E-ISSN xxxxxxxx

Jurnal Atribusi hukum

Vol. [1] Masalah [1], [2026]

Keamanan Siber Pemerintah Dan Aspek Hukum Administrasi Negara: Tanggung Jawab Administratif Dalam Perlindungan Sistem Informasi Publik Di Era Digital

Wanda Vebya Ayu Ananta, Puput Cahya Rani, Malykha Ajeng Lestari, Annisa Oktavini Putri,
anantawo8@gmail.com, puputcahyarani@gmail.com, malykhaajeng@gmail.com,
oktavianiannisa186@gmail.com,
Univesitas Teknokrat Indonesia, Universitas Muhammadiyah Kotabumi,

Abstrak

Artikel ini menganalisis tanggung jawab administratif institusi pemerintah dalam menjamin keamanan siber dalam layanan publik digital di Indonesia. Meningkatnya jumlah kebocoran data, serangan ransomware, dan akses tanpa izin ke sistem pemerintah menunjukkan bahwa keamanan siber tidak lagi hanya sekadar masalah teknis, tetapi juga menjadi perhatian hukum administrasi negara. Kegagalan dalam mengamankan sistem elektronik dapat mengindikasikan kelalaian atau ketidakpatuhan terhadap kewajiban hukum yang harus dipenuhi oleh pejabat publik.

Tujuan dari studi ini adalah untuk mengkaji bagaimana hukum administrasi mengatur tugas instansi pemerintah dalam menjaga keamanan sistem digital dan melindungi data pribadi warga negara, khususnya dalam kerangka Sistem Pemerintahan Berbasis Elektronik (SPBE), Undang-Undang Perlindungan Data Pribadi (UU PDP), dan Undang-Undang ITE. Artikel ini juga menyoroti peran teknik informatika dalam mendukung kepatuhan hukum melalui penguatan keamanan siber, penetration testing, manajemen risiko, dan prosedur respons insiden.

Dengan menggunakan metode yuridis normatif melalui pendekatan perundang-undangan dan konseptual, penelitian ini mengevaluasi sejauh mana tanggung jawab negara dalam mencegah insiden siber serta konsekuensi administratif yang timbul ketika kegagalan terjadi. Temuan menunjukkan bahwa kelemahan keamanan siber di institusi pemerintah dapat dikategorikan sebagai maladministrasi apabila disebabkan oleh kelalaian atau pengelolaan sistem yang tidak memadai. Artikel ini berkontribusi dalam menjembatani perspektif hukum dan teknis untuk membangun tata kelola digital yang akuntabel dan aman.

***Kata kunci*:** Hukum Administrasi Negara, Keamanan Siber, Sistem Pemerintahan, Maladministrasi, Perlindungan Data Publik.

Pendahuluan

Perkembangan teknologi informasi telah mendorong transformasi besar dalam tata kelola pemerintahan, termasuk di Indonesia melalui penerapan Sistem Pemerintahan Berbasis Elektronik (SPBE). Transformasi digital ini bertujuan meningkatkan efektivitas pelayanan publik, efisiensi birokrasi, serta transparansi administrasi pemerintahan. Namun, dalam beberapa tahun terakhir, Indonesia menghadapi lonjakan insiden serangan siber yang menyasar lembaga negara, mulai dari peretasan data, pencurian identitas, hingga kebocoran informasi sensitif. Fenomena ini menegaskan bahwa keamanan siber bukan hanya persoalan teknis, tetapi juga persoalan hukum administrasi karena menyangkut kewajiban pemerintah untuk melindungi data dan menjaga keandalan sistem yang digunakan dalam pelayanan publik.

Dalam konteks Hukum Administrasi Negara, pemerintah memiliki tanggung jawab untuk menyelenggarakan pemerintahan yang tertib, aman, dan

akuntabel. Kewajiban tersebut termasuk memastikan bahwa sistem elektronik yang digunakan telah memenuhi standar keamanan, memiliki manajemen risiko yang memadai, serta dikelola oleh aparatur yang kompeten. Ketika terjadi kebocoran data atau kegagalan sistem akibat kelalaian, maka hal tersebut dapat dikategorikan sebagai bentuk maladministrasi karena merugikan masyarakat sebagai pengguna layanan publik. Oleh karena itu, analisis mengenai keamanan siber perlu ditempatkan sebagai bagian integral dari tanggung jawab administratif negara.

