JAKSA
JURNAL KAJIAN ILMU HUKUM DAN POLITIK

LPPM Universitas Sains dan Teknologi Komputer
Vol. 4 No. 1 Februari 2026, Hal. 30-42
E-ISSN: 2988-5140; P-ISSN: 2988-7747
Link: https://journal.stekom.ac.id/index.php/Jaksa/index

Kedudukan Keputusan Pemerintah dalam Keadaan Darurat Digital Studi Tentang Batasan Konstitusional Atas Kebijakan *Cyber emergency*

Maulana Fahmi Idris*[1], Althea Serafim Kriswandaru[2]
[1, 2]*Program Studi Hukum, Universitas Sains dan Teknologi Komputer, Semarang, Indonesia*
E-mail: maulanafahmi@stekom.ac.id[*1], altheaserafim@stekom.ac.id[2]

Article Info

Keywords:
Cyber emergency, Constitutional Law, Digital Constitutionalism, Cybersecurity, State Sovereignty

Abstract

The rapid growth of digital technology has created new challenges for the constitutional framework of state power, particularly in the context of cyber emergencies. This research analyzes the role of government decisions in digital emergencies within the framework of Indonesian constitutional law. Using a socio-legal approach, the study examines the alignment between governmental actions and fundamental constitutional principles, such as legality, proportionality, accountability, and the protection of human rights. The findings reveal significant gaps between existing regulations and the need for constitutionally grounded responses to cyber threats. Current government measures tend to be reactive and lack comprehensive oversight mechanisms, posing risks to democratic governance and individual rights. The study recommends establishing a specific legal framework that clearly defines procedures, limitations, and oversight for cyber emergency actions, grounded in digital constitutionalism. By reinforcing constitutional supremacy in the digital era, the government can ensure that its responses to cybersecurity crises are both effective and respectful of citizens' fundamental rights.

DOI: https://doi.org/10.51903/mj9whz36
Submitted: 09 Sept 2025, Reviewed: 22 Nov 2025, Accepted: 30 Dec 2025
**Corresponding Author*

Abstrak

Perkembangan pesat teknologi digital telah menciptakan tantangan baru bagi kerangka ketatanegaraan, khususnya dalam konteks darurat siber. Penelitian ini menganalisis kedudukan dan dasar konstitusional terhadap keputusan pemerintah selama terjadinya kondisi darurat digital dalam kerangka hukum tata negara di Indonesia. Menggunakan pendekatan sosio-legal, studi ini mengkaji kesesuaian tindakan pemerintah dengan prinsip-prinsip konstitusional fundamental seperti legalitas, proporsionalitas, akuntabilitas, dan perlindungan hak asasi manusia. Temuan penelitian menunjukkan adanya kesenjangan signifikan antara regulasi yang berlaku dengan kebutuhan akan respons terhadap ancaman siber yang berlandaskan konstitusi. Langkah-langkah pemerintah saat ini cenderung bersifat reaktif dan belum didukung oleh mekanisme pengawasan yang komprehensif, sehingga menimbulkan risiko bagi tata kelola demokratis dan perlindungan hak-hak individu. Penelitian ini merekomendasikan pembentukan kerangka hukum khusus yang secara jelas mendefinisikan prosedur, batasan kewenangan, serta mekanisme pengawasan dalam tindakan darurat siber, dengan berlandaskan prinsip konstitusionalisme digital. Dengan memperkuat supremasi konstitusi di era digital, negara dapat memastikan bahwa respons terhadap krisis keamanan siber tetap efektif serta menghormati hak-hak fundamental warga negara.

Kata Kunci: *Darurat Siber, Hukum Tata Negara, Konstitusionalisme Digital, Keamanan Siber, Kedaulatan Negara*

I. PENDAHULUAN

Perkembangan teknologi informasi telah membawa dunia ke dalam era baru yang penuh tantangan dan kompleksitas, di mana hampir seluruh aktivitas manusia terkoneksi melalui ruang digital (Luo, 2024). Transformasi digital ini tidak hanya mendorong kemajuan di berbagai bidang seperti ekonomi, pendidikan, dan pemerintahan, tetapi juga membuka ruang baru bagi munculnya ancaman-ancaman yang belum pernah dihadapi sebelumnya (Radanliev, 2024). Negara, sebagai entitas penyelenggara kekuasaan, harus mampu beradaptasi dengan dinamika baru ini, termasuk dalam aspek pengelolaan keamanan nasional. Salah satu fenomena yang kini menjadi perhatian serius adalah darurat digital, yaitu situasi di mana gangguan atau serangan siber dapat mengancam stabilitas dan keamanan negara secara keseluruhan (AlDaajeh et al., 2022). Dalam kondisi seperti ini, pemerintah dituntut untuk mengambil keputusan cepat untuk memitigasi ancaman tersebut. Namun demikian, langkah-langkah yang diambil tidak boleh mengabaikan prinsip dasar negara hukum, yakni supremasi konstitusi, penghormatan terhadap hak asasi manusia, dan akuntabilitas kekuasaan (Abdelkader et al., 2024).

