianalisis mengunakan teknik analisis kualitatif, yang akan menghasilkan data deskriptif berupa kata-kata tertulis maupun lisan dari orang-orang dan perilaku yang diamati.[18] Dalam hal penelitian ini, maka teknik analisis kualitatif digunakan untuk menginterpretasikan data, pemahaman hasil analisis, merumuskan kesimpulan, serta menghasilkan rekomendasi atau saran terkait dengan permasalahan keamanan siber tanpa menarik hipotesa dan perhitungan secara statistik.[19] Jenis data yang dipergunakan dalam penelitian ini adalah data sekunder, yaitu data yang diperoleh dari dokumen-dokumen resmi, buku, dan penelitian-penelitian terdahulu melalui studi kepustakaan, yang berkaitan dengan permasalahan dalam penelitian ini. Data sekunder berasal dari bahan hukum primer, sekunder, dan tersier.[20]

C. Pembahasan

1. Konstruksi Hukum Siber Indonesia

Perkembangan dunia digital yang semakin pesat diiringi dengan ancaman-ancaman siber yang beresiko mengancam kedaulatan negara, sehinga keamanan dan pertahanan siber merupakan kewajiban negara untuk menjamin kedaulatan digital Indonesia. Keamanan dan pertahanan siber merupakan wujud dalam rangka untuk melindungi segenap tumpah bangsa, yang termaktub dalam konstitusi UUD 1945, serta dalam usaha untuk mempertahankan kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia, dan keselamatan segenap bangsa dari ancaman dan gangguan terhadap keutuhan bangsa dan negara sebagaimana diatur dalam Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara.

Keamanan siber secara harfiah dapat dimaknai sebagai kebijakan, alat, perlindungan, keamanan, pedoman, manajemen resiko, pelatihan, jaminan, serta teknologi yang digunakan untuk melindungi seluruh lingkungan siber dan organisasi dan aset pengguna, yang terdiri dari perangkat yang terhubung baik pada komputasi personal, infrakstruktur, aplikasi, layanan, sistem telekomunikasi maupun informasi yang disimpan dalam dunia maya.[21] Negara pada keamanan siber adalah sebagai suatu representasi kekuasaan yang menegaskan bahwa negara turut hadir di dalam lingkungan siber guna mengatur kehidupan warganya dalam rangka mencapai tujuan bersama.[22] Akan tetapi, kenyataannya keamanan siber seringkali tidak dijadikan prioritas dalam sarana dan prasarana elektronik, di tengah pemerintah saat ini sedang mentransformasi pelayananan publik dari sistem konvensional ke sistem berbasis elektronik melalui program SPBE, serta program Satu Data Indonesia, dengan tujuan untuk mengintegrasikan seluruh data baik dari instansi pusat maupun daerah. Penyelengaaran pelayanan publik berbasis elektronik ini, harus disertai dengan jaminan keamanan siber yang tidak menganggu kepentingan umum. Pasal 40 ayat (2) UU ITE mewajibkan pemerintah untuk

18 Lexy J. Moleong, Metodologi Penelitian Kualitatif, (Bandung: Rosdakarya, 2000), hlm. 3.
19 Abdulkadir Muhammad, *Hukum dan Penulisan Hukum*, (Bandung: Citra Aditya Bakti, 2004), hlm. 157.
20 Suratman dan Philip Dillah, Metode penelitian Hukum, (Bandung: Alfabeta, 2012), hlm. 115.
21 M. Prakoso Aji, "Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi)", *Jurnal Politica* 5, no. 2 (2022): 222-238.
22 *Ibid.*

melindungi kepentingan umum dari segala ancaman siber.

Bukti keamanan siber di Indonesia belum bisa menjamin terlindungnya data-data elektronik, adalah terjadinya kasus-kasus kebocoran data akibat serangan siber. Contoh kasus serangan siber yang pernah terjadi, adalah serangan *ransomware* pada PDNS, yang membuat pelayanan publik di beberapa instansi dalam beberapa hari menjadi lumpuh dan terhambat, serta berakibat pada kerugian ekonomi yang mencapai 6,3 triliun Rupiah serta surplus usaha yang hilang sebesar 2,7 triliun rupiah.[23] Serangan *ransomware* ini, tidak dapat dipandang sebagai suatu serangan siber biasa, tetapi apabila serangan tersebut tidak ditangani dengan baik, maka akan berujung pada serangan *availability of data*, atau berakibat akan hilangnya data *(data loss)* dalam sistem atau pusat data tersebut.[24] Kebocoran data ini menurut Ruby Alamsyah (Pakar Teknologi dan Ahli Forensik Siber), disebabkan oleh sistem pada PDNS belum dilengkapi dengan prosedur antisipasi terhadap gangguan atau serangan siber, sehingga seharusnya ketika sistem yang terdapat pada PDNS tersebut dibangun diiringi juga dengan prosedur keamanan siber, seperti *Business Continuity Plan* (BCP) atau *Disaster Recovery Plan* (DRP), serta dilengkapi dengan sistem pencadangan data melalui *Data Recovery Center* (DRC) yang akan menyimpan cadangan data apabila sistem utama mengalami kerusakan atau mati. Prosedur keamanan data sendiri telah diatur Pasal 24 ayat (1) dan (2) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP Nomor 71 Tahun 2019), yang mewajibkan penyelenggara sistem elektronik untuk memiliki sarana dan prasarana serta sistem untuk pencegahan dan penanggulangan terhadap ancaman dan serangan yang menimbulkan gangguan, kegagalan, dan kerugian, akan tetapi, kenyataannya pembangunan PDNS ini dibangun dengan melalaikan beberapa aspek dalam keamanan data.[25]

Selain membangun sistem pencegahan, sistem pemulihan dan pencadangan data merupakan salah satu bagian terpenting dalam instalasi pusat data, sebagaimana diatur dalam Pasal 40 ayat (4) dan (5) UU ITE, bahwa pemerintah atau instansi penyelenggara elektronik wajib menyediakan rekam cadang elektronik dengan tujuan untuk perlindungan data. Sistem pencadangan diatur lebih lanjut dalam Pasal 99 PP Nomor 71 Tahun 2019, ditujukan pada beberapa sektor yang dirincikan dalam ayat (2) Pasal *a quo*. Ketentuan Pasal *a quo,* mewajibkan instansi pemilik data elektronik untuk menyediakan rekam cadang elektroniknya serta menghubungkannya ke pusat data. Akan tetapi, terdapat kelemahan dalam kedua peraturan perundang-undangan tersebut, yaitu tidak adanya ketentuan terkait sanksi atau tindakan apabila instansi pemilik data tidak mematuhi kewajiban dalam menyediakan sarana dan prasarana pencadangan data.

Penyebab lainnya kebocoran data, selain tidak tersedianya sarana dan prasana

---

23 Info Bank News, "Ngeri! Segini Potensi Kerugian Ekonomi Akibat Peretasan PDN", https://infobanknews.com/ngeri-segini-potensi-kerugian-ekonomi-akibat-peretasan-pdn/ (diakses pada 17 Mei 2025).

24 Elsam, "Insiden Keamanan Siber dan Dugaan Kegagalan Pelindungan Data PDN Sementara, Harus Ditangani Secara Simultan dan Tuntas", https://www.elsam.or.id/siaran-pers/insiden-keamanan-siber-dan-dugaan-kegagalan-pelindungan-data-pdn-sementara--harus-ditangani-secara-simultan-dan-tuntas (diakses pada 17 Mei 2025).

25 Aryojati Ardipandanto, "Lemahnya Pengamanan Pusat Data Nasional Sementara Terhadap Serangan Siber," *Info Singkat* 16, no. 13 (2024): 9.

keamanan siber, adalah kurangnya koordinasi antara penyelenggara pusat data, dalam hal ini Kemenkominfo dengan BSSN sebagai lembaga yang berwenang dalam keamanan siber, walaupun keamanan siber telah diatur pada Perpres Nomor 47 Tahun 2023 tentang Strategi Nasional Keamanan Siber dan Manajemen Krisis (Perpres 47 Tahun 2023), tetapi nyatanya perpres ini belum cukup untuk mengakomodir dan mempertegas kewenangan dan koordinasi kelembagaan bahkan pada kasus PDNS terjadi kesalahpahaman dan saling melempar tanggung jawab antara Kemenkominfo dan BSSN serta instansi pengguna SPBE, seperti yang terjadi dalam RDP dengan Komisi 1 DPR RI 27 Juni 2024, sehingga sudah seharusnya keamanan siber diatur dalam aturan yang lebih tinggi dibandingkan saat ini, yaitu melalui UU Keamanan Siber.[26] Pengesahan UU Keamanan Siber menjadi opsi penting untuk mengatur tata kelola keamanan siber, salah satunya mempertegas peran dan tugas pokok dan fungsi antar lembaga dalam tata kelola keamanan siber serta juga dapat dimasukan beberapa ketentuan lain, seperti asuransi siber, yang memberikan perlindungan terhadap serangan siber, termasuk kerugian finansial yang diakibatkan oleh serangan siber tersebut.[27]

Selajutnya, serangan siber ini sebenarnya dapat dengan cepat ditindaklanjuti, apabila pemerintah membentuk lembaga pengawas PDP yang sebelumnya telah diamanatkan dalam UU PDP. Lembaga pengawas PDP menurut Pasal 60 UU PDP memiliki beberapa tugas pokok, yaitu merumuskan kebijakan perlindungan data pribadi, pengawasan terhadap instansi pengendali data pribadi, pemberian sanksi administratif, membantu APH dalam penegakan hukum pidana, bekerja sama dengan lembaga PDP negara lain, melakukan penilaian atas transfer PDP ke luar wilayah Indonesia, memberikan perintah kepada pengendali dan prosesor data pribadi, melakukan publikasi hasil pengawasan PDP, dan beberapa tugas pokok lainnya. Selain itu, Kemenkomdigi dan lembaga pengawas PDP dalam UU PDP, memiliki kedudukan yang berbeda. UU PDP mengkategorikan Kemenkomdigi sebagai suatu entitas publik dan menjadi salah satu subjek PDP, sehingga apabila kemudian dibentuk lembaga pengawas PDP, maka berdiri sebagai yang independen serta tidak di bawah koordinasi Kemenkomdigi. Ini disebabkan karena pada esensinya lembaga pengawas PDP adalah lembaga yang berwenang untuk mengawasi perlindungan data pribadi, apabila lembaga PDP di bawah koordinasi Kemenkomdigi, maka telah bertentangan dengan asas *nemo judex in causa sua,* yang mengharuskan seseorang tidak seharusnya mengawasi dirinya sendiri dalam hal ini Kemenkomdigi, karena dapat menimbulkan potensi *conflict of interest.*[28]

2. Insiden Pusat Data Nasional Sebagai Bukti Lemahnya Komitmen Terhadap Keamanan Siber

Ransomware menjadi salah satu bentuk serangan siber yang kerap menimbulkan kegaduhan di Indonesia. *Ransomware* sendiri adalah jenis *malware* (perangkat lunak

[26] BBC Indonesia, "Petinggi Kominfo mundur 'sebagai tanggung jawab moral' setelah Pusat Data Nasional diretas", https://www.bbc.com/indonesia/articles/c8vdmymmynzo (diakses pada 17 Mei 2025).
[27] BCA Insurance, "Asuransi Siber Pribadi (Personal Cyber Insurance)", https://bcainsurance.co.id/product/detail/asuransi-siber-pribadi-personal-cyber-insurance (diakses pada 17 Mei 2025).
[28] Juan Matheus dan Ariawan Gunadi, "Pembentukan Lembaga Pengawas Perlindungan Data Pribadi Di Era Ekonomi Digital : Kajian Perbandingan Dengan KPPU", *Jurnal Justisi* 10, no. 1, (2024): 20-35.

berbahaya) yang digunakan untuk menyandera aset korban, seperti dokumen, sistem, ataupun perangkat. Setelah aset terenkripsi, korban akan diminta membayar tebusan untuk mendekripsi dan kembali mendapatkan akses pada aset. *Ransomware* menargetkan individu, perusahaan, organisasi, bahkan pemerintah. Dampak dari *ransomware* dapat berupa kehilangan akses terhadap data, kerugian finansial, hingga penurunan reputasi.[29] Tidak berlebihan untuk mengatakan, bahwa imbas dari serangan *ransomware* sebagai malapetaka besar (*major havoc*) bagi korbannya.[30] Sebelum serangan terhadap PDNS, dalam beberapa tahun terakhir terdapat pelbagai serangan *ransomware* yang menarik perhatian publik sebagaimana dapat dilihat dalam ikhtisar berikut:[31]

Serangan *ransomware* pada PDNS menjadi yang terbesar, berdasarkan dampak yang ditimbulkannya pada layanan pemerintahan.

