MENDAPO Journal of Administration Law

ISSN Print: 2774-7840 ISSN Online: 2774-7905

Volume 6, Nomor 2 | 2025 | Halaman 144-162

Jurnal Office: Bagian Hukum Administrasi Negara, Fakultas Hukum Universitas Jambi, Jambi 36361

DOI. https://doi.org/10.22437/mendapo.v6i2.46550

The Harmonization of Administrative Regulatory Arrangements Toward Public Institutional Accountability in Handling Cybercrime in Indonesia

Harmonisasi Penataan Regulasi Administratif terhadap Akuntabilitas Lembaga Publik dalam Penanganan Cybercrime di Indonesia

Nuruzzaman MS

Faculty of Law, Department of Legal Studies, Universitas Nahdaltul Ulama Surakarta

Caesarhukum@gmail.com

Siti Fatimah

Faculty of Social Sciences and Law, Univet Bantara Sukoharjo

Sitifatimahshmh2022@gmail.com

Abstract

The rapid development of information technology has brought both positive impacts and significant challenges to public governance, particularly in addressing digital crimes. In Indonesia, the handling of cybercrime is not solely within the domain of criminal law but also requires the active involvement of state institutions within the framework of administrative law. Institutions such as the Ministry of Communication and Digital Affairs, the National Cyber and Crypto Agency, as well as other agencies like the Indonesian National Police and the Attorney General's Office, play strategic roles in maintaining the security and order of the national digital space. However, bureaucratic realities reveal persistent issues, including overlapping authorities, weak inter-agency coordination, and suboptimal implementation of administrative functions. Therefore, the harmonization and synchronization of administrative regulations have become urgent to ensure policy alignment, clear division of institutional responsibilities, and the reinforcement of transparency and accountability principles in digital governance. This article aims to analyze how the harmonization and synchronization of administrative regulations can enhance the accountability of public institutions in addressing digital crimes in Indonesia, using a normative juridical approach and descriptive-analytical methods.

***Keywords**: Cybercrime; Administrative Law; Regulatory Harmonization.*

Abstrak

Perkembangan teknologi informasi yang pesat membawa dampak positif sekaligus tantangan besar dalam tata kelola pemerintahan, khususnya dalam penanganan kejahatan digital. Di Indonesia, penanganan *cybercrime* tidak hanya menjadi domain hukum pidana, tetapi juga memerlukan peran aktif lembaga negara dalam kerangka hukum administrasi negara. Lembaga-lembaga seperti Kementerian Komunikasi dan Digital, Badan Siber dan Sandi Negara, serta lembaga lain seperti Kepolisian Negara Republik Indonesia dan Kejaksaan Agung memiliki fungsi strategis dalam menjaga keamanan dan ketertiban ruang digital nasional. Namun, realitas birokrasi menunjukkan masih adanya tumpang tindih kewenangan, lemahnya koordinasi antar instansi, dan belum optimalnya pelaksanaan fungsi administratif. Oleh karena itu, harmonisasi dan sinkronisasi regulasi administratif menjadi hal yang mendesak untuk memastikan adanya keselarasan kebijakan, pembagian tugas yang jelas, serta penguatan prinsip transparansi dan akuntabilitas dalam tata kelola keamanan digital. Artikel ini bertujuan untuk menganalisis bagaimana harmonisasi dan sinkronisasi regulasi administratif dapat mendorong peningkatan akuntabilitas lembaga publik dalam penanganan kejahatan digital di Indonesia, dengan menggunakan pendekatan yuridis normatif dan metode deskriptif analitis.

Kata Kunci: *Cybercrime,* Hukum Administrasi Negara, Harmonisasi Regulasi.

A. Pendahuluan

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan mendasar dalam cara negara berinteraksi dengan masyarakat. Teknologi digital menjadi sarana utama dalam penyelenggaraan administrasi pemerintahan, pelayanan publik, serta proses hukum. Namun, di balik manfaat yang ditawarkan, muncul tantangan serius berupa meningkatnya tindak pidana di ruang siber atau yang lazim disebut *cybercrime*. Kejahatan ini meliputi berbagai bentuk seperti pencurian data pribadi, penipuan daring, serangan siber terhadap infrastruktur digital negara, serta penyebaran konten ilegal melalui *platform digital.*[1]

Hukum pidana siber merupakan cabang dari hukum pidana yang khusus mengatur tentang tindak pidana yang dilakukan dengan menggunakan teknologi informasi dan komunikasi, terutama internet. Kejahatan siber, juga dikenal sebagai kejahatan dunia maya atau *cybercrime*, mencakup berbagai kegiatan ilegal yang memanfaatkan komputer, jaringan komputer, dan perangkat digital lainnya. Ruang

[1] Teguh Arifiyadi, *Cybercrime: Kejahatan Dunia Maya dan Penanggulangannya di Indonesia*, Jakarta: Rajagrafindo Persada, 2020, hlm. 55.

lingkup hukum pidana siber meliputi berbagai aspek yang berkaitan dengan pengaturan, pencegahan, penyelidikan, dan penindakan terhadap Kejahatan Siber.[2]

Perkembangan teknologi informasi dan komunikasi (TIK) mendorong peralihan berbagai aktivitas konvensional ke dalam bentuk digital. Transaksi perbankan, pengiriman dokumen, hingga aktivitas niaga kini dapat dilakukan melalui perangkat *mobile* seperti *smartphone* dan laptop, didukung oleh jaringan internet dan ketersediaan *hotspot* publik.[3] Transformasi ini membawa kemudahan, tetapi juga memunculkan risiko, termasuk meningkatnya kejahatan di dunia maya (*cybercrime*).[4] *Cybercrime* merupakan bentuk kejahatan yang dilakukan melalui atau terhadap sistem elektronik dan jaringan komputer, seperti peretasan, penipuan daring, dan penyebaran *malware.*[5]. Penanganannya tidak cukup hanya dengan hukum pidana, tetapi juga menuntut peran lembaga negara dalam kerangka hukum administrasi. Permasalahan seperti tumpang tindih kewenangan dan lemahnya koordinasi menunjukkan pentingnya harmonisasi dan sinkronisasi regulasi administratif antar instansi.