Keamanan siber dalam pemerintahan mencakup pengamanan terhadap infrastruktur digital, tata kelola data, mekanisme pertahanan terhadap serangan, serta prosedur *respons* ketika insiden terjadi. Istilah-istilah seperti cybersecurity, data breach, incident response, hingga risk assessment menjadi aspek penting dalam memahami bagaimana tata kelola pemerintahan digital seharusnya dijalankan. Di sisi lain, konsep-konsep utama dalam Hukum Administrasi Negara seperti kewajiban penyelenggaraan pemerintahan yang baik, tanggung jawab jabatan, diskresi, hingga prinsip akuntabilitas menjadi kunci untuk menilai apakah sebuah insiden siber merupakan risiko alami atau justru akibat kelalaian administratif.

Kebaruan penelitian ini terletak pada integrasi analisis antara aspek teknis keamanan siber dan aspek normatif Hukum Administrasi Negara. Sejauh ini, sebagian besar penelitian hanya menyoroti keamanan siber dari sudut pandang teknologi atau regulasi umum tanpa menghubungkannya secara langsung dengan tanggung jawab administratif pejabat pemerintah. Beberapa jurnal sebelumnya membahas keamanan siber sebagai bagian dari perlindungan data pribadi, sementara yang lain membahas maladministrasi dalam pelayanan publik, tetapi tidak mengaitkan keduanya secara eksplisit. Artikel ini menawarkan perspektif yang menggabungkan kedua disiplin tersebut untuk menunjukkan bahwa keamanan siber merupakan kewajiban hukum administratif, bukan semata kebutuhan teknis.

Selain itu, penelitian ini memberikan kontribusi dengan menonjolkan peran keilmuan Teknik Informatika dalam mendukung pemenuhan kewajiban administratif pemerintah. Penguatan keamanan sistem, uji penetrasi, manajemen risiko, hingga penyusunan *disaster recovery plan* merupakan kompetensi teknis yang sangat menentukan apakah pemerintah dapat mematuhi standar hukum dalam penyelenggaraan SPBE. Dengan demikian, hubungan antara Hukum Administrasi Negara dan Teknik Informatika menjadi semakin relevan dalam era transformasi digital.

Artikel ini penting secara nasional maupun internasional karena serangan siber terhadap lembaga pemerintahan merupakan isu global yang berdampak pada stabilitas negara, perlindungan warga, dan integritas layanan publik. Dengan mengkaji keamanan siber melalui perspektif hukum administrasi, artikel ini memperluas pemahaman akademik tentang bagaimana negara harus bertanggung

jawab dalam era digital dan bagaimana teknologi dapat menjadi fondasi penting dalam mewujudkan pemerintahan yang aman, efisien, dan akuntabel.

Masalah

Pertama, bagaimana tanggung jawab Hukum Administrasi Negara diterapkan dalam pengamanan sistem elektronik pemerintahan, khususnya ketika terjadi insiden siber seperti kebocoran data, peretasan, atau kegagalan sistem yang mengganggu pelayanan publik?

Kedua, bagaimana peran keilmuan Teknik Informatika, termasuk manajemen risiko, pengujian keamanan, dan tata kelola sistem, dapat mendukung pemenuhan kewajiban administratif pemerintah dalam menjaga keamanan siber pada penyelenggaraan layanan berbasis elektronik?

Metode

Penelitian ini bertujuan untuk menganalisis keterkaitan antara kewajiban Hukum Administrasi Negara dan aspek teknis keamanan siber dalam penyelenggaraan sistem elektronik pemerintahan. Untuk mencapai tujuan tersebut, penulis menggunakan pendekatan yuridis-normatif dengan fokus pada analisis peraturan perundang-undangan yang mengatur penyelenggaraan SPBE, keamanan informasi, perlindungan data, serta tanggung jawab administrasi pejabat pemerintah. Pendekatan ini digunakan untuk menilai bagaimana norma hukum membentuk kewajiban pemerintah dalam menjaga keamanan sistem digital yang digunakan dalam pelayanan publik.

Selain itu, penelitian ini menerapkan pendekatan konseptual untuk mengkaji istilah-istilah kunci seperti *cybersecurity*, data breach, incident response, risk assessment, dan konsep administratif seperti tanggung jawab jabatan, maladministrasi, asas-asas umum pemerintahan yang baik (AUPB), dan kewajiban pelayanan publik. Melalui pendekatan ini, penelitian dapat menghubungkan aspek teknis yang berkembang dalam disiplin Teknik Informatika dengan kewajiban administratif negara.