PDN hadir sebagai konsekuensi logis terbitnya Perpres Nomor 95 Tahun 2018, Perpres yang menjadi payung hukum SPBE ini secara eksplisit dalam Pasal 27 ayat (2) menyebutkan bahwa PDN merupakan satu dari tiga infrastruktur SPBE Nasional. Dalam lampiran Perpres *a quo* diuraikan lebih lanjut mengenai penyediaan PDN tersebut. Pertama, PDN merupakan fasilitas yang digunakan untuk penempatan, penyimpanan, pengolahan, dan pemulihan data bagi instansi pusat dan pemerintah daerah. Kedua, penyediaan PDN ditujukan untuk memberikan kemudahan bagi instansi pusat dan pemerintah daerah untuk mendapatkan layanan pusat data dan meningkatkan efisiensi

Tabel 2. Rekapitulasi Serangan *Ransomware* Tahun 2022-2024

Tahun	Target Serangan	Konteks
2022	Air Asia	Geng hacker Daixin mengenkripsi 5 juta data pegawai dan pengguna maskapai Air Asia.
2022	BI (Bank Indonesia)	16 Komputer BI Bengkulu diserang Conti ransomware.
2022	PGN (Perusahaan Gas Negara)	Geng Hive ransomware mengklaim telah berhasil melakukan serangan pada PGN. Menyebabkan *website* PGN sempat tidak bisa diakses.
2023	BSI (Bank Syariah Indonesia)	BSI terkena serangan ransomware LockBit. Layanan sempat terganggu, dan data nasabah bocor di *darkweb*.
2023	OJK (Otoritas Jasa Keuangan)	OJK diserang ransomware, layanan sistem informasi sempat tidak bisa diakses.
2024	KAI (Kereta Api Indonesia)	Ransomware Stormous berhasil meretas sistem KAI dengan kredensial karyawan melalui akses VPN.
2024	PDN (Pusat Data Nasional)	Ransomware BrainChiper menjebol PDN yang berimbas pada ratusan instansi pemerintahan.

Sumber: Katadata.co.id

29 BSSN, *Op. Cit*, hlm. 28.

30 Timothy MCintosh, et.all, "Ransomware Reloaded: Re-Examining Its Tren, Research and Mitigation in the Era of Data Exfiltration," *ACM Computing Surveys* 57, no. 1 (2024): 2.

31 Katadata, "Daftar Panjang Kerugian Serangan Ransomware di Indonesia," https://katadata.co.id/analisisdata/668cf48a48836/daftar-panjang-kerugian-serangan-ransomware-di-indonesia (diakses 6 Mei 2025).

biaya melalui pemanfaatan bersama PDN oleh instansi pusat dan pemerintah daerah. Ketiga, PDN dapat dilakukan dengan memprioritaskan pemanfaatan pusat data yang telah tersedia di instansi pusat dan pemerintah daerah dan yang memenuhi standar pusat data. Keempat, PDN diarahkan menggunakan teknologi komputasi awan sehingga bagi pakai data, aplikasi, dan infrastruktur dapat dilakukan. Perpres ini juga mengamanahkan pada Kemenkominfo sebagai penanggungjawab penyediaan PDN.

Lemahnya manajemen pengamanan seperti upaya mitigasi menjadi faktor utama penyebab insiden PDNS. Misalnya ketiadaan cadangan penyimpanan data, sebagaimana yang diungkapkan oleh Ketua BSSN Hinsa Siburian dalam rapat kerja dengan Komisi I DPR pasca serangan terjadi.[32] Hal tersebut sejalan dengan rumusan Pasal 40 ayat (4) Perpres Nomor 95 Tahun 2018 yang menjelaskan bahwa penyediaan cadangan dan pemulihan menjadi suatu yang harus dilakukan dalam penjaminan ketersediaan SPBE. Ketentuan tersebut diperkuat lagi melalui Pasal 24 huruf a Peraturan BSSN Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintah Berbasis Elektronik (Peraturan BSSN Nomor 4 Tahun 2021), terpenuhinya aspek ketersediaan SPBE salah satunya dengan menerapkan sistem pencadangan secara berkala. Belum sepenuhnya mengaplikasikan standar internasional keamanan siber seperti yang diakomodir melalui ISO *International Organization for Standardization* 27001 (ISO 27001) merupakan fakta yang menunjukkan bahwa infrastruktur pengamanan siber pada PDN dan PDNS belum secara matang dirancang.[33] Sejatinya keamanan dan keandalan dalam pelayanan publik berfungsi untuk menjaga serta mempertahankan kepercayaan masyarakat terhadap pemerintahan.[34]

Penyelesaian dan pertanggungjawaban atas serangan yang menargetkan PDNS ini, masih menimbulkan pertanyaan karena minimnya transparansi dan akuntabilitas dalam penanganannya. Mulai dari bagaimana tindak lanjut dan pertanggungjawaban atas kegagalan perlindungan data pribadi warga negara oleh kemenkominfo selaku pengendali data pribadi, sebagaimana yang ditegaskan dalam Pasal 47 UU PDP yang menyatakan pengendali data pribadi wajib bertanggungjawab atas pemrosesan data pribadi dan menunjukkan pertanggungjawaban dalam pemenuhan kewajiban pelaksanaan prinsip perlindungan data pribadi. Penanganan dalam pemulihan PDNS juga menjadi suatu hal yang masih menjadi misteri. Karena pada tanggal 1 Juli 2024 atau 11 hari setelah serangan dilancarkan peretas mengumumkan akan memberi kunci untuk membuka dekripsi data PDNS yang terenskripsi tersebut secara cuma-cuma pada tanggal 3 Juli 2024. Dari klaim Kemenkominfo, kunci yang diberikan berhasil digunakan untuk pemulihan data PDNS. Namun yang menjadi persoalan, tidak ada jaminan bahwa data yang telah diretas tidak disalahgunakan terlebih dahulu. Kemudian, apakah kunci yang diberikan

---

32 Kompas, "PDN Lumpuh, BSSN Ungkap Tak Ada "Backup" Data Jadi Masalah Utama," https://www.kompas.id/baca/polhuk/2024/06/27/pdn-lumpuh-bssn-ungkap-tak-ada-backup-data-jadi-masalah-utama?open_from=Tagar_Page (diakses pada 7 Mei 2025).

33 Aryojati Ardipandanto, *Op. Cit*: 7.

34 Pedro Robles and Daniel J. Mallinson, "Artificial Intelligence Technology, Public Trust, and Effective Governance," *Review of Policy Research* 42, no. 1 (2023): 12.

benar-benar berfungsi untuk memulihkan PDNS secara maksimal dan apakah dapat dipastikan kunci dekripsi bebas dari *malware* berbahaya.[35] Pasalnya pemberian kunci dekripsi secara gratis merupakan fenomena yang tidak biasa dalam modus serangan siber berjenis *ransomware,* terlepas dari alasan yang disampaikan pihak Brain Chiper dalam kasus ini.

3. Urgensi Reformasi Kebijakan dan Regulasi Keamanan Siber

Dalam era digital yang ditandai oleh ketergantungan terhadap teknologi informasi dan komunikasi, keamanan siber telah menjadi isu strategis nasional yang tak terelakkan. Perkembangan teknologi tidak hanya membawa kemudahan dan efisiensi,[36] tetapi juga memunculkan berbagai kerentanan dan risiko yang mengancam kedaulatan negara, hak-hak konstitusional warga negara, serta stabilitas sektor publik dan privat.[37] Namun, ironisnya, tata kelola keamanan siber di Indonesia hingga saat ini masih menunjukkan gejala keterlambatan regulatif, kelemahan institusional, serta fragmentasi kebijakan yang tidak selaras dengan prinsip-prinsip negara hukum modern. Evolusi pemikiran hukum modern memperlihatkan bahwa konsep negara hukum di tradisi Eropa Kontinental dirumuskan secara sistematis oleh sejumlah pemikir besar, seperti Immanuel Kant, Paul Laband, Julius Stahl, dan Johann Gottlieb Fichte, dengan menggunakan terminologi khas Jerman, yakni *Rechtsstaat.* Sementara itu, dalam tradisi Anglo-Amerika, gagasan serupa memperoleh artikulasinya melalui pemikiran A.V. Dicey yang memperkenalkan konsep *The Rule of Law* sebagai dasar penyelenggaraan negara. Lebih jauh, Julius Stahl mengartikulasikan gagasan *Rechtsstaat* sebagai suatu konstruksi normatif mengenai negara hukum yang bertumpu pada empat prinsip utama, yakni:[38]

1. Perlindungan hak asasi manusia.
2. Pembagian kekuasaan.
3. Pemerintahan berdasarkan undang-undang.
4. Peradilan tata usaha Negara.

Sementara itu, A.V. Dicey mengelaborasikan konsep *Rule of Law* melalui tiga karakteristik fundamental yang menjadi elemen konstitutif dari setiap negara hukum, yaitu:[39]

1. *Supremacy of Law.*
2. *Equality before the law.*
3. *Due Process of Law.*

Keempat prinsip *rechtsstaat* yang digagas oleh Julius Stahl, pada hakikatnya, dapat dipadukan dengan tiga karakteristik *Rule of Law* yang dirumuskan oleh A.V. Dicey untuk menegaskan atribut fundamental dari suatu negara hukum modern. Sintesis konseptual ini memperlihatkan bahwa perkembangan negara hukum kontemporer meniscayakan integrasi antara perlindungan hak asasi

---

35 Kompas, "Kronologi Serangan Ransomware ke PDN dan Penanganannya yang Tak Kunjung Usai," https://tekno.kompas.com/read/2024/07/10/12350077/kronologi-serangan-ransomware-ke-pdn-dan-penanganannya-yang-tak-kunjung-usai#google_vignette (diakses pada 8 Mei 2025).

36 Nolin, Jan, and Nasrine Olson. "The Internet of Things and convenience." *Internet Research* 26, no. 2 (2016): 361.

37 Reveron, Derek S., ed. *Cyberspace and national security: threats, opportunities, and power in a virtual world*. (Washington: Georgetown University Press, 2012), hlm. 229.