Dalam negara demokratis seperti Indonesia, tindakan pemerintah dalam menghadapi keadaan darurat digital harus tetap tunduk pada kerangka hukum yang sahih. Negara memang berkewajiban melindungi warganya dari berbagai bentuk ancaman, termasuk di ruang siber, namun kewenangan itu tidak boleh dijalankan secara sewenang-wenang (Rahman & Tang, 2022). Kebutuhan untuk bertindak cepat sering kali berbenturan dengan keharusan menjaga legalitas dan legitimasi tindakan tersebut di mata hukum (Arifin, 2022). Permasalahan ini menjadi semakin kompleks karena ruang digital tidak sepenuhnya dapat dikendalikan melalui mekanisme hukum konvensional, sehingga menimbulkan pertanyaan penting tentang sejauh mana batas kewenangan pemerintah dalam kondisi darurat digital (Muhidin et al., 2023). Pertanyaan-pertanyaan ini menjadi sangat relevan untuk dikaji lebih dalam, terutama untuk memastikan bahwa tindakan negara tetap berada dalam koridor konstitusi dan tidak mengorbankan prinsip-prinsip demokrasi yang telah diperjuangkan (Prasetyoningsih et al., 2025).

Fenomena darurat digital tidak hanya terjadi di Indonesia, tetapi juga di berbagai negara lain yang tengah menghadapi ancaman serupa (Anggoro et al., 2022). Berdasarkan laporan Global Risks Report tahun 2023 yang diterbitkan oleh World Economic Forum, serangan siber terhadap infrastruktur penting tercatat sebagai salah satu dari lima risiko global terbesar yang dihadapi dunia dalam dekade mendatang (Alam et al., 2022). Data menunjukkan bahwa sejak tahun 2020, jumlah serangan ransomware terhadap fasilitas publik meningkat sebesar 62 persen secara global, dengan kerugian ekonomi mencapai lebih dari 20 miliar dolar Amerika per tahun (Rohayati & Abdillah, 2024). Indonesia sendiri, menurut laporan Badan Siber dan Sandi Negara (BSSN) tahun 2023, mengalami lebih dari 300 juta anomali trafik siber, termasuk ribuan insiden yang menyerang sektor pemerintahan dan infrastruktur vital nasional (Mahaswa et al., 2025). Fakta ini menunjukkan betapa gentingnya ancaman di ruang digital dan kebutuhan mendesak untuk merumuskan kebijakan yang responsif sekaligus konstitusional (Adiprasetio et al., 2024).

Di dalam negeri, kasus-kasus peretasan terhadap situs resmi pemerintahan, pencurian data sensitif, dan sabotase sistem informasi publik semakin sering terjadi (Aslan et al., 2023). Salah satu insiden besar yang menjadi sorotan adalah peretasan sistem data Dukcapil yang membahayakan keamanan informasi penduduk (Afaq et al., 2022). Selain itu, bocornya data pelanggan operator seluler nasional pada tahun 2022 yang berdampak pada jutaan warga Indonesia mengungkapkan lemahnya sistem pertahanan siber nasional. Kejadian-kejadian ini memaksa pemerintah untuk merumuskan langkah darurat, namun belum ada landasan hukum spesifik yang mengatur tentang prosedur penanganan keadaan darurat di ruang digital secara rinci dalam kerangka hukum tata negara (Lehto, 2022). Ini memperlihatkan adanya kekosongan hukum yang berpotensi disalahgunakan atau menghasilkan kebijakan yang bertentangan dengan prinsip demokrasi dan perlindungan hak konstitusional warga negara (Raghupathi et al., 2023).

Berbagai literatur telah membahas hubungan antara tindakan pemerintah dalam situasi darurat dan prinsip-prinsip hukum tata negara. (Nampewo et al., 2022) menekankan bahwa dalam kondisi darurat, negara tetap wajib tunduk pada prinsip-prinsip fundamental hukum internasional dan nasional, termasuk penghormatan terhadap hak asasi manusia. Dalam konteks ini, tindakan-tindakan luar biasa hanya dibenarkan jika bersifat sementara, proporsional, dan dapat dipertanggungjawabkan secara hukum. (Rubinst & Barzilaif, 2022) menguraikan bahwa mekanisme derogasi terhadap hak-hak tertentu dalam keadaan darurat harus dilakukan secara hati-hati dan diawasi oleh lembaga-lembaga demokratis untuk mencegah penyalahgunaan kekuasaan. Di Indonesia, prinsip-prinsip ini tercermin dalam Pasal 28I dan 28J UUD 1945, yang menegaskan bahwa hak asasi manusia hanya dapat dibatasi oleh undang-undang demi penghormatan hak orang lain serta untuk memenuhi tuntutan keadilan dan ketertiban umum (Anastasi, 2023).

Selain itu, diskursus tentang kedaulatan digital (*digital sovereignty*) yang berkembang di kancah global turut memberikan warna baru dalam perdebatan mengenai peran negara dalam mengatur ruang siber (Jiang, 2024). Menurut (Madnick et al., 2024), kontrol negara terhadap internet harus ditempatkan dalam konteks perlindungan keamanan nasional, tetapi tetap mempertimbangkan hak-hak dasar individu. Dalam pandangan ini, tindakan pemerintah dalam dunia maya, termasuk dalam kondisi darurat, harus tetap mematuhi standar-standar internasional mengenai hak asasi manusia dan supremasi hukum. Di sisi lain, konsep "*cybe*r constitutionalism" yang diusung oleh (Fung, 2022) menggarisbawahi pentingnya menerapkan prinsip-prinsip konstitusional dalam pengaturan dunia maya, termasuk prinsip transparansi, akuntabilitas, dan pembatasan kekuasaan.