Data yang digunakan dalam penelitian ini berupa bahan hukum primer, seperti undang-undang, peraturan pemerintah, dan peraturan menteri; bahan hukum sekunder, seperti artikel jurnal, prosiding, dan laporan penelitian; serta bahan non-hukum teknis terkait standar keamanan siber dan manajemen risiko teknologi informasi. Data kemudian dianalisis secara kualitatif untuk menjelaskan pola hubungan antara kewajiban hukum administratif dan kebutuhan keamanan teknis dalam pengelolaan sistem pemerintahan berbasis elektronik.

Penelitian ini tidak menggunakan observasi lapangan maupun data empiris, melainkan menganalisis ketentuan hukum dan standar teknis yang relevan untuk menghasilkan temuan yang bersifat deskriptif-analitis.

Diskusi

Kerangka Hukum Administrasi Negara dalam Keamanan Siber Pemerintahan

Keamanan siber dalam penyelenggaraan pemerintahan bukan hanya isu teknis, tetapi juga merupakan kewajiban hukum yang lahir dari prinsip-prinsip Hukum Administrasi Negara (HAN). Dalam konteks modern, aktivitas pemerintah semakin bergantung pada sistem elektronik, basis data digital, dan jaringan internal maupun eksternal. Situasi ini menempatkan pemerintah pada posisi strategis sekaligus rentan: ketika sistem bekerja dengan baik, pelayanan publik menjadi efisien; tetapi ketika terjadi serangan siber, kebocoran data, atau kerusakan sistem, hak-hak masyarakat, kepastian hukum, dan legitimasi negara dapat terganggu. Oleh karena itu, keamanan siber bukan sekadar persoalan teknis IT, melainkan juga bagian dari tanggung jawab hukum administratif pemerintah.

Kerangka hukum utama yang menaungi keamanan siber dalam administrasi pemerintahan berakar pada prinsip *good governance*, khususnya kepastian hukum, akuntabilitas, ketertiban penyelenggaraan pemerintahan, dan tanggung jawab pejabat administrasi. Prinsip-prinsip ini mengharuskan pemerintah mengelola sistem elektronik secara profesional, aman, dan dapat dipertanggungjawabkan. Dalam konteks Indonesia, berbagai regulasi – seperti UU Administrasi Pemerintahan, UU ITE, PP tentang Penyelenggaraan Sistem dan Transaksi Elektronik, hingga Perpres terkait SPBE dan Keamanan Siber Nasional – menyatakan bahwa pemerintah wajib menyediakan sistem yang andal, terjaga integritasnya, dan mampu melindungi data pribadi maupun data strategis negara. Artinya, setiap instansi pemerintah tidak hanya dituntut mampu melayani, tetapi juga wajib mencegah kegagalan layanan akibat serangan atau kelalaian dalam mengelola sistem.

Salah satu titik penting dalam kerangka HAN adalah konsep tanggung jawab jabatan (*ambtelijke verantwoordelijkheid*). Pejabat administrasi negara dapat dimintai pertanggungjawaban apabila terjadi kerugian akibat tindakan atau kelalaian dalam pengelolaan sistem elektronik. Misalnya, jika terjadi kebocoran data penduduk dari server pemerintah, maka kelalaian dalam menerapkan standar keamanan—seperti tidak menerapkan enkripsi, tidak melakukan pembaruan sistem, atau mengabaikan hasil audit risiko—dapat menjadi dasar pertanggungjawaban administratif. Pada tataran tertentu, hal ini dapat berimplikasi pada sanksi administrasi, penilaian kinerja, ataupun tindakan korektif institusional. Dengan demikian, keamanan siber bukan hanya tugas teknis operator IT, melainkan kewajiban hukum pejabat pemerintah yang memiliki kewenangan pengelolaan.

Kerangka HAN juga memberikan landasan untuk memastikan bahwa kebijakan keamanan siber harus direncanakan secara sistematis melalui prosedur administratif yang baku. Setiap keputusan terkait teknologi misalnya pemilihan perangkat, penetapan standar keamanan, pengelolaan pusat data, atau kerja sama dengan pihak ketiga harus mengikuti prinsip legalitas dan asas kehati-hatian. Pemerintah tidak boleh mengambil keputusan teknologi secara sembarangan, sebab setiap sistem yang tidak memenuhi standar keamanan berpotensi menimbulkan kerugian bagi masyarakat. Oleh karena itu, tata kelola keamanan siber dalam administrasi pemerintahan harus selaras dengan asas kecermatan (zorgvuldigheid), yang mengharuskan seluruh proses pengambilan keputusan berbasis pada analisis risiko dan informasi teknis yang memadai.