38 Jimly Asshiddiqie. "Gagasan negara hukum Indonesia." *Makalah Disampaikan dalam Forum Dialog Perencanaan Pembangunan Hukum Nasional yang Diselenggarakan oleh Badan Pembinaan Hukum Nasional Kementerian Hukum dan*, vol. 1. (2011): 2.

39 *Ibid.*

manusia, pembatasan kekuasaan melalui mekanisme *checks and balances,* supremasi hukum, persamaan kedudukan di hadapan hukum, serta jaminan proses hukum yang adil. Lebih lanjut, *The International Commission of Jurists* memperluas konstruksi tersebut dengan menambahkan prinsip mengenai independensi serta imparsialitas kekuasaan kehakiman, yang dewasa ini dipandang sebagai *conditio sine qua non* bagi tegaknya demokrasi konstitusional dan keberlangsungan sistem negara hukum itu sendiri.[40] Oleh karena itu, urgensi reformasi kebijakan dan regulasi keamanan siber tidak semata-mata sebagai respons administratif, melainkan merupakan keharusan konstitusional dalam mewujudkan sistem perlindungan hukum yang menyeluruh, adil, dan menjamin hak-hak fundamental warga negara dalam ruang digital.

Secara normatif, konstitusi melalui Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD NRI 1945) menjamin hak setiap orang atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda. Jaminan ini mencakup pula dimensi digital yang kini menjadi perpanjangan eksistensi manusia modern. Namun, lemahnya perangkat regulasi siber telah menyebabkan terjadinya pelanggaran privasi, pencurian data, manipulasi informasi,[41] serta serangan siber terhadap infrastruktur kritikal negara yang tidak mendapatkan respons hukum yang tegas dan sistemik. Alih-alih menata regulasi yang berbasis hak dan akuntabilitas, negara justru terjebak dalam pendekatan otoriteristik melalui model-model pengawasan siber yang mengorbankan prinsip proporsionalitas dan akuntabilitas publik.

Ketiadaan UU Ketahanan dan Keamanan Siber merupakan *problem* yuridis fundamental dalam sistem hukum Indonesia. Fragmentasi pengaturan dalam UU ITE, UU PDP, serta regulasi teknis BSSN telah melahirkan disharmoni normatif, ketidakpastian hukum, serta tumpang tindih kewenangan institusional dalam menghadapi ancaman siber. Padahal, dalam rezim hukum tata negara modern, mensyaratkan prinsip supremasi hukum *(rule of law),* menuntut adanya kepastian hukum *(legal certainty),* kesatuan regulasi *(regulatory coherence),* dan perlindungan hak-hak sipil yang efektif *(effective enforcement).* Ketika serangan siber dikonstruksikan sebagai ancaman terhadap keamanan nasional, negara tidak boleh menjadikan keamanan sebagai justifikasi untuk mengesampingkan prinsip demokrasi dan konstitusionalitas. Model internasional yang memberi kewenangan luas pada lembaga siber tanpa kontrol demokratis tidak dapat diadopsi secara *acritis,* terlebih di tengah lemahnya mekanisme *checks and balances* dalam sektor keamanan Indonesia. Pengalaman dalam UU ITE menjadi preseden buruk tentang bagaimana legislasi dapat melahirkan pasal karet yang mengekang kebebasan berekspresi.

Di tengah transformasi digital global melalui kecerdasan buatan (AI), *internet of things (IoT)*, dan *big data* telah menciptakan lanskap baru dalam arena pertahanan negara yang tidak hanya bergantung pada kekuatan militer fisik, tetapi juga kapasitas digital nasional.[42] Negara-

40 *Ibid.*

41 Parulian, Sahat, Devi Anassafila Pratiwi, and Meiliya Cahya Yustina. "Studi tentang ancaman dan solusi serangan siber di indonesia." *Telecommunications, Networks, Electronics, and Computer Technologies (TELNECT)* 1, no. 2 (2021): 86.

42 Goundar, Sam, Archana Purwar, and Ajmer Singh, eds. *Applications of artificial intelligence, big data and internet of things in sustainable development.* (Boca Raton: CRC Press, 2022), hlm 2.

negara maju telah mereformasi kerangka hukum keamanan siber mereka dengan prinsip partisipatif, transparansi, dan akuntabilitas. Sebagai negara hukum yang berdasarkan Pancasila, Indonesia wajib membangun regulasi siber yang tidak sekadar responsif terhadap perkembangan teknologi, tetapi juga berakar pada mandat konstitusional untuk melindungi seluruh warga negara, termasuk dalam domain digital.

Di sisi lain, Lembaga seperti BSSN harus didukung oleh legitimasi hukum yang tegas namun tetap tunduk pada kontrol demokratis dan prinsip proporsionalitas.[43] UU Ketahanan dan Keamanan Siber ke depan harus secara limitatif mengatur kewenangan akses, penyimpanan, dan intersepsi data digital warga negara. Tanpa batasan regulasi yang tegas, terdapat risiko besar terjadinya praktik siber otoritarianisme yang bertentangan dengan nilai-nilai negara hukum dan demokrasi konstitusional.

Selanjutnya, reformasi kebijakan siber juga harus mengedepankan partisipasi publik dan prinsip keterbukaan *(open governance) s*ebagai entitas yang terdampak langsung oleh kebijakan digital, masyarakat sipil, komunitas teknologi, dan sektor privat harus dilibatkan dalam penyusunan kebijakan siber. Ini bukan semata-mata isu administratif, tetapi soal legitimasi hukum. Dalam paradigma demokrasi konstitusional, legitimasi regulasi diperoleh bukan hanya dari prosedur legislasi formal, melainkan dari proses deliberatif yang menjamin keterlibatan seluruh elemen masyarakat. Dengan demikian, hukum keamanan siber tidak akan menjadi alat represi negara, tetapi justru menjadi mekanisme perlindungan warga.

Secara garis besar, reformasi kebijakan dan regulasi keamanan siber di Indonesia harus diarahkan pada lima aspek utama yaitu (1) Pembentukan UU Keamanan dan Ketahanan Siber berbasis HAM, dan menjamin supremasi hukum, dipilih sebagai agenda prioritas karena hingga saat ini kerangka regulasi yang ada masih bersifat parsial, fragmentaris, dan sering kali tidak mengikat dalam konteks perlindungan hak-hak fundamental sehingga pembentukan regulasi yang komprehensif akan memberikan landasan yuridis yang kokoh, memastikan adanya kepastian hukum, serta menjawab kebutuhan mendesak untuk mengintegrasikan keamanan nasional dengan penghormatan terhadap hak-hak digital; (2) Harmonisasi peraturan sektoral yang saling tumpang tindih agar tidak menciptakan dualisme otoritas dan konflik kewenangan, sebagai jawaban atas kondisi hiper-produksi regulasi di Indonesia di mana terdapat tumpang tindih antara kewenangan BSSN, Kominfo, Polri, bahkan BIN dalam konteks siber yang berimplikasi pada inkoherensi kebijakan, inkonsistensi norma, dan potensi *abuse of power* akibat absennya delineasi kewenangan yang jelas sehingga harmonisasi menjadi kebutuhan mendesak untuk memastikan adanya tata kelola hukum yang konsisten, efisien, serta selaras dengan prinsip *good regulatory governance;* (3) Penguatan mekanisme pengawasan demokratis terhadap lembaga-lembaga yang memiliki otoritas siber, termasuk melalui audit hukum

[43] Chotimah, H.C. "Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]." *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional* 10, no. 2 (2019): 116.

dan pengawasan parlemen. Aspek yang dipilih untuk menghindari lahirnya rezim otoriter digital karena regulasi siber yang tidak diawasi secara ketat berpotensi melahirkan instrumen kontrol negara terhadap kebebasan sipil sehingga mekanisme pengawasan, baik dalam bentuk audit maupun pengawasan parlemen, menjadi instrumen esensial untuk menjaga akuntabilitas, transparansi, serta mencegah konsentrasi kekuasaan yang eksesif; (4) Pelibatan masyarakat sipil dan multi-pemangku kepentingan dalam setiap proses legislasi dan kebijakan. Dengan pertimbangan bahwa isu keamanan siber memiliki kompleksitas multidimensional yang tidak dapat diselesaikan secara *top-down* oleh negara semata, sehingga keterlibatan aktor non-negara baik akademisi, sektor swasta, maupun organisasi masyarakat sipil menjadi krusial untuk memastikan legitimasi demokratis dalam setiap produk hukum serta memperkuat basis sosial dari kebijakan yang dihasilkan, sejalan dengan prinsip partisipasi publik sebagai salah satu indikator *good governance* yang diakui secara internasional; serta (5) Perlindungan terhadap hak-hak digital warga negara secara eksplisit, khususnya dalam perlindungan data pribadi, privasi digital, dan kebebasan berinformasi. Menjadi landasan utama karena esensi negara hukum pada akhirnya terletak pada jaminan terhadap hak-hak warganya, termasuk hak atas privasi, perlindungan data pribadi, serta kebebasan berinformasi. Aspek ini semakin menguat seiring dengan meningkatnya ancaman pelanggaran data pribadi, penyalahgunaan *Artificial Intelligence*, dan praktik pengawasan digital yang berpotensi menggerus kebebasan sipil di ruang siber. Dengan mengintegrasikan perlindungan hak-hak digital ke dalam kerangka hukum nasional, negara tidak hanya menegaskan kewajibannya sebagai *duty bearer* dalam perspektif HAM, tetapi juga memastikan bahwa ruang digital tetap terjaga sebagai arena yang inklusif, adil, dan demokratis.

1) Perbandingan Internasional Kebijakan dan Regulasi Keamanan Siber

Di tengah revolusi industri 4.0 dan dominasi infrastruktur digital dalam seluruh aspek kehidupan, keamanan siber tidak lagi dapat diposisikan sebagai isu teknis belaka, melainkan telah menjelma menjadi persoalan struktural dalam sistem pemerintahan modern. Ketergantungan pada teknologi digital telah bergerak menuju *hiper-konektivitas* dimana telah meluaskan cakupan ancaman siber, yang kini mencakup aspek strategis seperti kedaulatan negara, keamanan nasional, perlindungan data pribadi, hingga integritas demokrasi elektoral.[44] Akibatnya, pendekatan terhadap isu ini haruslah bersifat konstitusional, demokratis, dan sesuai dengan prinsip negara hukum, tidak cukup jika hanya didekati melalui paradigma teknokratis dan administratif.

Di Indonesia, ketiadaan satu kerangka hukum nasional yang komprehensif dan visioner dalam tata kelola keamanan siber merupakan cacat yuridis yang menghambat pembentukan rezim hukum yang kohesif. Fragmentasi regulasi antara UU ITE, UU PDP, dan regulasi sektoral lainnya telah menimbulkan tumpang tindih kewenangan, lemahnya otoritas koordinasi, serta absennya standar minimum perlindungan terhadap hak-hak sipil dalam ruang digital. Konsekuensinya, kebijakan keamanan siber yang diambil kerap berjalan secara sektoral dan reaktif, bahkan dalam beberapa hal justru

[44] Aliane, Nadir, and Saima Jamil. "Human Side of Digital Transformation: Hyper Connectedness and Collaboration." *International Journal of Operations and Quantitative Management* 29, no. 1 (2023): 318.

bertentangan dengan prinsip-prinsip hak asasi manusia seperti hak atas privasi dan kebebasan berekspresi.