Indonesia sebagai negara dengan populasi pengguna internet yang sangat besar, yaitu mencapai lebih dari 210 juta pengguna pada tahun 2023 menurut laporan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), sangat rentan terhadap tindak pidana kejahatan digital.[6] Bentuk-bentuk kejahatan ini meliputi peretasan sistem *(hacking),* pencurian data pribadi *(data breach*), penipuan daring *(online fraud),* penyebaran informasi palsu *(hoaks),* penyalahgunaan media sosial, perjudian daring, serta eksploitasi seksual anak melalui internet. Kejahatan digital tidak hanya menimbulkan kerugian finansial, namun juga mengancam keamanan negara, merusak

[2] Muhammad Anthony Aldriano dan Mas Agus Priyambodo, "Cyber Crime Dalam Sudut Pandang Hukum Pidana," *Jurnal Kewarganegaraan* 6, no. 1 (2022).

[3] Budi Rahardjo, *Keamanan Sistem Informasi berbasis Internet*, Bandung: Informatika, 2006, hlm. 7.

[4] Oki Muraza dan Adi Nugroho, *Cyber Law: Aspek Hukum Teknologi Informasi*, Yogyakarta: Graha Ilmu, 2011, hlm. 23.

[5] Ridwan Khairandy, *Hukum Administrasi Negara dan Regulasi Dunia Siber*, Yogyakarta: FH UII Press, 2020, hlm. 88.

[6] Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), *Laporan Survei Internet Indonesia Tahun 2023*, (Jakarta: APJII, 2024), hlm. 5.

moral masyarakat, serta menurunkan kepercayaan publik terhadap sistem hukum dan keamanan digital nasional.

Laporan dari Badan Siber dan Sandi Negara (BSSN) menunjukkan bahwa selama tahun 2023, terdapat lebih dari 300 juta anomali serangan siber yang terdeteksi di berbagai sektor penting, termasuk pemerintahan, perbankan, pendidikan, dan infrastruktur vital.[7] Jumlah ini mengalami peningkatan signifikan dibandingkan tahun-tahun sebelumnya dan menunjukkan bahwa kejahatan digital bukan lagi sesuatu yang sporadis atau individual, melainkan telah menjadi bentuk kejahatan yang terorganisir, sistematis, dan bersifat lintas negara. Hal ini menimbulkan tantangan besar bagi penegakan hukum nasional yang selama ini lebih banyak berfokus pada bentuk-bentuk kejahatan konvensional.

Fenomena *cybercrime* bukan sekadar persoalan penegakan hukum pidana, tetapi juga merupakan isu tata kelola pemerintahan yang baik *(good governance)*. Dalam konteks negara hukum modern, *cybercrime* menuntut respons cepat dan sistematis dari berbagai lembaga negara yang bekerja dalam sistem administrasi publik. Oleh karena itu, hukum administrasi negara menjadi elemen penting dalam memastikan bahwa setiap lembaga negara menjalankan tugasnya secara akuntabel, transparan, dan bertanggung jawab.[8] Tanpa kerangka hukum administrasi yang jelas (tanpa adanya aturan hukum administrasi Negara yang tegas dan sistematis) maka lembaga-lembaga negara bisa menjalankan tugasnya secara tidak konsisten, tumpang tindih, atau bahkan menyimpang.

Dalam perspektif hukum administrasi negara, keberadaan kerangka hukum yang jelas, tegas, dan sistematis merupakan prasyarat utama bagi terselenggaranya pemerintahan yang tertib dan akuntabel. Aturan hukum administrasi berfungsi sebagai pedoman bagi lembaga negara dalam menjalankan kewenangan dan tanggung jawabnya sesuai dengan prinsip-prinsip legalitas, profesionalitas, serta akuntabilitas.[9]

---

[7] Badan Siber dan Sandi Negara, *Laporan Tahunan Keamanan Siber Nasional 2023*, (Jakarta: BSSN, 2024), hlm. 12–13

[8] Syabran Jabar, Akuntabilitas Dan Transparansi Dalam Perspektif Hukum Administrasi Negara, *Gudang Jurnal Multidisiplin Ilmu*, Vol. 12, No. 12 (2024), hlm. 720-728.

[9] Philipus M. Hadjon, *Pengantar Hukum Administrasi Indonesia*, Yogyakarta: Gadjah Mada University Press, 2005, hlm. 25.

Tanpa adanya aturan yang memadai, lembaga-lembaga negara berpotensi menjalankan tugasnya secara tidak konsisten, saling tumpang tindih, bahkan menyimpang dari fungsi dan batas kewenangan yang telah ditentukan oleh peraturan perundang-undangan. Kondisi ini tidak hanya menimbulkan ketidakteraturan dalam tata kelola pemerintahan, tetapi juga menghambat efektivitas pelayanan publik dan pelaksanaan fungsi pengawasan terhadap tindakan administrasi pemerintah. Oleh karena itu, penataan regulasi administratif yang terkoordinasi dan terintegrasi menjadi sangat penting agar setiap instansi memiliki kepastian hukum dalam bertindak serta dapat dimintai pertanggungjawaban atas setiap kebijakan yang diambil.[10]