Selanjutnya, dalam kerangka HAN, keamanan siber juga berkaitan dengan kualitas pelayanan publik. Pemerintah wajib menjamin keberlanjutan layanan meskipun terjadi gangguan. Kewajiban ini dikenal sebagai *continuity of public service*. Jika sistem layanan administrasi seperti pencatatan kependudukan, perpajakan, atau perizinan digital lumpuh akibat serangan, maka pemerintah dianggap gagal memenuhi kewajiban pelayanan. Oleh karena itu, regulasi HAN menjadi dasar bagi pemerintah untuk membangun *Disaster Recovery Plan (*DRP), pusat data cadangan (backup), mekanisme pemulihan sistem, serta prosedur mitigasi insiden siber. Kebijakan ini merupakan perwujudan asas kemanfaatan dan kepentingan umum, karena menjaga agar pelayanan publik tetap berjalan tanpa gangguan yang merugikan masyarakat.

Kerangka hukum juga mengatur mengenai transparansi dan pelaporan insiden. Pemerintah tidak boleh menutup-nutupi serangan siber yang berpotensi merugikan masyarakat. Prinsip keterbukaan informasi yang benar bukan sekadar publikasi mengharuskan pemerintah memberikan informasi yang cukup dan proporsional kepada publik mengenai insiden yang terjadi, langkah penanganan, dan upaya pemulihan. Hal ini merupakan bagian dari asas akuntabilitas, di mana setiap tindakan dan kebijakan pemerintah harus dapat dipertanggungjawabkan secara terbuka.

Dengan demikian, kerangka Hukum Administrasi Negara menyediakan fondasi normatif sekaligus instrumen pengawasan terhadap keamanan siber pemerintahan. Pengelolaan sistem elektronik bukan hanya persoalan teknis TI, tetapi merupakan bagian integral dari kewajiban hukum pemerintahan modern. Kerangka ini memastikan bahwa keamanan siber tidak dipandang sebagai proyek teknologi, melainkan sebagai kewajiban hukum negara dalam memberikan pelayanan publik yang aman, andal, dan bertanggung jawab.

Ancaman Siber dan Risiko Administratif bagi Pemerintah

Ancaman siber terhadap instansi pemerintah terus meningkat seiring percepatan transformasi digital birokrasi. Sistem pemerintahan yang sebelumnya berbasis manual kini bergantung pada infrastruktur elektronik untuk pelayanan publik, pengelolaan data, hingga koordinasi antarinstansi. Perubahan besar ini menjadikan pemerintah sebagai target utama kejahatan siber karena data yang mereka kelola bersifat strategis, masif, dan bernilai tinggi. Di sisi lain, meningkatnya digitalisasi tidak selalu diikuti dengan kesiapan hukum administrasi dan tata kelola keamanan yang memadai. Akibatnya, ancaman siber tidak hanya menimbulkan kerugian teknis, tetapi juga menimbulkan risiko administratif yang melekat pada tanggung jawab pejabat dan instansi pemerintah.

Jenis ancaman siber yang paling sering menyerang institusi pemerintahan mencakup *ransomware, phishing, social engineering, DDoS, deface, spyware, malware,* hingga kebocoran data melalui eksploitasi celah keamanan. Serangan tersebut dapat menyebabkan gangguan layanan publik, kerusakan data, manipulasi informasi, atau bahkan penghentian total sistem administratif. Dampaknya bagi instansi pemerintah jauh lebih serius dibandingkan sektor privat, karena: (1) pemerintah mengelola data demografis dan identitas warga, (2) pemerintah menyediakan layanan vital seperti administrasi kependudukan, kesehatan, pendidikan, dan keuangan, dan (3) serangan yang berhasil dapat mengancam stabilitas keamanan nasional.

Setiap bentuk ancaman ini memiliki korelasi langsung dengan risiko administratif. Misalnya, kebocoran data kependudukan akibat kelalaian dalam pengamanan server dapat dikualifikasikan sebagai pelanggaran terhadap asas-asas Hukum Administrasi Negara, khususnya asas kepatutan, kehati-hatian (*zorgvuldigheid*), dan akuntabilitas. Pejabat atau instansi yang bertanggung jawab atas sistem wajib memastikan adanya standar keamanan minimum, seperti enkripsi, pembaruan *patch*, mekanisme autentikasi berlapis, backup rutin, serta pengawasan lalu lintas data. Ketika langkah-langkah tersebut tidak dijalankan, maka konsekuensi administrasinya dapat berupa teguran, sanksi disiplin, audit internal, hingga pemberhentian.