Dari perspektif perbandingan hukum, model *Anglo-Saxon* seperti Amerika Serikat menunjukkan pentingnya supremasi hukum dan akuntabilitas horizontal dalam tata kelola keamanan siber, di mana lembaga pengawas independen memainkan peran penting sebagai penjaga hak sipil dalam menghadapi otoritas negara. Sementara itu, negara dengan sistem *Civil Law* seperti Prancis dan Jerman mengedepankan kepastian hukum melalui kodifikasi, meskipun kerap lambat dalam menyesuaikan dengan dinamika teknologi yang disruptif. Sebaliknya, pendekatan Nordik menunjukkan signifikansi tata kelola kolaboratif antara negara, sektor swasta, dan masyarakat sipil, yang tidak hanya memperkuat ketahanan siber nasional, tetapi juga menjamin transparansi serta partisipasi publik secara luas.[45]

Secara konseptual, arsitektur hukum keamanan siber harus didasarkan pada tiga pilar konstitusional yaitu perlindungan infrastruktur vital, penguatan kedaulatan digital, dan penghormatan terhadap hak konstitusional warga negara.[46] Ketiga pilar tersebut harus menjadi basis dalam pembentukan sistem hukum yang tidak hanya bersifat responsif terhadap insiden, tetapi juga preventif, adaptif, dan tanggap terhadap kompleksitas risiko multidimensional di ruang digital. Ketiadaan payung hukum dalam hal ini telah menjadi titik lemah mendasar Indonesia dalam membangun ketahanan siber nasional yang berkeadilan.

Dalam merumuskan reformasi hukum keamanan siber ke depan, penting bagi Indonesia untuk mengadopsi model yang sesuai dengan karakteristik sistem hukum nasional, tanpa mengabaikan praktik internasional yang telah teruji efektivitasnya. Pendekatan komparatif ini juga penting dalam rangka harmonisasi regulasi siber Indonesia dengan standar internasional, terutama ketika menyangkut kerja sama lintas batas negara, transfer data, dan penegakan hukum terhadap kejahatan siber transnasional. Tabel di bawah ini akan memberikan gambaran perbandingan kebijakan dan regulasi keamanan siber dari empat negara, yakni Amerika Serikat, Uni Eropa, Tiongkok, dan Singapura sebagai berikut:

Tabel 3. Perbandingan Internasional Kebijakan dan Regulasi Keamanan Siber

Negara	Instrumen Hukum	Pendekatan Regulasi	Ciri Kelembagaan	Prinsip Hukum yang Dominan	Relevansi Bagi Indonesia
Amerika Serikat	Cybersecurity Act, *National Institute of Standards and Technology* (NIST) Framework, Executive Orders	Berbasis sektor dan voluntary compliance	Terde-sentralisasi: lembaga federal dan negara bagian	Perlindungan privasi, prinsip kehati-hatian *(due diligence)*	Kelebihan : Fleksibel, berbasis risiko Kekurangan: Fragmentasi pengaturan Relevansi: Relevan untuk mengembangkan standar minimum teknis tanpa over-regulasi

[45] Noang, Edmondus Iswenyo. "Jaga Diri di Baltik." *Global Political Studies Journal* 6, no. 1 (2022): 27.
[46] Gani, Taufiq A. *Kedaulatan data digital untuk integritas bangsa*. (Aceh: Syiah Kuala University Press, 2023), hlm 23.

Uni Eropa (UE)	NIS Directive, *General Data Protection Regulation (*GDPR) Cybersecurity Act 2019	Terintegrasi dan berbasis HAM	*European Union Agency for Cybersecurity* (ENISA) sebagai badan koordinasi	*Rule of Law*, subsidiaritas, perlindungan data	Kelebihan: Menekankan HAM & transparansi Kekurangan: Kompleksitas implementasi antar negara anggota Relevansi: Cocok sebagai rujukan perlindungan hak digital warga
Tiongkok	Cybersecurity Law (2017), Data Security Law (2021), Personal Information Protection Law (2021)	Sentralistik dan represif	Dikuasai langsung oleh negara & partai	Keamanan nasional, supremasi negara	Kelebihan: Tangguh dalam kontrol Kekurangan: Melanggar prinsip privasi dan kebebasan digital Relevansi: Tidak cocok untuk negara demokratis seperti Indonesia
Singapura	Cybersecurity Act (2018), Personal Data Protection Act (PDPA)	Sentralistik namun akuntabel	CSA (*Cyber Security Agency*) sebagai otoritas tunggal	Efisiensi, keamanan nasional, proporsionalitas	Kelebihan: Efisien dan terkoordinasi Kekurangan: Rentan minim partisipasi publik Relevansi Model otoritas tunggal relevan jika diawasi parlemen

Sumber : Diolah dari berbagai sumber

Pemilihan Amerika Serikat, Uni Eropa, Tiongkok, dan Singapura sebagai obyek perbandingan dalam kajian kebijakan dan regulasi keamanan siber sebagaimana dalam tabel diatas didasarkan pada pertimbangan metodologis dan substansial. Secara metodologis, perbandingan lintas sistem hukum bukan dimaksudkan untuk mengadopsi secara utuh model yang ada, melainkan untuk menggali prinsip-prinsip normatif, instrumen kelembagaan, dan pola kebijakan yang dapat dijadikan *reference points* dalam pembentukan kerangka hukum nasional. Tradisi *comparative law* sendiri menekankan bahwa perbandingan tidak semata-mata dilakukan antar sistem hukum yang identik, tetapi justru menemukan nilai, pendekatan, maupun praktik terbaik dari yurisdiksi yang berbeda untuk memperkaya diskursus reformasi hukum.[47] Secara substansial, masing-masing yurisdiksi tersebut mewakili tipologi kebijakan keamanan siber global yang beragam dan relevan untuk dipelajari, sehingga membandingkan keempat yurisdiksi tersebut dapat diperoleh spektrum yang luas dari model *cyber governance* global dari model liberal-demokratis berbasis hak, ke model otoritarian-sentralistis, hingga model hibrid yang adaptif terhadap konteks lokal. Spektrum ini menjadi penting bagi Indonesia yang tengah berupaya merumuskan kerangka hukum keamanan siber

[47] Ratno Lukito. ""Compare But Not to Compare": Kajian Perbandingan Hukum di Indonesia." *Undang: Jurnal Hukum* 5, no. 2 (2022): 261.

yang responsif terhadap ancaman global, namun tetap berakar pada prinsip negara hukum dan nilai-nilai demokrasi konstitusional.

Lebih lanjut, tabel diatas menunjukkan bagaimana berbagai negara merespons kompleksitas ancaman digital dengan pendekatan hukum dan kebijakan yang mencerminkan sistem ketatanegaraan dan prinsip konstitusional masing-masing. Amerika Serikat, misalnya, mengambil pendekatan desentralistik namun terkoordinasi, dengan pembentukan lembaga khusus seperti *Cybersecurity and Infrastructure Security Agency (CISA)* di bawah *Department of Homeland Security.*[48] Di sisi lain, Uni Eropa memilih pendekatan harmonisasi hukum antarnegara anggota melalui *Network and Information Security (NIS) Directive dan General Data Protection Regulation (GDPR)* sebagai pilar utama tata kelola siber.[49] Pendekatan UE menunjukkan integrasi ideal antara keamanan nasional dan penghormatan terhadap prinsip negara hukum serta demokrasi partisipatif.[50]

Tiongkok menampilkan pendekatan yang lebih otoriter dan sentralistik, dengan pengendalian kuat dari negara terhadap ruang siber.[51] Sementara itu, Singapura mengadopsi model teknokratik melalui *Cybersecurity Act 2018.* Negara ini memberikan kewenangan luas kepada *Cyber Security Agency of Singapore (CSA)* sebagai otoritas tunggal dalam menangani ancaman siber. Meskipun efektif secara teknis dan operasional, pendekatan ini rentan terhadap kekurangan mekanisme pengawasan yang seimbang, sehingga menimbulkan kekhawatiran terhadap potensi pelanggaran hak dan kebebasan sipil.[52] Secara hukum, model Singapura mencerminkan pendekatan sentralistik yang lebih menitikberatkan pada efisiensi ketimbang akuntabilitas institusional.

Berbeda jauh dari negara-negara sebelumnya, Tiongkok menerapkan pendekatan yang sangat terpusat dan otoriter melalui *Cybersecurity Law 2017* yang berlandaskan pada prinsip *cyber sovereignty.*[53] Negara memiliki kendali penuh terhadap arus data, konten digital, dan aktivitas daring warga negaranya. Pendekatan ini secara hukum dapat dikritik sebagai bentuk *legal authoritarianism,* di mana hukum tidak berfungsi sebagai pelindung hak, melainkan sebagai instrumen penguatan kekuasaan negara. Dalam tataran negara hukum yang demokratis, model ini tidak sesuai karena mengabaikan prinsip *due process, checks and balances,* serta perlindungan hak asasi manusia.

Jika dikaitkan dalam tataran Indonesia, maka dapat disimpulkan bahwa Indonesia belum memiliki kerangka hukum keamanan

---

48 Lanz, Zachary. "Cybersecurity risk in US critical infrastructure: An analysis of publicly available US government alerts and advisories." *International Journal of Cybersecurity Intelligence & Cybercrime* 5, no. 1 (2022): 43.

49 Garg, Himani, M. Balasubramaniam, Ajay Kr Gupta, and Jitendra Singh. "'NIS'a Network Investigation System." In *Proceedings of Emerging Trends and Technologies on Intelligent Systems: ETTIS 2021*. (Singapore: Springer Nature, 2022): 251.

50 Markopoulou, Dimitra, Vagelis Papakonstantinou, and Paul De Hert. "The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation." *Computer Law & Security Review* 35, no. 6 (2019): 2.

51 Xu, Zonghuang, and Jin Shi. "Research on the national security risk assessment model: a case study of political security in China." *Humanities and Social Sciences Communications* 12, no. 1 (2025): 5.

52 Adma, Arinaldo, Yusuf Marsel Surbakti, and Puspita Sari. "Transformasi Sistem Pertahanan Siber Indonesia dengan BSSN Sebagai Poros & Motor Penggerak Menuju Angkatan Siber Mandiri di Masa Depan." *Jurnal Kajian Stratejik Ketahanan Nasional* 6, no. 1 (2023): 4.

53 Standing Committee of the National People's Congress, *Cybersecurity Law of the People's Republic of China*, adopted November 7, 2016, effective June 1, (2017).

siber yang utuh, komprehensif, dan berbasis prinsip konstitusional. Regulasi yang ada seperti UU ITE, UU PDP, dan PP PSTE hanya mengatur secara parsial, sementara peran BSSN sebagai otoritas teknis belum dibingkai dalam Undang-Undang yang memiliki legitimasi hukum tinggi. Banyak praktik pengaturan konten dan pemutusan akses oleh negara dilakukan tanpa mekanisme keberatan *(legal remedy),* tanpa pengawasan yudisial, dan seringkali tanpa transparansi. Hal ini menimbulkan persoalan serius dalam perspektif hukum tata negara karena bertentangan dengan prinsip *due process of law* dan jaminan hak konstitusional warga negara sebagaimana diatur dalam Pasal 28F dan 28G UUD NRI 1945.

Dari perbandingan ini, tampak jelas bahwa urgensi reformasi kebijakan dan regulasi keamanan siber di Indonesia tidak hanya mendesak dari sisi teknis, tetapi lebih penting dari sisi yuridis dan konstitusional. Negara perlu segera merumuskan UU Keamanan dan Ketahanan Siber yang berbasis prinsip negara hukum, menjamin hak asasi manusia digital, memperjelas struktur kelembagaan dan kewenangan otoritas, serta menyusun mekanisme *checks and balances* yang dapat mencegah penyalahgunaan kekuasaan di ruang digital. Selain itu, reformasi regulasi harus menjamin keterlibatan publik, akuntabilitas lembaga, dan ruang partisipasi bagi masyarakat sipil dalam pengambilan kebijakan siber nasional. Dengan demikian, Indonesia dapat membangun sistem keamanan siber yang tidak hanya kuat dalam menangkal serangan digital, tetapi juga kokoh secara konstitusional dan demokratis.