Lembaga-lembaga seperti Kementerian Komunikasi dan Digital (Komdigi), Badan Siber dan Sandi Negara (BSSN), Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK), dan Badan Intelijen Negara (BIN) adalah contoh entitas yang memiliki kewenangan administratif untuk menangani atau setidaknya merespons kejahatan digital sesuai dengan fungsi institusionalnya. Namun, kewenangan tersebut belum diimbangi dengan sistem regulasi administratif yang mampu mengarahkan, membatasi, dan mengevaluasi kinerja masing-masing lembaga. Tidak sedikit kasus kebocoran data, penipuan digital, serta penyalahgunaan sistem elektronik yang tidak direspons secara efektif oleh lembaga terkait, bahkan sering kali tanpa kejelasan sanksi administratif atau pertanggungjawaban publik.[11]

Ketiadaan regulasi administratif yang komprehensif dan berorientasi pada akuntabilitas menyebabkan lemahnya pengawasan terhadap lembaga negara. Hal ini menunjukkan adanya ketimpangan antara kewenangan dan pertanggungjawaban. Padahal, dalam prinsip negara hukum yang demokratis, akuntabilitas merupakan fondasi utama dalam mencegah penyalahgunaan kekuasaan dan membangun

---

[10] Ridwan Khairandy, *Hukum Administrasi Negara dan Regulasi Dunia Siber*, Yogyakarta: FH UII Press, 2020, hlm. 90.

[11] Wahyudi Djafar, Hukum Perlindungan Data Pribadi di Indonesia: Lanskap Urgensi dan Kebutuhan Pembaharuan (2019), *Jurnal Law UGM*, hal 1-14 dalam https://www.google.com/search?q=Hukum+Perlindungan+Data+Pribadi+di+Indonesia%3A+Lanskap%2C+Urgensi+dan+Kebutuhan+Pembaruan1+UGM&oq=Hukum+Perlindungan+Data+Pribadi+di+Indonesia%3A+Lanskap%2C+Urgensi+dan+Kebutuhan+Pembaruan1+UGM&aqs=chrome..69i57.2039j0j7&sourceid=chrome&ie=UTF-8, diakses pada 4 Agustus 2025.

kepercayaan publik terhadap institusi Negara.[12] Menurut Philipus M. Hadjon, fungsi hukum administrasi negara adalah membatasi tindakan penguasa dan menjamin adanya perlindungan hukum bagi masyarakat terhadap tindakan administratif yang sewenang-wenang.[13]

Di tengah derasnya arus digitalisasi dan kompleksitas ancaman siber, dibutuhkan sistem regulasi administratif yang tidak hanya memadai secara substansi, tetapi juga implementatif. Regulasi ini harus mampu memberikan rambu-rambu hukum yang jelas bagi setiap lembaga negara dalam menjalankan peran dan fungsinya dalam penanganan *cybercrime.* Regulasi tersebut juga harus mencakup indikator kinerja, sistem pengawasan, evaluasi kebijakan, serta sanksi administratif terhadap kelalaian atau pelanggaran prosedur. Tanpa regulasi administratif yang kuat, negara akan gagal menjamin hak-hak warga negara di ruang digital, termasuk hak atas keamanan informasi dan perlindungan data pribadi.[14]

Maka dari itu, penelitian ini difokuskan untuk menganalisis harmonisasi dan sinkronisasi regulasi administratif dalam memperkuat akuntabilitas lembaga publik dalam penanganan *cybercrime* di Indonesia. Penelitian ini perlu diimbangi dengan konfirmasi terhadap berbagai kajian akademik dan preseden normatif, guna menilai sejauh mana regulasi administratif telah diimplementasikan dalam mengawal tugas lembaga publik yang menangani isu-isu digital. Dengan pendekatan yuridis normatif dan analisis kritis terhadap kebijakan yang berlaku, penelitian ini diharapkan dapat memberikan sumbangan konseptual dalam merancang arsitektur hukum administrasi negara yang responsif terhadap dinamika perkembangan teknologi informasi.

B. Metode Penelitian

Penelitian ini menggunakan jenis penelitian hukum normatif, yaitu suatu metode penelitian yang bertumpu pada studi kepustakaan dan menganalisis bahan-bahan hukum yang bersifat normatif, baik berupa peraturan perundang-undangan, putusan

---

[12] Jimly Asshiddiqie, *Penguatan Sistem Pemerintahan yang Demokratis*, (Jakarta: Konstitusi Press, 2005), hlm. 77.

[13] Philipus M. Hadjon, *Pengantar Hukum Administrasi Indonesia*, (Yogyakarta: Gadjah Mada University Press, 2011), hlm. 145.

[14] Kadek Rima Anggen Suari dan I Made Sarjana, Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia, *Jurnal Analisis Hukum (JAH)*, Vol. 6, No. 1 April 2023, hlm. 132-146.

pengadilan, maupun doktrin dari para ahli hukum. Penelitian hukum normatif tidak bertujuan untuk menguji data empiris di lapangan, melainkan untuk mengkaji norma-norma hukum sebagai objek utama penelitian, serta menilai kesesuaian antara kaidah hukum yang berlaku dengan realitas normatif yang ideal.[15] Penelitian hukum yuridis normatif atau penelitian hukum normatif pada dasarnya merupakan suatu kegiatan yang akan mengkaji aspek-aspek (untuk menyelesaikan masalah-masalah yang ada di dalam) internal dari hukum positif.[16]

Penelitian ini, menggunakan dua pendekatan utama, yaitu pendekatan perundang-undangan *(statute approach)* dan pendekatan konseptual *(conceptual approach)***.** Pendekatan perundang-undangan digunakan untuk mengkaji peraturan-peraturan yang berkaitan langsung dengan penataan regulasi administratif dan pengaturan mengenai kewenangan serta akuntabilitas lembaga publik dalam menangani kejahatan digital. Beberapa regulasi yang menjadi fokus analisis meliputi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Peraturan Presiden Nomor 53 Tahun 2017 tentang BSSN, serta Peraturan Menteri Kominfo dan peraturan lembaga lainnya yang mengatur pengelolaan sistem elektronik, tata kelola data, dan penanganan insiden siber.[17] Sementara itu, pendekatan konseptual digunakan untuk mengeksplorasi teori-teori hukum yang berkaitan dengan hukum administrasi negara**,** prinsip akuntabilitas publik**,** serta harmonisasi regulasi dalam konteks tata kelola digital modern. Dengan pendekatan ini, peneliti berusaha menggali dan menafsirkan konsep-konsep seperti *good governance*, *administrative liability*, serta hubungan antara prinsip-prinsip hukum administrasi dengan praktik institusional lembaga negara yang menangani *cybercrime*.