Dalam konteks Indonesia, beberapa regulasi yang bersinggungan dengan darurat digital, seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) serta Peraturan Presiden tentang Strategi Keamanan Siber Nasional, memang memberikan landasan umum tentang pengelolaan ancaman siber. Namun, regulasi-regulasi ini belum secara spesifik mengatur prosedur atau batasan kekuasaan eksekutif dalam menangani situasi darurat digital. Seperti diungkap

oleh (Li et al., 2024), ada kebutuhan mendesak untuk menyusun regulasi yang lebih rinci, khususnya dalam menetapkan siapa yang berwenang mendeklarasikan darurat digital, prosedur apa yang harus diikuti, dan bagaimana akuntabilitasnya dipastikan. Tanpa kerangka hukum yang memadai, tindakan pemerintah bisa saja menimbulkan pelanggaran serius terhadap hak warga negara (Díaz-Rodríguez et al., 2023).

Studi-studi terkait yang telah ada lebih banyak membahas aspek teknis dan keamanan dari ancaman siber. Misalnya, (Cains et al., 2022) mengkaji pentingnya membangun ketahanan siber nasional melalui penguatan kapasitas teknis lembaga terkait, sedangkan (Admass et al., 2024) menyoroti perlunya peningkatan literasi keamanan digital masyarakat. Namun, kajian tentang kedudukan hukum tindakan pemerintah dalam menghadapi darurat digital dari perspektif hukum tata negara masih sangat terbatas. Hal ini menunjukkan bahwa aspek legal-konstitusional dari kebijakan *cyber emergency* belum mendapatkan perhatian yang cukup, baik dalam literatur akademik maupun dalam praktik kenegaraan di Indonesia.

Beberapa penelitian terkait telah mencoba mengeksplorasi konsep pengelolaan keadaan darurat di dunia maya, namun cenderung fokus pada studi kasus negara-negara lain atau mengulas secara umum tentang *cyber* security. Misalnya, penelitian yang dilakukan oleh (Zwilling et al., 2022) membahas perlindungan data pribadi dalam konteks serangan siber di Eropa, sementara (Wylde et al., 2022) meneliti bagaimana negara-negara Afrika mengadopsi kebijakan keamanan digital dalam menghadapi konflik bersenjata berbasis siber. Kedua studi tersebut penting, namun belum secara spesifik menyentuh pada permasalahan konstitusionalitas tindakan pemerintah dalam konteks darurat digital di negara hukum seperti Indonesia.

Adanya gap penelitian ini sangat jelas ketika membandingkan literatur yang ada dengan kebutuhan nyata di lapangan. Meski serangan siber meningkat drastis dan menjadi ancaman nyata terhadap keamanan nasional, kajian hukum tata negara mengenai legitimasi dan batasan tindakan pemerintah dalam merespons keadaan darurat digital masih minim. Sebagian besar studi lebih berfokus pada aspek teknis keamanan atau regulasi sektoral, tanpa membahas secara mendalam hubungan antara tindakan eksekutif, supremasi konstitusi, dan perlindungan hak asasi manusia. Padahal, dalam negara hukum, pembatasan terhadap kekuasaan pemerintah—bahkan dalam kondisi darurat—merupakan prinsip fundamental yang tidak boleh diabaikan.

Oleh karena itu, penelitian ini berupaya mengisi kekosongan tersebut dengan mengkaji kedudukan hukum tindakan pemerintah dalam menghadapi keadaan darurat digital dari perspektif hukum tata negara. Penelitian ini bertujuan untuk menganalisis bagaimana tindakan-tindakan tersebut dapat dijalankan tanpa mengabaikan prinsip-prinsip konstitusional, seperti legalitas, proporsionalitas, akuntabilitas, dan penghormatan terhadap hak asasi manusia. Dengan fokus pada konteks Indonesia, penelitian ini diharapkan dapat memberikan kontribusi teoritis dalam mengembangkan konsep digital constitutionalism serta kontribusi praktis dalam memberikan rekomendasi penyusunan regulasi yang

konstitusional terkait kebijakan *cyber emergency*. Penelitian ini menawarkan pendekatan interdisipliner yang menggabungkan analisis hukum tata negara dengan dinamika teknologi digital, menghadirkan perspektif baru yang selama ini belum banyak dijelajahi di dalam literatur hukum Indonesia maupun internasional.

II. METODOLOGI PENELITIAN

A. Pendekatan Penelitian

Penelitian ini menggunakan pendekatan *socio-legal*, yaitu mengkaji hukum tidak hanya sebagai seperangkat norma tertulis, melainkan juga sebagai praktik sosial yang berkembang dalam konteks kehidupan bermasyarakat dan bernegara. Pendekatan ini dipilih untuk menangkap dinamika nyata antara prinsip-prinsip hukum tata negara dengan tindakan konkret pemerintah dalam menghadapi keadaan darurat digital. Pendekatan socio-legal memungkinkan analisis yang lebih komprehensif terhadap penerapan norma konstitusional dalam praktik kebijakan *cyber emergency*, sekaligus memahami bagaimana hukum berinteraksi dengan kebutuhan teknis, politik, dan sosial dalam situasi krisis digital.