Selain itu, ancaman siber juga membuka peluang terjadinya penyalahgunaan wewenang apabila pejabat tidak kompeten atau sengaja membuat keputusan teknologi yang tidak sesuai standar demi kepentingan tertentu. Misalnya, memilih vendor keamanan tanpa mekanisme pengadaan yang benar atau mengabaikan rekomendasi teknis dari tim keamanan. Dalam perspektif Hukum Administrasi Negara, tindakan semacam ini dapat dikategorikan sebagai detournement de pouvoir (penyimpangan tujuan), yang menimbulkan pertanggungjawaban hukum dan administratif.

Dari sisi prosedural, ancaman siber dapat mengakibatkan instansi dianggap gagal memenuhi kewajiban pelayanan publik. Contohnya, serangan ransomware

yang membuat layanan kependudukan berhenti selama beberapa hari secara hukum dapat dianggap sebagai bentuk maladministrasi, karena pemerintah berkewajiban memastikan layanan tetap tersedia dan aman. Ombudsman, inspektorat, maupun lembaga pengawas lainnya dapat menilai bahwa kegagalan tersebut terjadi akibat kelalaian manajerial atau minimnya mitigasi risiko.

Kerugian negara juga merupakan bagian dari risiko administratif yang sering terabaikan. Ketika serangan siber menyebabkan kerusakan sistem, pemerintah harus mengeluarkan anggaran besar untuk pemulihan, penggantian server, atau membayar konsultan forensik digital. Jika ditemukan bahwa kerugian tersebut timbul karena kelalaian pejabat dalam menjaga keamanan sistem, maka pejabat dapat diminta tanggung jawab ganti rugi sesuai dengan prinsip pengelolaan keuangan negara.

Dengan demikian, ancaman siber bukan sekadar isu teknis yang dibebankan kepada tim IT, tetapi merupakan isu hukum administrasi yang menuntut akuntabilitas, kepatuhan prosedural, dan tata kelola yang transparan. Pemerintah wajib memahami bahwa setiap serangan yang berhasil bukan hanya melanggar keamanan digital, tetapi berpotensi melanggar kewajiban hukum sebagai penyelenggara administrasi negara. Oleh karena itu, penguatan keamanan siber harus dipandang sebagai bagian integral dari reformasi birokrasi, bukan sekadar urusan teknis digitalisasi.

Konsekuensi Hukum Administratif atas Kegagalan Keamanan Siber pada Instansi Pemerintah

Kegagalan pemerintah dalam menjaga keamanan siber tidak hanya berdampak pada aspek teknis, tetapi juga menimbulkan konsekuensi hukum administratif yang serius. Dalam perspektif Hukum Administrasi Negara (HAN), setiap tindakan atau keputusan pejabat publik yang menghasilkan kerugian, gangguan layanan, atau pelanggaran hak warga dapat menimbulkan pertanggungjawaban administratif. Hal ini sejalan dengan prinsip bahwa pemerintah wajib bertindak hati-hati, akuntabel, dan profesional dalam penyelenggaraan pemerintahan yang berbasis elektronik. Dengan demikian, insiden siber seperti kebocoran data, peretasan, hingga gangguan layanan merupakan indikator adanya potensi pelanggaran kewajiban hukum oleh pejabat administrasi.

Konsekuensi pertama yang dapat muncul adalah sanksi administratif terhadap pejabat atau instansi terkait. Sanksi ini dapat berupa teguran tertulis, peringatan, pembinaan khusus, penundaan promosi, hingga pencopotan jabatan apabila terbukti terjadi kelalaian serius. Kelalaian tersebut dapat berupa tidak diterapkannya standar keamanan minimal, seperti tidak melakukan enkripsi data, kurangnya pembaruan sistem, tidak adanya backup rutin, atau tidak menjalankan

audit keamanan. Dalam konteks ini, pejabat dianggap melanggar asas kecermatan dan asas kehati-hatian, yang menjadi bagian dari Asas-Asas Umum Pemerintahan yang Baik (AUPB). Kegagalan menyediakan sistem yang aman juga dapat dipandang sebagai pelanggaran asas profesionalitas dan asas akuntabilitas.