Sumber data dalam penelitian ini terdiri dari bahan hukum primer berupa peraturan perundang-undangan, dan bahan hukum sekunder berupa literatur ilmiah, jurnal hukum, buku referensi, hasil penelitian sebelumnya, serta pandangan dari

---

[15] Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*, Jakarta: Rajawali Pers, 2014, hlm. 13.

[16] Kornelius Benuf dan Muhamad Azhar, Metodologi Penelitian Hukum sebagai Instrumen Mungurai Permasalahan Hukum Kontemorer, *Jurnal Gema Keadilan*, ISSN: 0852-011, Volume 7 Edisi I, Juni 2020, hlm. 20-33.

[17] Peter Mahmud Marzuki, *Penelitian Hukum*, (Jakarta: Kencana Prenada Media Group, 2010), hlm. 133-134.

pakar hukum administrasi dan *cyber law*. Selain itu, juga digunakan bahan hukum tersier seperti kamus hukum dan ensiklopedia hukum sebagai pelengkap pemahaman atas istilah dan konteks normatif tertentu. Metode analisis yang digunakan bersifat deskriptif-kualitatif, yaitu dengan cara mendeskripsikan isi normatif dari peraturan dan literatur yang dikaji, kemudian menganalisisnya secara sistematis untuk menilai harmonisasi penataan regulasi administratif dalam mendorong akuntabilitas lembaga publik. Penilaian ini dilakukan melalui identifikasi apakah regulasi yang berlaku sudah mampu mengarahkan dan membatasi pelaksanaan kewenangan lembaga, sejauh mana peraturan tersebut menciptakan mekanisme pengawasan dan pertanggungjawaban, serta bagaimana regulasi tersebut diimplementasikan dalam praktik administratif lembaga publik saat menangani kasus-kasus kejahatan digital.[18]

C. Pembahasan Dan Analisis

1. Urgensi Harmonisasi Regulasi Administratif dalam Penanganan *Cybercrime*

Era digital saat ini, ancaman *cybercrime* semakin kompleks dan berkembang secara dinamis, baik dalam bentuk maupun modus operandinya. Berbeda dengan kejahatan konvensional, kejahatan digital bersifat lintas batas (*borderless*), tidak mengenal yurisdiksi geografis yang kaku, serta melibatkan sistem elektronik yang seringkali tidak terawasi secara optimal oleh negara. Oleh karena itu, pendekatan penegakan hukum terhadap *cybercrime* tidak bisa lagi hanya berpijak pada hukum pidana saja, tetapi harus diimbangi dengan penguatan sistem administrasi negara dalam aspek regulasi, koordinasi kelembagaan, dan kontrol kebijakan.[19]

Tindak Pidana Siber di Indonesia telah menjadi ancaman serius, terutama di sektor ekonomi yang rentan, di tengah perkembangan terus-menerus era digital. Kejahatan siber seperti pencurian data nasabah, penipuan online, perdagangan ilegal, dan serangan terhadap sistem perbankan terus meningkat.[20] Tren tersebut

---

[18] Jonner Marulitua Butarbutar, Revolusi Digital dan Tantangan Kriminologis: Analisis terhadap Tren Kriminalitas dalam Era Digitalisasi, *Media Hukum Indonesia (MHI)*, e-ISSN: 3032-6591, May-2025. Vol. 2, No. 6, pp 145-150.

[19] Andi Hamzah, *Aspek-Aspek Pidana di Bidang Komputer*, Jakarta: Sinar Grafika, 2020, hlm. 78.

[20] Nabila Aulia Agustin dan Refania Meilani Firdos, "Studi Literatur : Ancaman Cybercrime di Indonesia dan Pentingnya Pemahaman akan Fenomena Kejahatan

menimbulkan kerugian finansial bagi masyarakat dan mengancam stabilitas keamanan nasional dan pertumbuhan ekonomi. Upaya penegakan hukum perlu disesuaikan dan diperkuat untuk mengatasi tantangan yang dihadapi dalam lingkungan digital yang terus berubah dan berkembang pesat ini, karena penegakan hukum menghadapi berbagai masalah, terutama dalam upaya untuk mengharmonisasikan regulasi yang berkaitan dengan penggunaan internet.

Hukum administrasi negara memiliki fungsi strategis dalam mengatur bagaimana kekuasaan negara dijalankan oleh aparatur pemerintahan. Di sinilah pentingnya penataan regulasi administratif: sebagai alat untuk membatasi, mengatur, dan mengarahkan kewenangan lembaga publik agar selaras dengan prinsip akuntabilitas dan perlindungan hak warga negara. Tanpa regulasi administratif yang baik, lembaga-lembaga negara rentan bertindak secara tidak efisien, tumpang tindih, atau bahkan abai terhadap tanggung jawab yang diemban dalam ruang digital.[21]

Harmonisasi regulasi administratif merupakan kebutuhan mendesak dalam tata kelola penanganan kejahatan siber di Indonesia. Saat ini, peran dan kewenangan lembaga seperti Kementerian Komunikasi dan Digital (Komdigi), Badan Siber dan Sandi Negara (BSSN), Kepolisian Negara Republik Indonesia (Polri), dan Kejaksaan Agung belum terkoordinasi secara optimal karena belum adanya regulasi administratif yang secara eksplisit mengatur pembagian fungsi dan mekanisme koordinasi antar lembaga. Ketidakharmonisan ini menciptakan tumpang tindih kewenangan dan ketidakjelasan garis koordinasi, yang pada akhirnya menyebabkan inefisiensi birokrasi dan lemahnya respons terhadap insiden siber. Dalam praktiknya, koordinasi antar instansi sering bersifat sektoral dan ad-hoc, sehingga penanganan insiden siber berjalan tidak sistematis dan rentan memperlambat upaya mitigasi maupun penegakan hukum. BSSN yang seharusnya menjadi koordinator nasional pun belum memiliki pijakan hukum yang kuat untuk memimpin secara administratif.