2) Model Reformasi Kebijakan dan Regulasi Keamanan Siber

a. Urgensi Pembentukan UU Keamanan dan Ketahanan Siber

Keamanan siber telah menjadi isu strategis nasional yang semakin signifikan seiring dengan ketergantungan Indonesia terhadap teknologi digital dalam penyelenggaraan pemerintahan, pelayanan publik, dan kegiatan ekonomi. Namun demikian, kompleksitas ancaman siber yang semakin canggih tidak diimbangi oleh kerangka hukum yang kokoh, komprehensif, dan terintegrasi. Hingga saat ini, Indonesia masih belum memiliki Undang-Undang khusus mengenai keamanan siber dan hal ini menjadi titik lemah serius dalam sistem pertahanan dan keamanan nasional. Keadaan ini mengancam tidak hanya keamanan informasi strategis negara, tetapi juga menimbulkan risiko pelanggaran hak konstitusional warga negara atas privasi dan perlindungan data pribadi.

Dari perspektif teori hukum administrasi negara, setiap tindakan pemerintah harus berlandaskan pada peraturan perundang-undangan atau dalam nomenklatur Belanda dikenal dengan *"het beginsel van wetmatigheid van bestuur"*[54] yang dapat menjadi basis hukum dalam melakukan tindakan administratif dan represif terhadap serangan atau kejahatan siber. Oleh karena itu, dalam menjalankan fungsi pelayanan publik, setiap aparatur pemerintahan wajib tunduk dan taat pada hukum. Ketundukan ini penting agar penyelenggaraan kekuasaan negara tidak menyimpang sebagaimana dikemukakan oleh Lord Acton: *"Power tends to corrupt, but absolute power corrupts absolutely."* Implikasi dari prinsip tersebut menegaskan bahwa Negara Indonesia sebagai

[54] Ridwan, H. R. "Hukum administrasi negara." (Jakarta : RajaGrafindo Persada, 2006), hlm. 91.

negara hukum harus dapat membahagiakan rakyatnya, konsekuensinya, dapat diperhatikan dampak-dampak tanggung jawab negara dalam mewujudkan kesejahteraan rakyat semakin berkembang dan baru.[55] Dalam tataran ini, absennya UU Keamanan dan Ketahanan Siber mengakibatkan BSSN dan instansi terkait berada dalam posisi lemah karena tidak memiliki dasar hukum primer *(primary legislation)* dalam menjalankan fungsi strategisnya.

Serangan siber tidak lagi bersifat teknis semata, melainkan telah berevolusi menjadi alat geopolitik dan *warfare modern.* Keamanan siber hari ini merupakan bagian dari pertahanan negara yang tidak kalah penting dari pertahanan militer konvensional. Menurut prinsip *sovereign cybersecurity*, negara memiliki kedaulatan penuh untuk mengatur, mengontrol, dan melindungi infrastruktur siber nasional dari serangan pihak asing maupun aktor domestik yang bersifat *subversif.*[56] Namun, prinsip ini tidak dapat ditegakkan secara efektif tanpa fondasi hukum yang kokoh berupa undang-undang organik yang mengatur mekanisme preventif, mitigatif, dan represif dalam keamanan siber.

Pembentukan UU Keamanan dan Ketahanan Siber juga memiliki dimensi konstitusional yang berkaitan langsung dengan perlindungan hak asasi manusia di ruang digital. Dalam Pasal 28G dan 28J UUD NRI 1945 menjamin hak atas rasa aman dan perlindungan dari ancaman terhadap hak pribadi. Dalam era digital, hak ini mencakup perlindungan terhadap pencurian data pribadi, penyadapan ilegal, hingga disinformasi sistematis yang dapat merusak reputasi atau keamanan personal seseorang. Oleh karena itu, pembentukan UU Keamanan dan Ketahanan Siber harus diarahkan untuk menyeimbangkan antara perlindungan negara dari serangan siber dan perlindungan individu dari pelanggaran hak digital oleh negara atau entitas privat. Di sinilah pentingnya kontrol konstitusional terhadap upaya-upaya *surveillance* agar tidak menyimpang menjadi praktik otoritarianisme digital yang melanggar prinsip negara hukum demokratis.

Banyak negara telah lebih dahulu membentuk UU Keamanan dan Ketahanan Siber sebagai bagian dari strategi nasional. Misalnya, *Cybersecurity Act* di Uni Eropa, *Cybersecurity Law* di Tiongkok, dan *Cybersecurity and Infrastructure Security Agency Act* (CISA) di Amerika Serikat. Regulasi tersebut bukan hanya menetapkan kerangka kebijakan keamanan siber, tetapi juga mengatur struktur koordinasi, klasifikasi insiden, serta sanksi hukum yang jelas dan tegas. Indonesia dapat belajar dari prinsip-prinsip *good cyber governance* tersebut, antara lain:

a. *Clear legislative mandate* bagi lembaga pengelola siber;
b. Transparansi dan akuntabilitas dalam pelaksanaan kebijakan;
c. Partisipasi publik dalam perumusan kebijakan keamanan digital; dan
d. Penyeimbangan antara keamanan dan kebebasan sipil *(security-liberty balance).*

Dengan demikian, dalam era disrupsi digital dan intensifikasi ancaman siber lintas negara, urgensi pembentukan kerangka hukum yang kokoh dan komprehensif dalam bentuk

[55] Lord Acton, "Power tends to corrupt, and absolute power corrupts absolutely," in a letter to Bishop Mandell Creighton, April 3, 1887, as cited in Brian Martin, *Information Liberation: Challenging the Corruptions of Information Power* (London: Freedom Press, 1998), hlm. 1.

[56] Timmers, Paul. "Ethics of AI and cybersecurity when sovereignty is at stake." *Minds and Machines* 29, no. 4 (2019): 635.

UU Keamanan dan Ketahanan Siber menjadi keniscayaan yang tidak dapat ditunda. Negara berkewajiban melindungi segenap tumpah darah Indonesia, termasuk di dalamnya perlindungan terhadap ruang digital nasional yang menjadi medan baru bagi aktivitas ekonomi, politik, pertahanan dan hak-hak sipil warga negara. Oleh karena itu, dalam menyusun UU Keamanan dan Ketahanan Siber ke depan, diperlukan landasan *legal framework* yang tidak hanya menjawab kebutuhan teknokratis semata tetapi juga memenuhi prinsip-prinsip negara hukum, demokrasi, dan kedaulatan digital secara integral yang dapat dipaparkan dalam tabel berikut:

Tabel. *Legal Framework* dalam Menyusun UU Keamanan dan Ketahanan Siber

No.	Aspek/Substansi	Keterangan	Eksaminasi Normatif
1.	**Tujuan Regulasi**	Menyusun fondasi hukum keamanan siber yang menjamin stabilitas nasional dan perlindungan hak konstitusional warga negara dalam ruang digital.	Regulasi harus seimbang antara kepentingan nasional dan jaminan hak asasi manusia (HAM), menghindari *overregulasi* yang membatasi kebebasan berekspresi atau privasi digital.
2.	**Subjek dan Objek Hukum Siber**	Menentukan siapa yang tunduk (subjek) dan sistem/ infrastruktur apa yang dilindungi (objek) oleh UU Keamanan dan Ketahanan Siber.	Subjek tidak boleh dibatasi hanya pada instansi publik, tetapi juga entitas privat, dengan cakupan objek meliputi sistem elektronik kritis dan data strategis nasional.
3.	**Kewenangan Lembaga Koordinatif (BSSN)**	Menegaskan peran tunggal BSSN sebagai pemegang otoritas pusat dalam kebijakan keamanan siber.	Perlu dibentuk batasan hukum tegas agar tidak terjadi *excessive discretion* dan tumpang tindih dengan lembaga lain seperti Kominfo, Polri, atau TNI.
4.	**Standar Minimum Keamanan Siber**	Mewajibkan instansi pemerintah dan pelaku usaha menerapkan protokol keamanan siber sesuai standar minimum nasional.	Standar keamanan wajib berbasis best practices internasional (ISO/ IEC 27001)[57] dan wajib audit reguler untuk mencegah kelalaian sistemik.
5.	**Perlindungan Data dalam Infrastruktur Publik**	Menjamin pengelolaan dan pengamanan data warga negara dalam sistem elektronik milik negara.	UU Keamanan dan Ketahanan Siber harus selaras dan tidak kontradiktif dengan UU Perlindungan Data Pribadi, serta menghindari duplikasi pengaturan dan multitafsir yurisdiksi hukum.

[57] Masike Malatji. "Management of enterprise cyber security: A review of ISO/IEC 27001: 2022." Dalam *2023 International conference on cyber management and engineering (CyMaEn)*. IEEE, (2023): 117.

6.	**Pengaturan Lintas Negara dan Kerja Sama Internasional**	Memuat prinsip kerja sama siber bilateral dan multilateral, termasuk pengakuan mutual terhadap standardisasi keamanan antar negara.	Mengingat ancaman siber bersifat transnasional, perlu dasar hukum untuk menjalin *mutual legal assistance treaties* (MLAT) atau kerjasama G2G. Ini konsisten dengan prinsip *comitas gentium.*
7.	**Perlindungan Hak Asasi Manusia**	Menjamin bahwa keamanan siber tidak digunakan untuk membungkam hak kebebasan berekspresi dan hak atas privasi secara sewenang-wenang.	UU Keamanan dan Ketahanan Siber harus tunduk pada prinsip proporsionalitas dan legalitas dalam pembatasan hak konstitusional. Setiap pembatasan wajib diuji dengan uji kepatutan *(constitutional test).*[58]
8.	**Tata Kelola dan Akuntabilitas**	Menjamin mekanisme pengawasan, transparansi, dan akuntabilitas dalam pelaksanaan UU Keamanan dan Ketahanan Siber .	Diperlukan badan pengawas independen agar pelaksanaan undang-undang tidak melanggar prinsip *rule of law* dan *checks and balances.*
9.	**Sanksi dan Penegakan Hukum**	Menetapkan sanksi administratif, perdata, hingga pidana bagi pelanggaran keamanan siber secara proporsional dan terukur.	Sanksi harus mengacu pada prinsip *ultimum remedium* dan memperhatikan prinsip proporsionalitas, legalitas, serta perlindungan terhadap *whistleblower*[59] dan *hacker etis.*
10	**Kedaulatan Digital dan Strategi Nasional**	Mewujudkan kedaulatan digital melalui regulasi yang melindungi infrastruktur nasional dari ancaman global dan intervensi asing.	Harus ada penguatan peran negara tanpa menutup kerjasama internasional dan interdependensi global, melalui perjanjian bilateral atau kerangka ASEAN *Cyber Norms.*[60]