Konsekuensi kedua adalah penilaian maladministrasi oleh lembaga pengawas eksternal seperti Ombudsman RI. Gangguan layanan publik akibat serangan siber dapat dikategorikan sebagai penundaan pelayanan, penyalahgunaan wewenang, atau tidak memberikan pelayanan sebagaimana mestinya. Jika layanan administrasi kependudukan, perizinan, atau kesehatan terganggu dalam waktu lama, Ombudsman dapat menyatakan adanya maladministrasi karena pemerintah tidak mampu menjaga kelangsungan layanan. Meski serangan siber mungkin berasal dari pihak luar, tetapi ketidakmampuan pemerintah dalam menyiapkan mitigasi yang memadai menjadi dasar penilaian disiplin administrasi.

Konsekuensi ketiga berkaitan dengan tanggung jawab keuangan negara. Ketika sistem diretas dan pemerintah harus mengeluarkan biaya pemulihan, pembelian perangkat keamanan tambahan, atau jasa konsultan, angka yang dikeluarkan termasuk kerugian negara apabila serangan tersebut terjadi akibat kelalaian pejabat. Dalam kondisi tertentu, pejabat dapat diminta mengembalikan kerugian melalui mekanisme tuntutan ganti rugi. Hal ini menegaskan bahwa keamanan siber berkaitan erat dengan prinsip efisiensi dan efektivitas pengelolaan anggaran negara.

Konsekuensi keempat adalah pertanggungjawaban hukum personal apabila terdapat unsur penyalahgunaan wewenang. Misalnya, memilih vendor keamanan secara tidak transparan, mengabaikan hasil audit keamanan, atau memanipulasi laporan risiko. Dalam kerangka HAN, tindakan tersebut dapat dikualifikasikan sebagai detournement de pouvoir (penyimpangan tujuan), yang membuka kemungkinan sanksi administratif berat dan pemeriksaan etik. Konsekuensi ini menjadi penting karena banyak kegagalan keamanan bukan hanya akibat lemahnya sistem, tetapi juga lemahnya manajemen risiko dan intervensi kebijakan yang tidak profesional.

Selain itu, terdapat pula konsekuensi terkait pengawasan berlapis dari lembaga seperti BSSN, Inspektorat Jenderal, BPKP, hingga Komisi Informasi. Kegagalan keamanan siber dapat memicu audit menyeluruh terhadap tata kelola SPBE dan keamanan informasi. Jika ditemukan ketidakpatuhan terhadap PP 95/2018 atau kebijakan BSSN terkait keamanan siber nasional, pemerintah pusat dapat memberikan rekomendasi wajib perbaikan atau bahkan melakukan intervensi langsung pada sistem tertentu.

Dengan demikian, konsekuensi hukum administratif akibat kegagalan keamanan siber sangat luas dan komprehensif. Pemerintah tidak hanya menanggung dampak teknis, tetapi juga harus bertanggung jawab secara normatif,

prosedural, finansial, dan etik. Hal ini menegaskan bahwa keamanan siber merupakan bagian integral dari kewajiban administrasi negara yang harus dipenuhi demi menjamin hak-hak masyarakat, keandalan birokrasi digital, serta kepercayaan publik terhadap negara.

Tantangan dan Peluang Kolaborasi antara Hukum Administrasi Negara dan Teknik Informatika dalam Penguatan Keamanan Siber Pemerintah

Kolaborasi antara Hukum Administrasi Negara (HAN) dan Teknik Informatika semakin menjadi kebutuhan mendesak seiring meningkatnya frekuensi serangan siber yang menargetkan institusi pemerintah di Indonesia. Tantangan utama yang muncul bukan hanya terkait aspek teknis, tetapi juga mencakup struktur regulasi, tata kelola kelembagaan, serta kesenjangan kompetensi antara aktor hukum dan teknologi. Namun, di balik tantangan tersebut, terdapat peluang besar untuk membangun birokrasi digital yang lebih aman, akuntabel, dan responsif terhadap perkembangan teknologi. Pembahasan ini menguraikan tantangan substantif yang dihadapi pemerintah serta peluang strategis yang dapat dimaksimalkan melalui kolaborasi antardisiplin.