Digital," *Jurnal Mahasiswa Teknik Informatika 3*, no. 1 (2024): 126-31, https://doi.org/10.35473/jamastika.v3i1.2841

[21] HR. Ridwan, *Hukum Administrasi Negara*, Jakarta: Rajawali Pers, 2019, hlm. 45-47.

Sebagaimana dinyatakan dalam kajian Hanif bahwa belum ada keterpaduan antara kewenangan teknis dan administratif antar institusi dalam sistem keamanan siber nasional.[22] Hal ini diperkuat oleh Kurniawan dan Alamsyah yang menyatakan bahwa belum adanya harmonisasi regulasi menyebabkan tumpang tindih kewenangan antara BSSN, Komdigi, dan aparat penegak hukum lainnya.[23] Oleh karena itu, diperlukan pembaruan regulasi dan pembentukan sistem koordinasi administratif yang terstruktur dan mengikat, agar semua lembaga dapat bekerja secara sinergis dan akuntabel dalam menghadapi tantangan kejahatan siber di Indonesia.[24]

Praktiknya, berbagai peraturan perundang-undangan di Indonesia belum terintegrasi secara harmonis, terutama terkait penanganan kejahatan siber. Sebagai contoh, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang telah diubah menjadi UU Nomor 19 Tahun 2016, belum secara eksplisit mengatur mekanisme koordinasi administratif antar lembaga dalam pengelolaan kasus *cybercrime*. Hal ini tercermin dari keterbatasan kewenangan BSSN yang tidak memiliki status Penyidik Pegawai Negeri Sipil (PPNS), sehingga ia tidak bisa menindaklanjuti notifikasi temuan keamanan secara mandiri yang menjadi tanggung jawab administratif Kominfo (sekarang Komdigi).[25]

Akibatnya, tanggung jawab administratif lembaga seperti BSSN, Komdigi, serta Polri dan Kejaksaan, menjadi tidak terstruktur, sulit dievaluasi secara objektif, dan memicu tumpang tindih kewenangan yang melemahkan efektivitas respons terhadap serangan siber (karena belum ada payung hukum jelas yang

---

[22] M. Hanif, Koordinasi Antar Lembaga dalam Sistem Keamanan Siber Nasional, *Jurnal Ilmu Administrasi Negara*, Vol. 10 No. 1 (2020): hlm. 51-52.

[23] Kurniawan dan Alamsyah, Kelembagaan Penanganan Kejahatan Siber di Indonesia: Kajian terhadap Kewenangan BSSN, *Jurnal Hukum & Pembangunan*, Vol. 51 No. 1 (2021): hlm. 125-128.

[24] Wahyudi Djafar, Urgensi Pembentukan RUU Keamanan dan Ketahanan Siber, *Jurnal Media Hukum*, Vol. 27 No. 2 (2020): hlm. 221-223.

[25] https://www.suara.com/tekno/2023/08/23/010500/bssn-terkendala-jalankan-fungsi-karena-uu-ite, diakses 4 Mei 2025.

mengikat koordinasi administratif).[26] Lemahnya integrasi kelembagaan dalam kerangka hukum administratif telah menjadi hambatan struktural utama dalam membangun tata kelola keamanan siber yang efektif di Indonesia.

Oleh karena itu, harmonisasi regulasi administratif menjadi urgensi mutlak yang harus segera diwujudkan, baik melalui revisi regulasi yang sudah ada maupun penyusunan undang-undang baru seperti RUU Keamanan Siber yang menyelaraskan fungsi dan koordinasi lintas lembaga.

2. Kewenangan Administratif Lembaga Publik dan Tantangannya

Penanganan kejahatan digital tidak dapat dipisahkan dari peran lembaga publik yang memiliki kewenangan administratif dalam tata kelola ruang siber di Indonesia. Berbagai lembaga negara telah diberikan mandat untuk menjalankan fungsi-fungsi strategis dalam mengatur, mengawasi, serta melakukan tindakan administratif terhadap aktivitas digital yang berpotensi atau terbukti melanggar hukum. Namun, dalam praktiknya, implementasi kewenangan tersebut menghadapi berbagai kendala struktural, prosedural, dan normatif.

2.1. Lembaga-Lembaga Kunci dan Fungsi Administratifnya

Beberapa lembaga publik utama yang berperan dalam penanganan *cybercrime* melalui pendekatan administratif antara lain:

a. Kementerian Komunikasi dan Digital (Komdigi) memiliki kewenangan administratif berdasarkan berbagai regulasi, seperti Memberikan izin dan mendaftarkan Penyelenggara Sistem Elektronik (PSE), Mengawasi konten dan sistem elektronik, dan Menjatuhkan sanksi administratif terhadap PSE yang melanggar ketentuan, misalnya berupa teguran, pembatasan akses, hingga pemblokiran situs.[27] Namun, pelaksanaan fungsi ini sering tidak konsisten. Sebagai contoh, kebijakan pemblokiran situs atau aplikasi kerap dilakukan tanpa mekanisme keberatan yang transparan, dan proses evaluasi terhadap pemilik sistem elektronik pun

[26] https://www.antaranews.com/berita/3692379/bssn-sebut-tugas-dan-fungsinya-belum-optimal-karena-terkendala-uu-ite, diakses 5 Mei 2025.