Sumber : Diolah dari berbagai sumber

Urgensi pembentukan UU Keamanan dan Ketahanan Siber semakin tak terelakkan seiring meningkatnya eskalasi ancaman siber yang menyasar tidak hanya sektor privat, tetapi juga infrastruktur strategis negara. Pertama, undang-undang ini harus secara tegas dan mengikat menetapkan standar minimum keamanan nasional untuk memastikan keseragaman pengamanan antar sektor. Standar tersebut harus mencakup prinsip pengamanan berlapis, pengujian kerentanan berkala *(vulnerability assessment),* serta kewajiban pelaporan insiden dalam jangka waktu tertentu. Ketidakseragaman standar yang berlaku saat ini telah menimbulkan celah hukum dan kelemahan struktural yang berbahaya bagi keamanan nasional. Kedua, pengaturan kelembagaan dalam UU dimaksud harus memberikan legitimasi konstitusional

58 Santoso, Purwo, Hasrul Hanif, and Rachmad Gustomy. "Menembus ortodoksi kajian kebijakan publik." (Yogyakarta: Fisipol UGM, 2004), hlm. 105.
59 Gedion Onyango,. "Whistleblower protection in developing countries: a review of challenges and prospects." *SN Business & Economics* 1, no. 12 (2021): 169.
60 Chotimah, H.C. *Op Cit*: 124.

dan yuridis kepada satu entitas dengan otoritas tunggal dan koordinatif, seperti BSSN guna menghindari tumpang tindih kewenangan yang melemahkan efektivitas respons insiden siber.[61] Ketiga, UU ini harus menjadi *lex specialis* yang mengintegrasikan perlindungan data strategis negara yang tersebar dalam berbagai regulasi sektoral. Ketiadaan satu rezim hukum berisiko menghambat pembuktian dan penindakan hukum terhadap pelanggaran atas sistem digital milik negara. Oleh karena itu, UU Keamanan dan Ketahanan Siber harus dirancang sebagai payung hukum utama yang menjamin perlindungan infrastruktur digital negara, baik dalam layanan publik daring, sistem pemerintahan elektronik, maupun komunikasi diplomatik, guna menjamin kedaulatan digital Indonesia secara utuh.

Dengan demikian, DPR dan Pemerintah harus menempatkan RUU Keamanan dan Ketahanan Siber sebagai prioritas legislasi nasional, mengingat potensi ancaman siber yang semakin sistemik. Pemerintah juga perlu melibatkan akademisi, masyarakat sipil, sektor swasta, dan komunitas teknologi dalam perumusan RUU, guna memastikan bahwa UU yang lahir nantinya inklusif, visioner, dan tidak represif.

b. Struktur Kelembagaan yang Ideal dalam Tata Kelola Keamanan Siber Nasional

Di tengah berkembangnya ekosistem digital dan meningkatnya kompleksitas ancaman siber global, penguatan struktur kelembagaan dalam sektor keamanan siber menjadi suatu keniscayaan. Negara tidak hanya dituntut hadir, tetapi harus membentuk suatu sistem kelembagaan yang efisien, terintegrasi, dan bertanggung jawab secara hukum dalam menjamin perlindungan terhadap infrastruktur informasi vital, hak-hak digital warga negara, serta kedaulatan nasional di ruang siber. Saat ini, wewenang terkait keamanan siber tersebar di berbagai institusi mulai dari BSSN, Kominfo, TNI, Polri, BIN, hingga sektor-sektor kementerian/ lembaga lainnya.[62] Kondisi ini menimbulkan redundansi kebijakan, inkonsistensi prosedural hingga ketidakjelasan pertanggungjawaban hukum. Fragmentasi ini juga menimbulkan celah koordinasi yang berdampak fatal terutama dalam penanggulangan insiden siber secara *real-time.* Tanpa adanya pusat kendali yang terintegrasi dan tegas secara hukum, maka yang terjadi bukan hanya kelemahan dalam respons, tetapi juga liabilitas hukum negara ketika terjadi pelanggaran hak privasi warga negara atau pembiaran atas pelanggaran kedaulatan siber oleh aktor negara lain.

Untuk membangun sistem kelembagaan yang ideal, penguatan peran BSSN menjadi syarat mutlak. BSSN yang dibentuk berdasarkan Peraturan Presiden Nomor 28 Tahun 2021 Tentang Badan Siber dan Sandi Negara (Perpres No. 28 Tahun 2021) telah diberikan mandat untuk menyelenggarakan keamanan siber secara nasional. Namun, dasar hukum kelembagaan BSSN yang hanya berpijak pada peraturan presiden melemahkan posisi yuridisnya sebagai otoritas nasional yang mengikat lintas sektor. Untuk menjadikan BSSN sebagai *commanding institution* dalam bidang keamanan siber maka perlu dilakukan kodifikasi pengakuan legal

[61] Disantara, Fradhana Putra. "Tripartite Collaborative Institutions: Skema Konvergensi Institusi Untuk Mewujudkan Ketahanan Siber Indonesia." *Istinbath: Jurnal Hukum* 18, no. 2 (2021): 207.

[62] Center for Digital Society, *Strategi Keamanan Siber Indonesia: Rekomendasi Rencana Aksi dan Implementasi* (Yogyakarta: Faculty of Social and Political Sciences, Universitas Gadjah Mada, 2019), hlm. 7.

melalui UU Keamanan dan Ketahanan Siber.[63] Penguatan ini mutlak disertai mekanisme akuntabilitas publik, audit kelembagaan, dan pengawasan independen terhadap tindakan-tindakan strategis BSSN agar tetap selaras dengan prinsip negara hukum. Dalam desain ideal, BSSN harus memiliki fungsi sebagai:

a) Pusat deteksi dan respons ancaman siber *(Cyber Threat Intelligence Center).*
b) Koordinator teknis lintas sektor *(Cross-sectoral Technical Coordinator).*
c) Penetap standar dan akreditasi keamanan siber nasional.
d) Pengendali sistem klasifikasi infrastruktur informasi kritikal.
e) Otoritas siber tunggal yang memegang *law enforcement liaison,* baik ke aparat nasional maupun kerja sama internasional.

Selain itu, struktur kelembagaan yang ideal harus memperhatikan prinsip *checks and balances* dalam demokrasi. Diperlukan pembentukan lembaga pengawas independen seperti *National Cybersecurity Board* (NCB) yang berperan mengawasi pelaksanaan kebijakan siber dari sisi perlindungan hak asasi manusia, menilai aspek kehati-hatian dalam kebijakan negara, serta menjembatani dialog antara pemerintah, sektor swasta, dan masyarakat sipil. Kehadiran NCB juga penting untuk memastikan bahwa tindakan pemerintah dalam ruang siber tidak menjelma menjadi instrumen represif melainkan tetap berada dalam kerangka prinsip negara hukum.

Lebih jauh, relasi antara negara dan sektor non-negara khususnya sektor swasta dan masyarakat sipil harus dijembatani dalam sebuah sistem kemitraan siber publik swasta yang terlembaga. Hal ini penting mengingat sebagian besar infrastruktur digital nasional dikelola oleh entitas non pemerintah seperti penyedia layanan *cloud,* platform digital, dan operator telekomunikasi. Dengan demikian, negara tidak dapat bekerja sendiri melainkan harus membangun kerangka kerja kolaboratif yang diatur secara legal yang mencakup forum koordinasi permanen, skema audit keamanan bersama,[64] mekanisme perlindungan pelapor pelanggaran *(whistleblower),*[65] serta pelibatan CSO *(Civil Society Organization)* dalam edukasi[66] dan advokasi keamanan digital. Ini dapat diwujudkan dalam bentuk:

a) Forum koordinasi permanen antara BSSN dan pelaku industri digital.
b) Pengakuan terhadap peran CSO dalam advokasi regulasi dan edukasi keamanan digital.
c) Skema audit bersama dan sertifikasi sistem keamanan oleh entitas netral.
d) Perlindungan terhadap pelapor insiden keamanan siber *(whistleblower protection).*

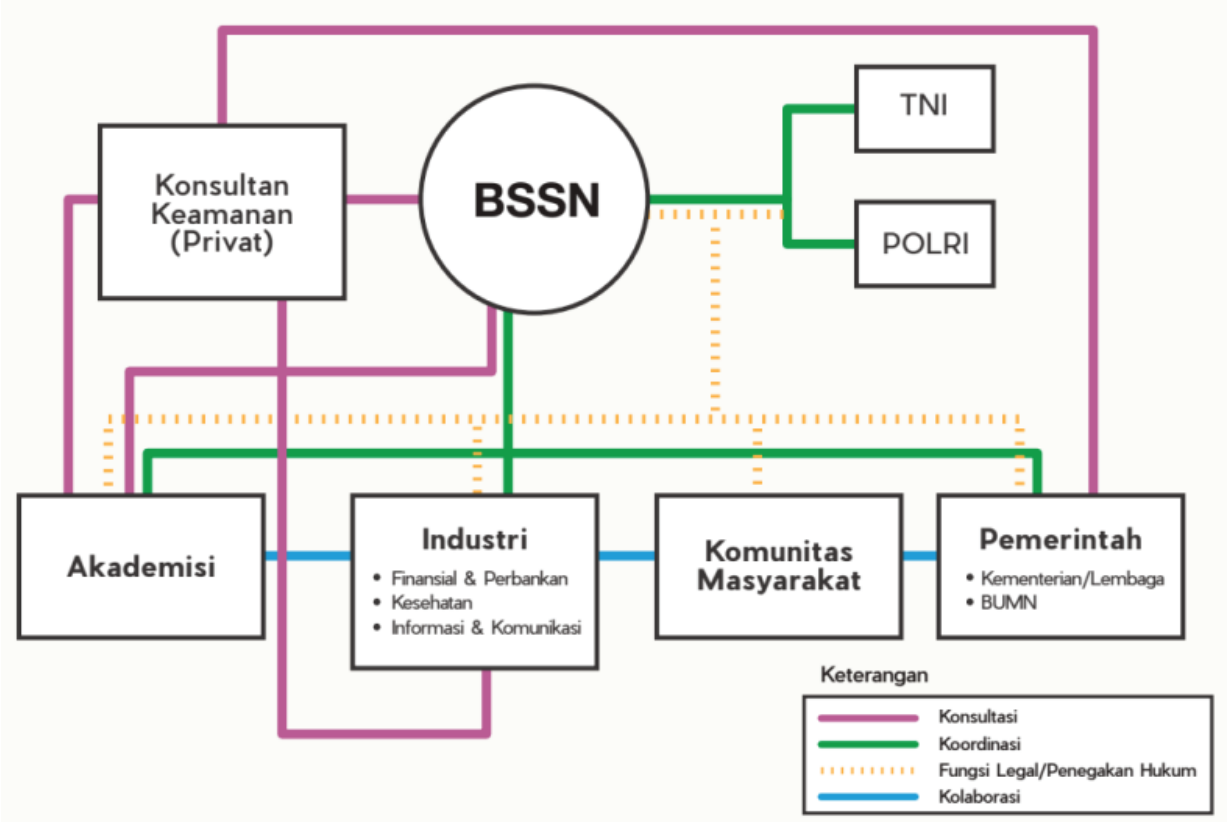
Akhirnya, agar koordinasi antar lembaga berjalan efektif dan kebijakan siber memiliki kekuatan yang mengikat lintas sektoral, struktur kelembagaan keamanan siber khususnya BSSN harus berada langsung di bawah koordinasi Presiden. Hal ini bukan hanya akan

63 Adma, Arinaldo, Yusuf Marsel Surbakti, and Puspita Sari, *Op. Cit*: 9.
64 Chotimah, H. C. *Op. Cit*:123.
65 Noho, Surafli. "Perlindungan Hukum terhadap Whistleblower Berdasarkan UU No. 31 Tahun 2014 tentang Perlindungan Saksi dan Korban." *Lex Crimen* 5, no. 5 (2016): 69.
66 Waskita, Allisa Salsabilla, and Hasan Sidik. "Diplomasi Siber Indonesia dalam Penyelenggaraan Capacity Building on National Cybersecurity Strategy Workshop 2019." *Padjadjaran Journal of International Relations* 5, no. 2 (2023): 151.