Tantangan pertama terletak pada disharmoni regulasi, di mana berbagai aturan yang mengatur keamanan sistem, perlindungan data, dan tata kelola digital masih tersebar dalam banyak peraturan yang belum sepenuhnya selaras. Misalnya, aturan keamanan informasi dalam PP SPBE, Perpres Satu Data Indonesia, PP Perlindungan Data Pribadi, serta beberapa regulasi sektoral seringkali memiliki standar teknis yang berbeda. Ketidaksinkronan ini membuat instansi pemerintah kesulitan menentukan prioritas kepatuhan dan standar keamanan yang harus diterapkan. Bagi Teknik Informatika, ketidakselarasan regulasi ini menyebabkan ambiguitas dalam penerjemahan konsep hukum ke dalam prosedur teknis. Bagi HAN, kondisi ini menyulitkan penentuan apakah suatu tindakan pejabat dapat dinilai lalai, karena ketiadaan standar baku yang jelas.

Tantangan selanjutnya adalah keterbatasan sumber daya manusia, baik pada sisi hukum maupun teknologi. Banyak pejabat administrasi belum memahami karakter ancaman digital modern seperti *ransomware, SQL injection, exploit zero-day, atau advanced persistent threat (APT)*. Di sisi lain, para profesional TI tidak selalu memahami prinsip-prinsip dasar pertanggungjawaban administratif, kewajiban kehati-hatian, asas-asas umum pemerintahan yang baik (AUPB), serta batas kewenangan pejabat publik. Kesenjangan keahlian ini menghambat koordinasi dalam penanganan insiden, sehingga respons pemerintah sering terlambat atau tidak sistematis. Ketika serangan siber terjadi, kelambatan pengambilan keputusan dapat berpotensi menimbulkan kerugian publik dalam skala luas, dan pada saat yang sama memicu pertanggungjawaban hukum bagi pejabat.

Tantangan ketiga adalah keterbatasan infrastruktur dan sistem keamanan, terutama di instansi pemerintah daerah. Banyak aplikasi pelayanan publik dibangun dengan standar keamanan rendah, tidak diperbarui (outdated), dan tidak menggunakan protokol enkripsi yang memadai. Infrastruktur yang rapuh ini menyebabkan pemerintah mudah diserang, tetapi pada saat yang sama sulit untuk memenuhi standar akuntabilitas administratif. Dalam konteks HAN, sistem yang lemah dapat menjadi bukti adanya kelalaian pemerintah jika terbukti tidak memenuhi standar minimum pengelolaan keamanan data.

Tantangan keempat berkaitan dengan mekanisme koordinasi antarinstansi. Penanganan kejahatan siber sering membutuhkan kolaborasi antara BSSN, Kominfo, Polri, dan instansi terkait. Namun, koordinasi sering terganggu oleh pembagian kewenangan yang tidak jelas dan prosedur birokrasi yang lambat. Dari sudut pandang HAN, koordinasi yang buruk dapat memperpanjang rantai pertanggungjawaban dan memperbesar risiko maladministrasi karena tindakan yang tidak terkoordinasi dapat dinilai sebagai bentuk ketidakcermatan.

Di balik berbagai tantangan tersebut, terdapat peluang besar bagi kolaborasi HAN dan Teknik Informatika. Peluang pertama adalah penguatan regulasi berbasis standar teknis yang terukur. Pemerintah dapat mengembangkan standar keamanan minimum yang berlaku nasional, yang menggabungkan prinsip AUPB dengan *best practices* keamanan siber seperti ISO 27001, *NIST Cybersecurity Framework, atau OWASP*. Keberadaan standar baku ini tidak hanya membantu ahli TI merancang sistem yang aman, tetapi juga memberikan acuan hukum yang jelas untuk menilai kelalaian pejabat.

Peluang berikutnya adalah pengembangan kapasitas SDM lintas disiplin. Program pelatihan yang mempertemukan ahli hukum dan TI dapat membantu menciptakan pemahaman komprehensif antara kedua bidang. Misalnya, pelatihan mitigasi insiden siber yang melibatkan penjelasan tentang batas kewenangan administratif, prosedur dokumentasi bukti, dan mekanisme pertanggungjawaban dalam HAN. Kolaborasi ini dapat menghasilkan kebijakan yang lebih tepat karena setiap keputusan administrasi akan mempertimbangkan aspek teknis dan hukum secara simultan.