[27] Peraturan Menteri Komunikasi dan Digital Nomor 1 Tahun 2025 tentang Organisasi dan Tata Kerja Kementerian Komunikasi dan Digital

belum berjalan maksimal. Hal ini menimbulkan pertanyaan tentang sejauh mana komdigi menjalankan fungsinya secara akuntabel.

b. Badan Siber dan Sandi Negara (BSSN), BSSN dibentuk melalui Peraturan Presiden Nomor 53 Tahun 2017 dengan fungsi Melakukan deteksi, perlindungan, dan respons terhadap insiden siber, Menetapkan kebijakan nasional di bidang keamanan siber, dan Membangun sistem keamanan informasi nasional. Meskipun memiliki wewenang luas, BSSN belum sepenuhnya mampu mengkoordinasikan seluruh institusi terkait keamanan siber. Ketiadaan payung hukum setingkat undang-undang dan minimnya keterlibatan publik dalam proses audit keamanan sistem elektronik menunjukkan lemahnya instrumen akuntabilitas administratif di lembaga ini.[28]

c. Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK), PPATK memiliki mandat administratif untuk menganalisis dan mengevaluasi transaksi keuangan mencurigakan, termasuk yang berkaitan dengan *cybercrime* seperti Penipuan daring (*online fraud*), Pencucian uang hasil tindak pidana digital, dan Kripto yang digunakan untuk transaksi ilegal. Namun, kerja PPATK sering kali terhambat koordinasi teknis dengan lembaga penindak dan pelapor. Selain itu, kurangnya transparansi hasil analisis administratif juga menyulitkan akuntabilitas lembaga ini kepada publik.[29]

d. Polri dan Kejaksaan. Meskipun dominan pada aspek penegakan hukum pidana, Polri dan Kejaksaan juga memiliki kewenangan administratif terbatas, seperti Melakukan penyitaan dan pemblokiran atas aset digital, dan Mengajukan permintaan informasi atau pemutusan akses digital ke lembaga lain. Namun, keterlibatan mereka dalam sistem administrasi pemerintahan siber masih bersifat reaktif dan belum terintegrasi secara administratif dengan sistem nasional penanganan cybercrime.

2.2. Tantangan Implementasi Kewenangan Administratif.

[28] Peraturan Presiden Republik Indonesia Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara

[29] Lihat: PPATK, *Laporan Tahunan 2023*, Jakarta, hlm. 43-44

Meskipun secara normatif masing-masing lembaga telah memiliki kewenangan, implementasi administratifnya menghadapi sejumlah tantangan utama:[30]

a. Tumpang Tindih dan Fragmentasi Kewenangan. Tidak adanya regulasi yang memayungi secara komprehensif tata kelola siber nasional menyebabkan setiap lembaga bekerja secara sektoral dan sporadic. Hal ini menyebabkan Kebingungan dalam alur koordinasi penanganan insiden, Lemahnya konsolidasi kebijakan dan Duplikasi kerja antar lembaga yang memboroskan sumber daya.
b. Ketiadaan SOP Terpadu Nasional. Belum adanya standar operasional prosedur (SOP) nasional dalam penanganan administratif kejahatan digital menyebabkan Tidak adanya standar waktu dan cara pelaporan insiden siber, Perbedaan parameter antara lembaga soal apa yang dianggap "kritis" atau "darurat" dan Masyarakat kesulitan memahami jalur pelaporan dan penyelesaian administratif.
c. Minimnya Sistem Evaluasi Kinerja dan Pengawasan Eksternal. Hingga saat ini, belum ada lembaga pengawas independen yang secara khusus bertugas mengevaluasi pelaksanaan kewenangan administratif lembaga-lembaga tersebut. Laporan tahunan lembaga siber tidak memuat indikator kinerja akuntabilitas, melainkan lebih banyak bersifat administratif formalitas. Tanpa pengawasan yang kuat, potensi penyalahgunaan wewenang atau kelalaian tidak dapat dicegah secara efektif.
d. Lemahnya Penegakan Sanksi Administratif Internal. Peraturan yang telah mengatur sanksi administratif seringkali tidak dijalankan. Misalnya, banyak PSE yang melanggar kewajiban perlindungan data tidak pernah diberikan sanksi berarti. Dalam praktiknya, sanksi administratif seringkali dipolitisasi atau tidak diproses karena konflik kepentingan antar institusi negara.

[30] https://siplawfirm.id/tantangan-dan-prospek-hukum-administrasi-negara-di-era-digital/?lang=id, diakses 05 Agustus 2025.

2.3. Dampak dari Ketidakefektifan Kewenangan Administratif

Kelemahan pelaksanaan kewenangan administratif berdampak besar terhadap efektivitas penegakan hukum *cybercrime* secara umum:

a. Masyarakat kehilangan kepercayaan pada kemampuan negara mengelola ruang digital
b. Kejahatan digital berulang karena tidak ada mekanisme pencegahan administratif yang kuat;
c. Institusi negara sulit dievaluasi, karena tidak adanya pelaporan publik dan indikator akuntabilitas;
d. Ketimpangan hukum antara pengguna digital dan pengelola sistem, yang berdampak pada pelanggaran hak warga negara.

Dengan demikian, memperjelas, mempertegas, dan mengintegrasikan kewenangan administratif lembaga publik menjadi suatu keharusan untuk mewujudkan tata kelola digital yang akuntabel, responsif, dan demokratis.