B. Jenis dan Sumber Data

Jenis data yang digunakan adalah data sekunder dan data empiris terbatas. Data sekunder terdiri dari dokumen hukum seperti Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahan-perubahannya, serta berbagai peraturan pemerintah terkait keamanan siber dan penanganan keadaan darurat. Selain itu, digunakan juga literatur akademik yang relevan, seperti jurnal hukum, laporan riset kebijakan, hasil kajian institusi internasional, serta teori tentang digital constitutionalism. Untuk melengkapi data normatif, dikumpulkan juga data empiris berupa studi kasus tentang penerapan kebijakan darurat digital di Indonesia, serta analisis pernyataan resmi pejabat negara, kebijakan operasional Badan Siber dan Sandi Negara (BSSN), dan publikasi berita terkait insiden *cyber emergency*.

C. Teknik Pengumpulan Data

Data dikumpulkan melalui studi kepustakaan sistematis dan analisis dokumentasi terhadap peraturan perundang-undangan, dokumen kebijakan, laporan insiden keamanan digital, serta artikel ilmiah yang relevan. Selain itu, dilakukan pemantauan terhadap media massa, laporan resmi lembaga pemerintahan, serta bahan diskusi publik untuk menangkap dinamika penerapan hukum dalam konteks darurat digital. Data dikategorisasikan berdasarkan relevansi terhadap tema konstitusionalitas, tindakan eksekutif, dan hak-hak dasar warga negara.

D. Teknik Analisis Data

Analisis data dilakukan secara kualitatif dengan menggunakan metode content analysis dan contextual analysis. Content analysis digunakan untuk menelaah teks hukum, regulasi, dan dokumen kebijakan guna mengidentifikasi prinsip-prinsip konstitusional yang berlaku. Sementara itu, *contextual analysis* digunakan untuk memahami penerapan norma-norma tersebut dalam konteks sosial-politik saat menghadapi ancaman digital. Teknik ini memungkinkan peneliti untuk melihat bagaimana keputusan pemerintah saat *cyber emergency* diinterpretasikan, dijalankan, serta sejauh mana mematuhi prinsip-prinsip konstitusi. Analisis juga melibatkan interpretasi kritis terhadap ketegangan antara kebutuhan keamanan nasional dan perlindungan hak asasi manusia.

E. Strategi Validasi Data

Untuk menjaga validitas hasil penelitian, dilakukan triangulasi sumber data. Data hukum dibandingkan dengan data empiris berupa praktik kebijakan pemerintah dan laporan publik untuk melihat konsistensi antara norma dan realitas. Selain itu, validasi dilakukan dengan membandingkan temuan penelitian ini dengan hasil studi-studi terdahulu yang relevan, serta dengan prinsip-prinsip internasional tentang hak asasi manusia dalam kondisi darurat digital. Validasi akademik tambahan diperoleh melalui diskusi dengan pakar hukum tata negara dan teknologi informasi.

F. Batasan Penelitian

Penelitian ini dibatasi pada konteks Indonesia dan berfokus pada aspek konstitusionalitas tindakan pemerintah dalam situasi darurat digital. Analisis tidak mencakup perbandingan hukum secara internasional secara rinci, ataupun aspek teknis operasional pertahanan siber. Batasan ini ditetapkan untuk menjaga konsistensi penelitian dengan fokus utama pada hubungan antara supremasi konstitusi dan kekuasaan negara dalam ruang digital.

G. Prosedur Penelitian

Penelitian diawali dengan identifikasi fenomena darurat digital di Indonesia, diikuti dengan telaah mendalam terhadap dokumen hukum dan literatur akademik untuk membangun kerangka teoretis. Selanjutnya, dilakukan pengumpulan data empiris tentang kebijakan pemerintah dan respon publik terhadap insiden keamanan siber. Analisis dilakukan secara simultan terhadap norma hukum dan praktik sosial yang terjadi, dengan mengidentifikasi kesenjangan antara prinsip-prinsip konstitusional dan realitas tindakan pemerintah. Proses ini dilengkapi dengan refleksi kritis untuk merumuskan rekomendasi konstitusional terhadap kebijakan *cyber emergency* yang lebih akuntabel dan sesuai prinsip negara hukum.

Untuk memperjelas alur penelitian ini, gambar 1 menyajikan diagram alur penelitian yang menggambarkan tahapan dari pengumpulan data hingga analisis dan penyusunan rekomendasi.

Gambar 1. Diagram Alur Penelitian tentang Kedudukan Keputusan Pemerintah dalam Keadaan Darurat Digital

III. HASIL DAN PEMBAHASAN

Penelitian ini menemukan bahwa tindakan pemerintah Indonesia dalam menghadapi keadaan darurat digital belum memiliki landasan konstitusional yang kuat dan rinci. Berdasarkan analisis terhadap peraturan perundang-undangan dan studi kasus insiden siber, terlihat adanya kesenjangan antara kebutuhan respons cepat pemerintah dan prinsip-prinsip konstitusional seperti legalitas, proporsionalitas, dan akuntabilitas. Dalam praktiknya, beberapa tindakan diambil berdasarkan diskresi eksekutif yang luas, tanpa pengawasan legislatif maupun yudisial yang memadai.