mempercepat pengambilan keputusan strategis terkait insiden siber berskala nasional tetapi juga memperkuat posisi kelembagaan BSSN sebagai pemegang otoritas tertinggi dalam domain keamanan siber. Penempatan ini juga sejalan dengan karakter sistem presidensial di Indonesia, di mana koordinasi lintas sektor dan pengendalian terhadap sumber daya strategis berada di bawah presiden sebagai kepala negara dan kepala pemerintahan. Selain itu, diberikan pula kerangka rekomendasi koordinasi multisektoral yang difokuskan pada penguatan sistem keamanan siber di Indonesia, sebagai berikut:

kuat melalui Undang-Undang, bersifat terpusat namun akuntabel, melibatkan pengawasan independen, dan mampu membangun kerja sama sinergis antara negara dan non negara. Tanpa itu, tata kelola keamanan siber Indonesia akan terus berada dalam kondisi rentan, baik dari sisi efektivitas penanggulangan ancaman maupun dari sisi jaminan perlindungan hak konstitusional warga negara. Pembentukan struktur kelembagaan yang terintegrasi, sah secara hukum, dan terbuka terhadap kontrol publik bukan lagi sekadar pilihan teknokratis melainkan kewajiban konstitusional negara

Gambar 1. Rekomendasi Skema Koordinasi Multisektoral



Sumber: Center for Digital Society, Universitas Gadjah Mada

Dengan demikian, struktur kelembagaan yang ideal dalam keamanan siber harus dibangun atas dasar legitimasi hukum yang dalam menjaga kedaulatan digital dan supremasi hukum di era transformasi digital.

c. Keseimbangan antara Keamanan dan Kebebasan

Dalam negara hukum yang demokratis, pembentukan kebijakan keamanan siber harus ditempatkan dalam kerangka konstitusional yang tidak hanya menjamin perlindungan terhadap infrastruktur digital negara, tetapi juga tidak boleh mengorbankan hak-hak konstitusional warga negara. Keamanan dan kebebasan bukanlah dikotomi, melainkan dua nilai yang harus dirumuskan secara seimbang dan saling memperkuat. Negara wajib menjaga ruang digital yang aman sekaligus menjamin hak atas privasi, kebebasan berekspresi, dan kebebasan berkomunikasi sebagaimana dijamin dalam Pasal 28E, 28G, dan 28I UUD NRI 1945. Sayangnya, praktik regulasi siber di Indonesia masih menyisakan persoalan konstitusionalitas. Misalnya, ketentuan dalam UU ITE, khususnya Pasal 27 dan 28, sering dijadikan alat kriminalisasi kebebasan berekspresi, serta tidak dilengkapi mekanisme pengawasan yudisial yang memadai terhadap praktik pengawasan digital oleh negara. Ini menunjukkan lemahnya prinsip legalitas, proporsionalitas, dan akuntabilitas publik dalam kebijakan keamanan siber nasional.

Oleh karena itu, diperlukan regulasi siber yang tunduk pada standar hak asasi manusia dan prinsip negara hukum. Setiap bentuk pembatasan kebebasan harus berbasis undang-undang, untuk tujuan yang sah seperti keamanan nasional, serta dilakukan secara proporsional. Prinsip ini juga merupakan bagian dari standar internasional yang telah diratifikasi Indonesia melalui UU No. 12 Tahun 2005 tentang Pengesahana *International Covenant on Civil and Political Rights (ICCPR).* Maka, desain hukum keamanan siber nasional harus menempatkan perlindungan HAM sebagai fondasi normatif, agar legitimasi demokratis dan konstitusional tidak tergerus oleh alasan keamanan yang eksesif.

Kebijakan keamanan siber harus bergeser dari pendekatan *state centric* menuju pendekatan *rights based* yang menempatkan warga negara sebagai subjek hukum yang dijamin hak konstitusionalnya. Legislasi harus secara tegas mengatur perlindungan atas hak privasi, hak atas enkripsi data pribadi, larangan pemantauan massal tanpa dasar hukum, serta menjamin prinsip *due process of law* dalam setiap penegakan hukum siber. Desain kelembagaan, khususnya terhadap BSSN, perlu diperkuat melalui mekanisme pengawasan independen dan transparan oleh parlemen, ombudsman, dan masyarakat sipil. Penggunaan teknologi pemantauan siber oleh aparat penegak hukum juga wajib tunduk pada kontrol yudisial guna mencegah penyimpangan represif.

Secara yuridis, pembentukan UU Keamanan dan Ketahanan Siber ke depan harus mampu mengintegrasikan prinsip-prinsip hukum yang menjamin keseimbangan antara perlindungan keamanan dan perlindungan kebebasan. Beberapa prinsip penting yang harus dijadikan rujukan normatif antara lain (1) prinsip legalitas bahwa setiap pembatasan harus berdasarkan hukum;[67] (2) prinsip proporsionalitas bahwa pembatasan tidak boleh berlebihan dan harus seimbang dengan tujuan keamanan;[68] (3) prinsip *necessity* bahwa pembatasan hanya boleh dilakukan bila benar-benar diperlukan;[69] serta (4) prinsip akuntabilitas dan pengawasan

[67] Varuhas, Jason NE. "The principle of legality." *The Cambridge Law Journal* 79, no. 3 (2020): 578.
[68] Ellis, Evelyn, ed. *The principle of proportionality in the laws of Europe*. (Oxford: Hart Publishing, 1999), hlm 32.
[69] Brudner, Alan. "A theory of necessity." *Oxford Journal of Legal Studies* 7, no. 3 (1987): 340.

bahwa setiap tindakan yang mempengaruhi kebebasan harus dapat dipertanggungjawabkan dan terbuka terhadap pengawasan publik.[70]

Dengan demikian, urgensi menjaga keseimbangan antara keamanan dan kebebasan tidak hanya menjadi kebutuhan praktis, melainkan merupakan imperatif konstitusional. Negara tidak boleh menggunakan narasi keamanan sebagai tameng untuk menggerus kebebasan yang telah dijamin oleh konstitusi. Sebaliknya, negara justru dituntut untuk membangun tata kelola keamanan siber yang berbasis pada hukum, demokrasi, dan penghormatan terhadap hak asasi manusia. Dalam hal inilah, pembentukan UU Keamanan dan Ketahanan Siber yang berbasis konstitusi dan berorientasi pada hak-hak warga negara menjadi krusial dalam mewujudkan keamanan yang demokratis dan kebebasan yang terlindungi.

D. Penutup

Serangan siber pada PDNS di tahun 2024 dan juga beberapa kasus serangan siber ke beberapa instansi lainnya, menunjukkan bahwa negara masih memiliki komitmen yang rendah dalam konteks keamanan siber. Skor keamanan siber di Indonesia lebih rendah dibandingkan dengan negara-negara ASEAN lainnya. Penyebab keamanan siber di Indonesia sangat lemah, diakibatkan oleh beberapa sebab. *Pertama*, terdapat fragmentasi kebijakan di bidang siber yang tidak selaras dengan prinsip-prinsip negara hukum modern. *Kedua,* peraturan perundang-undangan saat ini, baik di tingkat undang-undang seperti UU ITE dan UU PDP serta peraturan pelaksana lainnya, yang belum efektif dalam hal keamanan dan ketahanan siber nasional. *Ketiga*, pemerintah masih abai dan lalai untuk mempersiapkan sistem keamanan siber serta sistem penanggulangan apabila terjadi serangan siber, seperti sistem pencadangan dan sebagainya. *Keempat*, buruknya koordinasi antar lembaga dalam hal ini Kemenkomdigi dan BSSN dalam keamanan siber, karena saat ini hubungan dan koordinasi antar dua lembaga ini belum diatur secara jelas dalam peraturan perundang-undangan yang berlaku saat ini.

Berangkat dari permasalahan keamanan siber di atas, maka dapat disimpulkan bahwa Indonesia belum memiliki kerangka hukum keamanan siber yang utuh, komprenhensif dan berbasis prinsip konstitusional, berbeda dengan negara-negara maju yang telah menreformasi kerangka hukum keamanan siber-nya dengan mengedepankan prinsip partisipatif, transparansi, dan akuntabilitas. Oleh sebab itu, negara perlu merumuskan UU Keamanan dan Ketahanan Siber yang mengatur keamanan dan ketahanan siber secara komprehensif, yang tidak hanya sebatas akan keamanan siber secara fisik, tetapi juga mengedepankan prinsip-prinsip konstitusional dan demokrasi.

UU Keamanan dan Ketahanan Siber tidak hanya menyasar pada sektor privat saja, tetapi juga infrastruktur strategis negara, yang pada UU ini akan menetapkan minimum keamanan nasional serta keseragaman pengamanan sektor dan memberikan legitimasi konstitusional dan yuridis kepada satu entitas dengan otoritas tunggal dan koordinatif, serta terakhir UU ini mengintegrasikan perlindungan data strategis negara yang tersebar pada berbagai regulasi sektoral. Selain itu, bahwa diperlukan penguatan lembaga dalam hal ini BSSN dengan

[70] Pelizzo, Riccardo, and Frederick Stapenhurst. *Government accountability and legislative oversight.* (New York: Routledge, 2013), hlm. 32.

diiringi pembentukan lembaga independen yang memiliki fungsi untuk mengawasi pelaksanaan kebijakan di bidang keamanan dan ketahanan siber, serta juga membangun relasi yang kolaboratif secara legal dengan pihak-pihak di luar pemerintah. Terakhir, keamanan siber juga harus dilakukan dengan pendekatan *right based*, yang menempatkan warga negara sebagai subjek hukum yang dijamin hak konstitusionalnya, sehingga pada dasarnya regulasi di bidang keamanan siber harus mampu menjaga keseimbangan antara perlindungan keamanan siber dengan perlindungan kebebasan.

DAFTAR PUSTAKA

Buku

Abdulkadir Muhammad, *Hukum dan Penulisan Hukum*, (Bandung: Citra Aditya Bakti, 2004).

BSSN, *Lanskap Keamanan Siber Indonesia 2024* (Jakarta: BSSN, 2024).

Catur Nugroho, *Cyber Society Teknologi, Media Baru, dan Distrupsi Informasi* (Jakarta: Kencana, 2020).

Center for Digital Society, *Strategi Keamanan Siber Indonesia: Rekomendasi Rencana Aksi dan Implementasi* (Yogyakarta: Faculty of Social and Political Sciences, Universitas Gadjah Mada, 2019).

Ellis, Evelyn, ed. *The principle of proportionality in the laws of Europe*. (Oxford: Hart Publishing, 1999).

Gani, Taufiq A. *Kedaulatan data digital untuk integritas bangsa*. (Aceh: Syiah Kuala University Press, 2023).

Garg, Himani, M. Balasubramaniam, Ajay Kr Gupta, and Jitendra Singh. "'NIS'a Network Investigation System." In *Proceedings of Emerging Trends and Technologies on Intelligent Systems: ETTIS 2021*. (Singapore: Springer Nature, 2022.

Goundar, Sam, Archana Purwar, and Ajmer Singh, eds. *Applications of artificial intelligence, big data and internet of things in sustainable development*. (Boca Raton: CRC Press, 2022).

Lexy J. Moleong, Metodologi Penelitian Kualitatif, (Bandung: Rosdakarya, 2000).