3. Analisis Regulasi Administratif yang Berlaku

Regulasi-regulasi yang telah dikeluarkan oleh pemerintah menunjukkan bahwa negara telah berupaya membentuk kerangka kerja hukum administratif untuk menangani *cybercrime*, antara lain:

3.1. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang mengatur kewajiban pengendali data dan pengelola sistem elektronik untuk menjaga keamanan data serta menyusun kebijakan internal sebagai bentuk tanggung jawab administratif.

3.2. Permenkominfo Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Privat**,** yang mewajibkan platform digital untuk mendaftar, memenuhi standar keamanan sistem, dan menyediakan fitur pelaporan konten illegal.

3.3. Perpres Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital**,** yang mengatur langkah-langkah mitigasi, audit sistem elektronik, serta sistem klasifikasi informasi strategis.

Namun, regulasi-regulasi tersebut belum menyentuh aspek akuntabilitas kelembagaan secara menyeluruh. Tidak ada regulasi yang mengatur secara eksplisit tentang Sanksi administratif bagi pejabat publik atau instansi yang gagal

mencegah atau menangani kejahatan digital, Standar pelaporan publik terhadap kinerja lembaga dalam penanganan cybercrime dan Keterlibatan publik dalam pengawasan digital atau transparansi informasi siber.

Padahal, menurut teori *New Public Management* (NPM)**,** akuntabilitas bukan hanya berorientasi pada hasil *(output),* tetapi juga pada proses administratif yang dijalankan secara efisien dan transparan.[31]

4. Solusi Normatif dan Rekomendasi Penataan Regulasi

Reformasi regulasi administratif yang efektif dalam menangani *cybercrime* harus dimulai dari *grand design* yang menyeluruh dan modular, yakni kerangka hukum administrasi digital yang jelas mengatur kewenangan lembaga, prosedur koordinasi, indikator kinerja, serta sanksi administratif yang tegas. Hal ini sangat penting mengingat belum adanya regulasi komprehensif, jika hanya bersifat sektoral, akan menimbulkan tumpang tindih kewenangan dan kebingungan institusional.[32]

Untuk memperkuat regulasi administratif terhadap akuntabilitas lembaga publik, diperlukan langkah-langkah strategis sebagai berikut:

4.1. Reformulasi regulasi administratif yang memperjelas indikator kinerja, mekanisme pelaporan, dan jenis sanksi administratif bagi lembaga yang lalai menjalankan tugas penanganan *cybercrime*;

4.2. Penyusunan SOP terpadu nasional antar lembaga publik yang menangani sistem elektronik dan keamanan data;

4.3. Penguatan lembaga pengawas independen, seperti Komisi Perlindungan Data Pribadi (yang direncanakan dalam UU PDP), agar dapat melakukan audit administratif secara berkala;

4.4. Transparansi kinerja lembaga publik secara digital, melalui portal resmi yang dapat diakses masyarakat untuk melihat respons terhadap kasus cybercrime;

---

[31] Christopher Hood, *The New Public Management in the 1980s: Variations on a Theme, OECD Journal on Budgeting*, 1983.

[32] Wahyu Beny Mukti Setiawan, Erifendi Churniawan & Femmy Silaswaty Faried, Upaya Regulasi Teknologi Informasi dalam Menghadapi Serangan Siber guna Menjaga Kedaulatan Negara Kesatuan Republik Indonesia, *Jurnal USM Law Review*, Vol. 3 No. 2 (2020), hlm. 275-295.

4.5. Pendidikan administrasi siber bagi aparatur negara agar memiliki kapasitas teknis dan pemahaman yuridis yang cukup dalam menangani masalah digital.

D. Kesimpulan

Harmonisasi penataan regulasi administratif merupakan elemen krusial dalam membangun sistem penanganan *cybercrime* yang efektif dan akuntabel di Indonesia. Saat ini, koordinasi antar lembaga seperti Komdigi, BSSN, Polri, dan Kejaksaan masih berjalan secara sektoral tanpa kerangka regulasi administratif yang terpadu. Ketiadaan pengaturan yang eksplisit mengenai mekanisme koordinasi antar lembaga menyebabkan tumpang tindih kewenangan, ketidakjelasan peran, serta lemahnya akuntabilitas institusional. Undang-Undang ITE yang menjadi payung hukum utama dalam penanganan kejahatan siber lebih banyak mengatur aspek substansi pidana dan belum menjangkau dimensi koordinasi administratif. Akibatnya, lembaga-lembaga yang seharusnya bersinergi justru bekerja sendiri-sendiri, sehingga menimbulkan inefisiensi birokrasi dan respons yang lamban terhadap insiden siber. Oleh karena itu, harmonisasi regulasi administratif bukan hanya penting, tetapi menjadi syarat mendasar bagi terciptanya sistem tata kelola keamanan siber yang profesional, terukur, dan dapat dipertanggungjawabkan.

E. Saran

1. Penyusunan Regulasi Khusus Terkait Koordinasi Lintas Lembaga**.** Pemerintah dan DPR perlu segera menyusun regulasi yang secara spesifik mengatur mekanisme koordinasi administratif antar lembaga dalam penanganan cybercrime. RUU Keamanan dan Ketahanan Siber atau revisi UU ITE dapat menjadi instrumen hukum strategis untuk mengakomodasi kebutuhan ini.
2. Penguatan Kelembagaan BSSN sebagai Koordinator Nasional. BSSN perlu diperkuat secara yuridis dan administratif sebagai lembaga koordinator utama keamanan siber nasional, dengan kewenangan yang jelas dan terukur, termasuk hak akses data dan otoritas integrasi sistem informasi antar instansi.
3. Penerapan Standar Akuntabilitas dan Evaluasi Kinerja. Diperlukan sistem evaluasi akuntabilitas yang berbasis indikator kinerja lintas sektor untuk menilai efektivitas penanganan kejahatan siber oleh lembaga publik. Ini

mencakup transparansi dalam pelaporan insiden, mekanisme audit koordinasi, dan pengawasan berbasis teknologi.