Analisis terhadap regulasi nasional seperti Undang-Undang ITE dan peraturan Badan Siber dan Sandi Negara (BSSN) menunjukkan bahwa kerangka hukum saat ini lebih fokus pada pencegahan serangan siber secara umum, bukan pada pengaturan mekanisme keadaan darurat digital secara spesifik. Tidak terdapat aturan prosedural yang mengatur syarat, tata cara, atau batasan tindakan pemerintah dalam kondisi krisis digital. Akibatnya, kebijakan darurat yang diambil cenderung bersifat ad hoc dan berpotensi mengabaikan hak konstitusional warga negara.

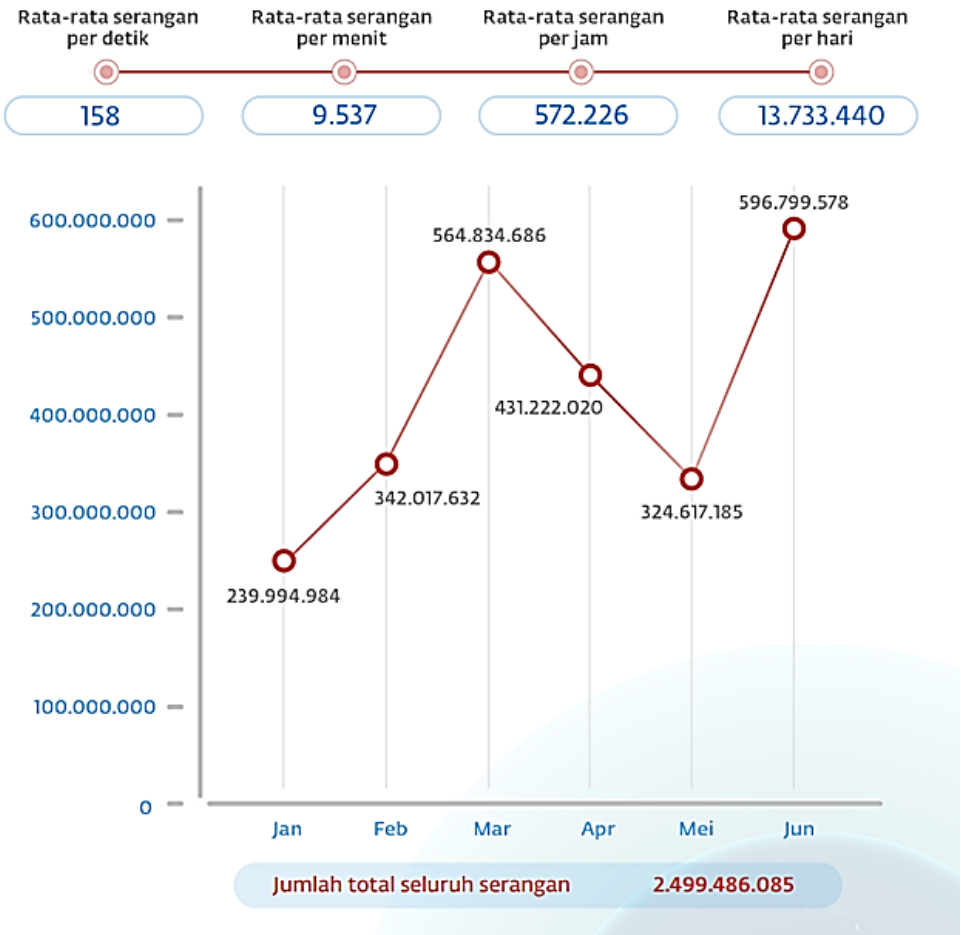
Temuan utama lainnya menunjukkan bahwa dalam beberapa kasus insiden siber, pemerintah mengambil langkah-langkah seperti pemutusan akses internet lokal atau nasional tanpa mekanisme pengujian proporsionalitas yang ketat. Hal ini bertentangan dengan prinsip-prinsip demokrasi yang mewajibkan pembatasan hak dasar harus dilakukan secara hati-hati, terbatas, dan didasarkan pada hukum yang jelas. Untuk memperjelas hasil penelitian, analisis kebijakan ini disajikan pada tabel 1.

Tabel 1. Analisis Kesesuaian Kebijakan Pemerintah dengan Prinsip Konstitusional

Prinsip Konstitusi	Temuan Lapangan	Evaluasi
Legalitas	Tidak semua tindakan berbasis regulasi khusus *cyber emergency*	Lemah
Proporsionalitas	Beberapa tindakan bersifat overbroad (pemutusan akses massal)	Tidak proporsional
Akuntabilitas	Pengawasan legislatif dan yudisial minim terhadap tindakan darurat	Rendah
Perlindungan HAM	Risiko pelanggaran hak kebebasan berpendapat dan akses informasi tinggi	Bermasalah

Sumber: Hasil Analisis Penelitian, 2025

Sebagai tambahan, gambaran tentang tren insiden serangan siber di Indonesia juga menjadi dasar menguatkan perlunya kerangka konstitusional yang jelas, seperti yang ditunjukkan dalam gambar 2.