Lord Acton, "Power tends to corrupt, and absolute power corrupts absolutely," in a letter to Bishop Mandell Creighton, April 3, 1887, as cited in Brian Martin, *Information Liberation: Challenging the Corruptions of Information Power* (London: Freedom Press, 1998).

Michael P. Fischerkeller, Emily O. Goldman, dan Richard J. Harknett, *Cyber Persistence Theory Redefining National Security in Cyberscpace* (New York: Oxford University Press, 2022).

Muhaimin, *Metode Penelitian Hukum,* (Mataram: Mataram University Pers, 2020).

Myriam Dunn Cavelty, *The Politics of Cyber-Security* (New York: Routledge, 2025).

Pelizzo, Riccardo, and Frederick Stapenhurst. *Government accountability and legislative oversight*. (New York: Routledge, 2013).

Peter Mahmud Marzuki (Peter Mahmud I), *Penelitian Hukum*: Edisi Revisi, (Jakarta: Kencana Prenada Media Group, 2005).

Reveron, Derek S., ed. *Cyberspace and national security: threats, opportunities, and power in a virtual world*. (Washington: Georgetown University Press, 2012).

Ridwan, H. R. "Hukum administrasi negara." (Jakarta : RajaGrafindo Persada, 2006).

Santoso, Purwo, Hasrul Hanif, and Rachmad Gustomy. "Menembus ortodoksi kajian kebijakan publik." (Yogyakarta: Fisipol UGM, 2004).

Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif : Suatu Tinjauan Singkat,* ed. 17, (Jakarta : Rajawali Pers, 2015).

Suratman dan Philip Dillah, Metode penelitian Hukum, (Bandung: Alfabeta, 2012).

Makalah dan Hasil Penelitian

Adma, Arinaldo, Yusuf Marsel Surbakti, and Puspita Sari. "Transformasi Sistem Pertahanan Siber Indonesia dengan BSSN Sebagai Poros & Motor Penggerak Menuju Angkatan Siber Mandiri di Masa Depan." *Jurnal Kajian Stratejik Ketahanan Nasional* 6, no. 1 (2023).

Ahmad Irwan Hamzani dkk, "Legal Research Method: Theoretical and Implementative Review", *International Journal of Membrane Science and Technology* 10, no. 2 (2023).

Aliane, Nadir, and Saima Jamil. "Human Side of Digital Transformation: Hyper Connectedness and Collaboration." *International Journal of Operations and Quantitative Management* 29, no. 1 (2023).

Aryojati Ardipandanto, "Lemahnya Pengamanan Pusat Data Nasional Sementara Terhadap Serangan Siber," *Info Singkat* 16, no. 13 (2024).

Brudner, Alan. "A theory of necessity." *Oxford Journal of Legal Studies* 7, no. 3 (1987).

Chotimah, H. C. Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional* 10, no. 2 (2019).

Disantara, Fradhana Putra. "Tripartite Collaborative Institutions: Skema Konvergensi Institusi Untuk Mewujudkan Ketahanan Siber Indonesia." *Istinbath: Jurnal Hukum* 18, no. 2 (2021): 207.

Gedion Onyango,. "Whistleblower protection in developing countries: a review of challenges and prospects." *SN Business & Economics* 1, no. 12 (2021).

Jimly Asshiddiqie. "Gagasan negara hukum Indonesia." *Makalah Disampaikan dalam Forum Dialog Perencanaan Pembangunan Hukum Nasional yang Diselenggarakan oleh Badan Pembinaan Hukum Nasional Kementerian Hukum dan*, vol. 1. (2011).

Juan Matheus dan Ariawan Gunadi, "Pembentukan Lembaga Pengawas Perlindungan Data Pribadi Di Era Ekonomi Digital : Kajian Perbandingan Dengan KPPU", *Jurnal Justisi* 10, no. 1, (2024).

Lanz, Zachary. "Cybersecurity risk in US critical infrastructure: An analysis of publicly available US government alerts and advisories." *International Journal of Cybersecurity Intelligence & Cybercrime* 5, no. 1 (2022).

Lawrance J. Trautman, "Cybersecurity What About U.S Policy?" *Journal of Law, Technology & Policy* 2015, no. 341 (2015).

M. Prakoso Aji, "Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi)", *Jurnal Politica* 5, no. 2 (2022).

Markopoulou, Dimitra, Vagelis Papakonstantinou, and Paul De Hert. "The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation." *Computer Law & Security Review* 35, no. 6 (2019).

Masike Malatji. "Management of enterprise cyber security: A review of ISO/IEC 27001: 2022." Dalam *2023 International conference on cyber management and engineering (CyMaEn)*. IEEE, (2023).

Noang, Edmondus Iswenyo. "Jaga Diri di Baltik." *Global Political Studies Journal* 6, no. 1 (2022).

Noho, Surafli. "Perlindungan Hukum terhadap Whistleblower Berdasarkan UU No. 31 Tahun 2014 tentang Perlindungan Saksi dan Korban." *Lex Crimen* 5, no. 5 (2016).

Nolin, Jan, and Nasrine Olson. "The Internet of Things and convenience." *Internet Research* 26, no. 2 (2016).

Oona A. Hathaway, et.all, " The Law of Cyber Attack," *California Law Review* 100, no. 817 (2012).

Parulian, Sahat, Devi Anassafila Pratiwi, and Meiliya Cahya Yustina. "Studi tentang ancaman dan solusi serangan siber di indonesia." *Telecommunications, Networks, Electronics, and Computer Technologies (TELNECT)* 1, no. 2 (2021).

Pedro Robles and Daniel J. Mallinson, "Artificial Intelligence Technology, Public Trust, and Effective Governance," *Review of Policy Research* 42, no. 1 (2023).

Ratno Lukito. ""Compare But Not to Compare": Kajian Perbandingan Hukum di Indonesia." *Undang: Jurnal Hukum* 5, no. 2 (2022).

Standing Committee of the National People's Congress, *Cybersecurity Law of the People's Republic of China*, adopted November 7, 2016, effective June 1, (2017).

Timmers, Paul. "Ethics of AI and cybersecurity when sovereignty is at stake." *Minds and Machines* 29, no. 4 (2019).

Timothy MCintosh, et.all, "Ransomware Reloaded: Re-Examining Its Tren, Research and Mitigation in the Era of Data Exfiltration," *ACM Computing Surveys* 57, no. 1 (2024.

Varuhas, Jason NE. "The principle of legality." *The Cambridge Law Journal* 79, no. 3 (2020).

Waskita, Allisa Salsabilla, and Hasan Sidik. "Diplomasi Siber Indonesia dalam Penyelenggaraan Capacity Building on

National Cybersecurity Strategy Workshop 2019." *Padjadjaran Journal of International Relations* 5, no. 2 (2023).

Wasyihun Sema Admass, Yirga Yayeh Munaye, and Abebe Abeshu Diro, "Cyber Security: State of The Art, Challenges and Future Directions," *Cyber Security and Applications* 2, (2024).

Xu, Zonghuang, and Jin Shi. "Research on the national security risk assessment model: a case study of political security in China." *Humanities and Social Sciences Communications* 12, no. 1 (2025).

Internet

BBC Indonesia, "Petinggi Kominfo mundur 'sebagai tanggung jawab moral' setelah Pusat Data Nasional diretas", https://www.bbc.com/indonesia/articles/c8vdmymmynzo (diakses pada 17 Mei 2025).

BCA Insurance, "Asuransi Siber Pribadi (Personal Cyber Insurance)", https://bcainsurance.co.id/product/detail/asuransi-siber-pribadi-personal-cyber-insurance (diakses pada 17 Mei 2025).

Elsam, "Insiden Keamanan Siber dan Dugaan Kegagalan Pelindungan Data PDN Sementara, Harus Ditangani Secara Simultan dan Tuntas**",** https://www.elsam.or.id/siaran-pers/insiden-keamanan-siber-dan-dugaan-kegagalan-pelindungan-data-pdn-sementara--harus-ditangani-secara-simultan-dan-tuntas (diakses pada 17 Mei 2025).

Hukumonline, "Ini 41 RUU yang Masuk Prolgenas Prioritas 2025," https://www.hukumonline.com/berita/a/ini-41-ruu-yang-masuk-prolegnas-prioritas-2025-lt673c52dc1bcb0/?page=2 (diakses 5 Mei 2025)

Info Bank News, "Ngeri! Segini Potensi Kerugian Ekonomi Akibat Peretasan PDN", https://infobanknews.com/ngeri-segini-potensi-kerugian-ekonomi-akibat-peretasan-pdn/ (diakses pada 17 Mei 2025).

Katadata, "Daftar Panjang Kerugian Serangan Ransomware di Indonesia," https://katadata.co.id/analisisdata/668cf48a48836/daftar-panjang-kerugian-serangan-ransomware-di-indonesia (diakses 6 Mei 2025).

Kompas, "Kronologi Serangan Ransomware ke PDN dan Penanganannya yang Tak Kunjung Usai," https://tekno.kompas.com/read/2024/07/10/12350077/kronologi-serangan-ransomware-ke-pdn-dan-penanganannya-yang-tak-kunjung-usai#google_vignette (diakses pada 8 Mei 2025).

Kompas, "PDN Lumpuh, BSSN Ungkap Tak Ada "Backup" Data Jadi Masalah Utama," https://www.kompas.id/baca/polhuk/2024/06/27/pdn-lumpuh-bssn-ungkap-tak-ada-backup-data-jadi-masalah-utama?open_from=Tagar_Page (diakses pada 7 Mei 2025).

Kompas.id, "Bencana Nasional Serangan ke Pusat Data Nsional Bisa Buka Perang Siber dan Ancaman Negara." https://www.kompas.id/baca/polhuk/2024/06/26/bencana-nasional-akibat-serangan-ke-pusat-data-nasional (diakses 5 Mei 2025). Pasca serangan *ransomware* tersebut Kejaksaan mengendus terdapat indikasi dugaan tindak pidana korupsi dalam Pengadaan barang/jasa pada pengelolaan PDN. Lihat dalam Tempo, "Kejaksaan Usut Dugaan Korupsi Pusat Data Nasional Usai Serangan Ransomware Juni 2024," https://www.tempo.co/hukum/kejaksaan-usut-dugaan-korupsi-pusat-data-nasional-usai-serangan-ransomware-juni-2024--1220952 (diakses 5 Mei 2025).

NCSI, "National Cyber Security Index," https://ncsi.ega.ee/ncsi-index/?order=rank&archive=1 (diakses 5 Mei 2025).

Tempo, "Kronologi Pusat Data Nasional Jebol Hingga Desakan Menkominfo Budi Arie Mundur dari Jabatannya." https://www.tempo.co/politik/kronologi-pusat-data-nasional-jebol-hingga-desakan-menkominfo-budi-arie-mundur-dari-jabatannya-44552 (diakses 5 Mei 2025).

Peraturan Perundang-Undangan

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

Undang-Undang Nomor 12 Tahun 2005 Tentang Pengesahan *International Covenant on Civil and Political Rights*

Peraturan Presiden Nomor 95 Tahun 2018 Tentang Sistem Pemerintahan Berbasis Elektronik

Peraturan Presiden Nomor 39 Tahun 2019 Tentang Satu Data Nasional

Peraturan Presiden Nomor 82 Tahun 2023 Tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional

Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Peraturan Presiden Nomor 28 Tahun 2021 Tentang Badan Siber dan Sandi Negara

Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 Tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintah Berbasis Elektronik