4. Pendidikan dan Peningkatan Kapasitas Aparatur. Harmonisasi regulasi juga harus diiringi dengan peningkatan kapasitas sumber daya manusia di masing-masing instansi, agar seluruh aparat mampu memahami dan menerapkan sistem koordinasi administratif secara optimal.

DAFTAR KEPUSTAKAAN

Artikel/Buku

Alamsyah, Kurniawan, Kelembagaan Penanganan Kejahatan Siber di Indonesia: Kajian terhadap Kewenangan BSSN, *Jurnal Hukum & Pembangunan*, Vol. 51 No. 1 (2021).

Arifiyadi, Teguh, *Cybercrime: Kejahatan Dunia Maya dan Penanggulangannya di Indonesia*, Jakarta: Rajagrafindo Persada, 2020,

Asshiddiqie, Jimly, *Penguatan Sistem Pemerintahan yang Demokratis*, Jakarta: Konstitusi Press, 2005.

Azhar, Kornelius Benuf dan Muhamad, Metodologi Penelitian Hukum sebagai Instrumen Mungurai Permasalahan Hukum Kontemorer, *Jurnal Gema Keadilan*, ISSN: 0852-011, Volume 7 Edisi I, Juni 2020.

Badan Siber dan Sandi Negara, *Laporan Tahunan Keamanan Siber Nasional 2023*, Jakarta: BSSN, 2024.

Butarbutar, Jonner Marulitua, Revolusi Digital dan Tantangan Kriminologis: Analisis terhadap Tren Kriminalitas dalam Era Digitalisasi, *Media Hukum Indonesia (MHI)*, e-ISSN: 3032-6591, May-2025. Vol. 2, No. 6.

Djafar, Wahyudi, Hukum Perlindungan Data Pribadi di Indonesia: Lanskap Urgensi dan Kebutuhan Pembaharuan (2019), *Jurnal Law UGM*, hal 1-14 dalam https://www.google.com/search?q=Hukum+Perlindungan+Data+Pribadi+di+Indonesia%3A+Lanskap%2C+Urgensi+dan+Kebutuhan+Pembaruan1+UGM&oq=Hukum+Perlindungan+Data+Pribadi+di+Indonesia%3A+Lanskap%2C+Urgensi+dan+Kebutuhan+Pembaruan1+UGM&aqs=chrome..69i57.2039j0j7&sourceid=chrome&ie=UTF-8, diakses pada 4 Agustus 2025.

Faried, Wahyu Beny Mukti Setiawan, Erifendi Churniawan & Femmy Silaswaty, Upaya Regulasi Teknologi Informasi dalam Menghadapi Serangan Siber guna Menjaga Kedaulatan Negara Kesatuan Republik Indonesia, *Jurnal USM Law Review*, Vol. 3 No. 2 (2020),

Firdos, Nabila Aulia Agustin dan Refania Meilani, "Studi Literatur : Ancaman Cybercrime di Indonesia dan Pentingnya Pemahaman akan Fenomena Kejahatan Digital," *Jurnal Mahasiswa Teknik Informatika 3*, no. 1 (2024): 126-31, https://doi.org/10.35473/jamastika.v3i1.2841

Hadjon, Philipus M., *Pengantar Hukum Administrasi Indonesia*, Yogyakarta: Gadjah Mada University Press, 2005.

Hood, Christopher, The New Public Management in the 1980s*: Variations on a Theme, OECD Journal on Budgeting*, 1983.

Mamudji, Soerjono Soekanto dan Sri, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*, Jakarta: Rajawali Pers, 2014,

Marzuki, Peter Mahmud, *Penelitian Hukum*, Jakarta: Kencana Prenada Media Group, 2010.

Nugroho, Oki Muraza dan Adi, *Cyber Law: Aspek Hukum Teknologi Informasi*, Yogyakarta: Graha Ilmu, 2011.

Jabar, Syabran, Akuntabilitas Dan Transparansi Dalam Perspektif Hukum Administrasi Negara, *Gudang Jurnal Multidisiplin Ilmu*, Vol. 12, No. 12 (2024),

Khairandy, Ridwan, *Hukum Administrasi Negara dan Regulasi Dunia Siber*, Yogyakarta: FH UII Press, 2020.

Priyambodo, Muhammad Anthony Aldriano dan Mas Agus, "Cyber Crime Dalam Sudut Pandang Hukum Pidana," *Jurnal Kewarganegaraan* 6, no. 1 (2022).

Rahardjo, Budi, *Keamanan Sistem Informasi berbasis Internet*, Bandung: Informatika, 2006,

Ridwan, HR., *Hukum Administrasi Negara*, Jakarta: Rajawali Pers, 2019, hlm. 45-47.

Sarjana, Kadek Rima Anggen Suari dan I Made, Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia, *Jurnal Analisis Hukum (JAH)*, Vol. 6, No. 1 April 2023.

Internet

https://www.suara.com/tekno/2023/08/23/010500/bssn-terkendala-jalankan-fungsi-karena-uu-ite, diakses 4 Mei 2025.

https://www.antaranews.com/berita/3692379/bssn-sebut-tugas-dan-fungsinya-belum-optimal-karena-terkendala-uu-ite, diakses 5 Mei 2025.

https://siplawfirm.id/tantangan-dan-prospek-hukum-administrasi-negara-di-era-digital/?lang=id, diakses 05 Agustus 2025.

Peraturan Perundang-Undangan

Peraturan Presiden Republik Indonesia Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara.

Peraturan Menteri Komunikasi dan Digital Nomor 1 Tahun 2025 tentang Organisasi dan Tata Kerja Kementerian Komunikasi dan Digital

,