Gambar 2. Tren Jumlah Insiden Siber di Indonesia 2020–2024 (Sumber: Laporan Tahunan BSSN, 2024)

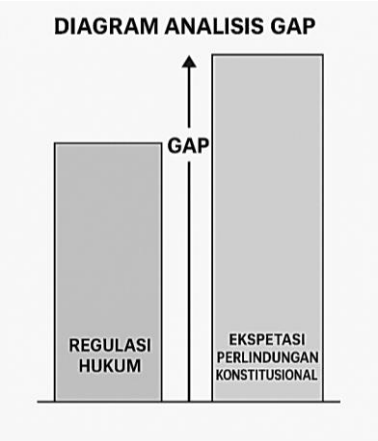
Dalam studi ini juga ditemukan bahwa model pendekatan pemerintah Indonesia lebih reaktif dibandingkan preventif, sebagaimana dapat dilihat dalam kecenderungan kebijakan yang diterapkan pasca-insiden besar. Tabel 2 menunjukkan pendekatan kebijakan pemerintah terhadap insiden siber

Tabel 2. Pendekatan Kebijakan Pemerintah terhadap Insiden Siber

Tahun	Insiden Besar	Tindakan Pemerintah	Pendekatan
2020	Peretasan Data Dukcapil	Peningkatan enkripsi lokal	Reaktif
2022	Kebocoran data operator seluler	Pemutakhiran SOP keamanan server	Reaktif
2023	Peretasan situs KPU	Penyusunan Tim Respons Darurat Khusus	Reaktif

Sumber: Data Olahan Peneliti dari Laporan Resmi dan Berita Nasional, 2025

Untuk memperlihatkan seberapa besar kesenjangan antara regulasi hukum dan ekspektasi perlindungan konstitusional, Gambar 3 menunjukkan diagram analisis gap.



Gambar 3. Gap Antara Regulasi dan Perlindungan Konstitusional *(Sumber: Hasil Olahan Peneliti, 2025)*

Dengan demikian, temuan dalam bagian ini menunjukkan adanya kebutuhan mendesak untuk menyusun regulasi baru yang secara eksplisit mengatur prosedur, batasan, serta mekanisme pengawasan terhadap tindakan pemerintah dalam keadaan darurat digital, agar sejalan dengan prinsip-prinsip negara hukum yang demokratis.

Pembahasan

Temuan penelitian ini memperlihatkan bahwa dalam konteks darurat digital, Indonesia belum sepenuhnya menginternalisasi prinsip-prinsip konstitusional dalam kebijakan yang diambil pemerintah. Padahal, dalam sistem negara hukum, keadaan darurat sekalipun tetap harus tunduk pada aturan hukum yang jelas, terbuka, dan akuntabel. Fenomena ini sejalan dengan temuan (Zysset, 2022) dan (Malíř & Grinc, 2024) yang menegaskan bahwa dalam situasi krisis, pembatasan hak hanya dapat dibenarkan jika dilakukan berdasarkan hukum, diperlukan secara ketat, dan proporsional.

Perbandingan dengan praktik negara lain menunjukkan bahwa beberapa negara, seperti Jerman dan Kanada, telah mengadopsi regulasi khusus untuk menangani *cyber emergency*, yang mencakup ketentuan deklarasi darurat, masa berlaku, pembatasan hak-hak tertentu, serta mekanisme pengujian yudisial terhadap tindakan pemerintah. Pendekatan ini memberikan model yang baik bagi Indonesia

untuk memperkuat legitimasi konstitusional dalam menghadapi ancaman digital, sekaligus menjaga keseimbangan antara keamanan nasional dan perlindungan hak-hak warga negara.

Kesenjangan yang ditemukan antara norma hukum positif dan praktik nyata tindakan pemerintah dalam *cyber emergency* juga menunjukkan adanya risiko akumulasi kekuasaan eksekutif tanpa kontrol memadai. Hal ini berpotensi menciptakan kondisi "darurat yang dilegalkan" (legality of emergency) yang bertentangan dengan prinsip negara demokrasi. Dalam konteks digital, kecenderungan untuk memperluas kekuasaan negara tanpa batas hukum yang ketat akan memperlemah kepercayaan publik terhadap pemerintah dan menimbulkan masalah legitimasi yang serius.

Implikasi penting dari hasil penelitian ini adalah perlunya penyusunan kerangka hukum khusus tentang *cyber emergency* yang berbasis konstitusi. Regulasi ini harus mengatur prosedur deklarasi darurat digital, kriteria pembatasan hak, mekanisme kontrol legislatif dan yudisial, serta kewajiban pemerintah untuk mempertanggungjawabkan setiap tindakan yang diambil. Regulasi semacam ini akan memastikan bahwa tindakan dalam keadaan darurat tidak menjadi alat pembenaran pelanggaran hak-hak dasar.

Penelitian ini juga menegaskan pentingnya integrasi prinsip digital constitutionalism dalam hukum nasional. Dalam era informasi, perlindungan terhadap hak digital seperti kebebasan berekspresi, hak atas privasi, dan hak atas akses informasi menjadi semakin penting untuk dijamin, bahkan dalam kondisi darurat. Oleh karena itu, pendekatan hukum tata negara Indonesia ke depan harus lebih responsif terhadap dinamika ruang digital dan tidak semata-mata mengadopsi pendekatan konvensional terhadap keadaan darurat.

Meskipun penelitian ini memberikan kontribusi penting dalam memperkaya diskursus mengenai kedudukan tindakan pemerintah dalam keadaan darurat digital, terdapat beberapa keterbatasan yang perlu diakui. Penelitian ini berfokus pada konteks Indonesia tanpa melakukan analisis empiris lapangan secara mendalam, seperti wawancara dengan pembuat kebijakan atau analisis terhadap kasus-kasus litigasi konkret di pengadilan. Selain itu, penelitian ini mengandalkan data sekunder yang tersedia secara publik, sehingga interpretasi terhadap praktik kebijakan mungkin belum sepenuhnya mencerminkan kompleksitas politik internal dalam pengambilan keputusan darurat.

Berdasarkan keterbatasan tersebut, rekomendasi untuk penelitian selanjutnya adalah memperluas studi dengan pendekatan empiris, misalnya melalui wawancara mendalam dengan pembuat kebijakan, legislator, dan aktor masyarakat sipil untuk memahami dinamika aktual dalam proses pengambilan keputusan darurat digital. Selain itu, perlu dilakukan studi perbandingan hukum secara sistematis dengan negara-negara lain yang telah memiliki regulasi *cyber emergency* berbasis konstitusi, guna menggali praktik-praktik terbaik yang dapat diadopsi di Indonesia. Penelitian di masa depan juga disarankan untuk mengkaji peran lembaga pengawasan independen dalam mengontrol tindakan pemerintah dalam situasi darurat digital, sebagai upaya untuk memperkuat prinsip akuntabilitas dalam negara hukum demokratis.

IV. KESIMPULAN

Penelitian ini menunjukkan bahwa tindakan pemerintah Indonesia dalam menghadapi keadaan darurat digital masih menghadapi tantangan serius dari perspektif hukum tata negara. Meskipun ada kebutuhan mendesak untuk merespons ancaman di ruang siber, langkah-langkah yang diambil sering kali belum berlandaskan pada kerangka hukum yang spesifik dan konstitusional. Analisis terhadap regulasi yang ada dan praktik kebijakan menunjukkan bahwa prinsip legalitas, proporsionalitas, akuntabilitas, serta perlindungan hak asasi manusia belum sepenuhnya diintegrasikan dalam pengelolaan darurat digital. Ketidakhadiran mekanisme pengawasan legislatif dan yudisial yang kuat atas tindakan eksekutif dalam keadaan darurat memperbesar risiko terjadinya pelanggaran hak-hak konstitusional warga negara dan penyalahgunaan kekuasaan.

Oleh karena itu, perlu ada pembaruan hukum yang mengatur secara rinci tentang prosedur, batasan, dan kontrol terhadap kebijakan *cyber emergency* dalam kerangka konstitusi Indonesia. Penelitian ini menegaskan bahwa supremasi konstitusi harus tetap menjadi landasan utama, bahkan dalam situasi krisis digital. Konsep digital constitutionalism perlu diinternalisasikan ke dalam sistem hukum nasional agar perlindungan terhadap hak-hak digital warga negara tetap terjamin. Dengan membangun regulasi yang berbasis konstitusionalitas, respons negara terhadap ancaman siber dapat menjadi lebih legitimate, transparan, dan demokratis, sekaligus menjaga kepercayaan publik terhadap pemerintah dalam era digital yang semakin kompleks.

REFERENCES

Abdelkader, S., Amissah, J., Kinga, S., Mugerwa, G., Emmanuel, E., Mansour, D. E. A., Bajaj, M., Blazek, V., & Prokop, L. (2024). Securing modern power systems: Implementing comprehensive strategies to enhance resilience and reliability against *cyber*-attacks. *Results in Engineering*, *23*. https://doi.org/10.1016/j.rineng.2024.102647

Adiprasetio, J., Rahmawan, D., Wibowo, K. A., Aliifa, D. N., & Hartanto, R. D. (2024). Shrinking civic space and the media: How Indonesian media frame environmental issues. *Journal of Civil Society*, *20*(3), 249–268. https://doi.org/10.1080/17448689.2024.2358924

Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). *Cyber* security: State of the art, challenges and future directions. *Cyber Security and Applications*, *2*. https://doi.org/10.1016/j.csa.2023.100031

Afaq, S. A., Husain, M. S., Bello, A., & Sadia, H. (2022). A Critical Analysis of *Cyber* Threats and Their Global Impact. *Computational Intelligent Security in Wireless Communications*, 201–220. https://doi.org/10.1201/9781003323426-12

Alam, M. M., Fawzi, A. M., Islam, M. M., & Said, J. (2022). Impacts of COVID-19 pandemic on national security issues: Indonesia as a case study. *Security Journal*, *35*(4), 1067–1086. https://doi.org/10.1057/s41284-021-00314-1

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Raymond Choo, K. K. (2022). The role of national *cyber*security strategies on the improvement of *cyber*security education. *Computers and Security*, *119*. https://doi.org/10.1016/j.cose.2022.102754

Anastasi, A. (2023). Rule of Law in Times of Emergency. *Encyclopedia of Contemporary Constitutionalism*, 1–

17. https://doi.org/10.1007/978-3-319-31739-7_223-1

Anggoro, F., Caraka, R. E., Prasetyo, F. A., Ramadhani, M., Gio, P. U., Chen, R. C., & Pardamean, B. (2022). Revisiting Cluster Vulnerabilities towards Information and Communication Technologies in the Eastern Island of Indonesia Using Fuzzy C Means. *Sustainability (Switzerland)*, *14*(6). https://doi.org/10.3390/su14063428

Arifin, S. (2022). Post-Pandemic Legislation in Indonesia: A Virtual Platform for Future Legislative Options? *International Journal of Parliamentary Studies*, *2*(2), 240–262.

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of *Cyber* Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics (Switzerland)*, *12*(6). https://doi.org/10.3390/electronics12061333

Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2022). Defining *Cyber* Security and *Cyber* Security Risk within a Multidisciplinary Context using Expert Elicitation. *Risk Analysis*, *42*(8), 1643–1669. https://doi.org/10.1111/risa.13687

Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., López de Prado, M., Herrera-Viedma, E., & Herrera, F. (2023). Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. *Information Fusion*, *99*. https://doi.org/10.1016/j.inffus.2023.101896

Fung, C. J. (2022). China's use of rhetorical adaptation in development of a global *cyber* order: a case study of the norm of the protection of the public core of the internet. *Journal of Cyber Policy*, *7*(3), 256–274. https://doi.org/10.1080/23738871.2023.2178946

Jiang, M. (2024). Models of State Digital Sovereignty From the Global South: Diverging Experiences From China, India and South Africa. *Policy and Internet*. https://doi.org/10.1002/poi3.427

Lehto, M. (2022). *Cyber*-Attacks Against Critical Infrastructure. *Computational Methods in Applied Sciences*, *56*, 3–42. https://doi.org/10.1007/978-3-030-91293-2_1

Li, Z., Zhang, W., Zhang, H., Gao, R., & Fang, X. (2024). Global Digital Compact: A Mechanism for the Governance of Online Discriminatory and Misleading Content Generation. *International Journal of Human-Computer Interaction*. https://doi.org/10.1080/10447318.2024.2314350

Luo, Y. (2024). Paradigm shift and theoretical implications for the era of global disorder. *Journal of International Business Studies*, *55*(2), 127–135. https://doi.org/10.1057/s41267-023-00659-2

Madnick, B., Huang, K., & Madnick, S. (2024). The evolution of global *cyber*security norms in the digital age: A longitudinal study of the *cyber*security norm development process. *Information Security Journal*, *33*(3), 204–225. https://doi.org/10.1080/19393555.2023.2201482

Mahaswa, R. K., Gebbyano, N., & Hardiyanti. (2025). Bioinspired technology and the uncanny Anthropocene. *Technology in Society*, *81*. https://doi.org/10.1016/j.techsoc.2024.102801

Malíř, J., & Grinc, J. (2024). Fundamental rights limitations in states of emergency: The Czech pattern. *States of Emergency and Human Rights Protection: The Theory and Practice of the Visegrad Countries*, 103–123. https://doi.org/10.4324/9781032637815-8

Muhidin, Suparman, E., Perwira, I., & Hamzah, M. G. (2023). Digital Acceleration During Covid-19 Pandemic: How the Indonesian Constitutional Court Brings the Citizens Justice. *International Journal for Court Administration*, *14*(2), 1–19. https://doi.org/10.36745/ijca.504

Nampewo, Z., Mike, J. H., & Wolff, J. (2022). Respecting, protecting and fulfilling the human right to health. *International Journal for Equity in Health*, *21*(1). https://doi.org/10.1186/s12939-022-01634-3

Prasetyoningsih, N., Rochimah, T. H. N., & Istiqomah, N. R. (2025). The State Authority to Limit Citizens' Digital Rights by Restricting Internet Access. *Lecture Notes in Networks and Systems*, *1281 LNNS*, 157–168. https://doi.org/10.1007/978-3-031-83520-9_15

Radanliev, P. (2024). *Cyber* diplomacy: defining the opportunities for *cyber*security and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. *Journal of Cyber Security Technology*, 1–51. https://doi.org/10.1080/23742917.2024.2312671

Raghupathi, W., Raghupathi, V., & Saharia, A. (2023). Analyzing Health Data Breaches: A Visual Analytics Approach. *AppliedMath*, *3*(1), 175–199. https://doi.org/10.3390/appliedmath3010011

Rahman, R. A., & Tang, S. M. (2022). Fake News and Internet Shutdowns in Indonesia: Symptoms of Failure to Uphold Democracy. *Constitutional Review*, *8*(1), 151–183. https://doi.org/10.31078/consrev816

Rohayati, Y., & Abdillah, A. (2024). Digital Transformation for Era Society 5.0 and Resilience: Urgent Issues from Indonesia. *Societies*, *14*(12). https://doi.org/10.3390/soc14120266

Rubinst, R. R., & Barzilaif, G. (2022). Only Sovereignty? Global Emergencies Between Domestic and International Law. *Cornell International Law Journal*, *55*(2), 139–186.

Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., Khan, I., Hewage, C., & Platts, J. (2022). *Cyber*security, Data Privacy and Blockchain: A Review. *SN Computer Science*, *3*(2). https://doi.org/10.1007/s42979-022-01020-4

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). *Cyber* Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

Zysset, A. (2022). To Derogate or to Restrict? The COVID-19 Pandemic, Proportionality and the Justificatory Gap in European Human Rights Law. *Jus Cogens*, *4*(3), 285–301. https://doi.org/10.1007/s42439-022-00065-6