Peluang ketiga adalah pemanfaatan teknologi untuk meningkatkan akuntabilitas administratif. Sistem logging, audit trail, pemantauan otomatis, artificial intelligence-based anomaly detection, hingga dashboard risiko real-time dapat memperkuat proses pengawasan internal. Semakin lengkap rekam jejak digital, semakin mudah bagi instansi untuk membuktikan bahwa mereka telah melaksanakan kewajiban kehati-hatian. Teknologi ini membuat prinsip-prinsip HAN seperti akuntabilitas dan transparansi dapat diterapkan lebih efektif.

Selain itu, terdapat peluang pengembangan mekanisme respons insiden terpadu (*integrated incident response center*). Dengan struktur komando yang jelas dan SOP yang disepakati lintas instansi, respon pemerintah terhadap serangan

siber akan lebih cepat, lebih tepat, dan lebih mudah dipertanggungjawabkan secara hukum.

Dengan demikian, tantangan dan peluang dalam kolaborasi antara Hukum Administrasi Negara dan Teknik Informatika menunjukkan bahwa kedua bidang ini tidak dapat dipisahkan dalam menghadapi ancaman siber modern. Melalui penguatan regulasi, peningkatan kapasitas SDM, pemanfaatan teknologi, dan koordinasi kelembagaan yang lebih baik, pemerintah dapat membangun ekosistem keamanan siber yang lebih kuat dan secara bersamaan memenuhi prinsip-prinsip dasar pertanggungjawaban administrasi.

Integrasi Keahlian Hukum dan Informatika

Integrasi antara keahlian Hukum Administrasi Negara dan Teknik Informatika merupakan kebutuhan strategis dalam era digital, khususnya ketika pemerintah semakin bergantung pada sistem elektronik untuk memberikan layanan publik. Hukum menetapkan berbagai kewajiban, batasan, prosedur, serta standar akuntabilitas yang harus dipatuhi oleh setiap instansi pemerintah. Namun, pemenuhan seluruh kewajiban tersebut tidak dapat dilakukan hanya dengan pendekatan normatif; dibutuhkan dukungan teknis dari disiplin ilmu Informatika agar sistem yang dibangun benar-benar aman, andal, dan sesuai standar tata kelola yang baik.

Dalam konteks keamanan siber pemerintahan, hukum mendefinisikan tanggung jawab pejabat, kewajiban menjaga kerahasiaan dan integritas data, hingga konsekuensi administratif bila terjadi kelalaian. Di sisi lain, Teknik Informatika menyediakan perangkat ilmu seperti *risk assessment, penetration testing, threat modeling, enkripsi data, audit log, dan disaster recovery* yang memungkinkan instansi pemerintah menerapkan kewajiban tersebut secara konkret. Dengan demikian, hukum berfungsi sebagai *normative guideline,* sementara TI berfungsi sebagai operational enforcer yang memastikan standar keamanan benar-benar berjalan dalam praktik.

Sinergi ini juga penting dalam proses pembuatan kebijakan. Regulasi yang terlalu abstrak atau tidak memahami realitas teknis sering kali menciptakan celah keamanan, standar yang tidak realistis, atau prosedur yang tidak dapat diimplementasikan. Oleh karena itu, kolaborasi antara ahli hukum dan ahli TI diperlukan sejak tahap perumusan kebijakan, perancangan sistem, pengawasan, hingga evaluasi pasca-insiden. Pemerintah membutuhkan mekanisme *cross-disciplinary teamwork* untuk memastikan bahwa setiap aturan dapat diwujudkan secara teknis, dan setiap desain teknis memenuhi standar hukum.

Dengan integrasi tersebut, pemerintah tidak hanya mampu mencegah insiden siber, tetapi juga meminimalkan potensi pelanggaran administratif,

meningkatkan kepatuhan birokrasi, serta memperkuat kepercayaan publik terhadap layanan digital negara. Sinergi hukum dan informatika adalah fondasi utama bagi tata kelola SPBE yang aman, modern, dan akuntabel.

Kesimpulan

Kajian mengenai keamanan siber pemerintah dari perspektif Hukum Administrasi Negara dan Teknik Informatika menunjukkan bahwa perlindungan sistem elektronik negara bukan hanya persoalan teknis, tetapi juga persoalan hukum dan tata kelola. Pemerintah, sebagai penyelenggara layanan publik berbasis digital, memikul kewajiban administratif untuk menjamin keamanan, keandalan, dan kontinuitas sistem sesuai asas-asas umum pemerintahan yang baik (AUPB). Ketika terjadi insiden siber seperti kebocoran data, peretasan, atau gangguan layanan tanggung jawab hukum dapat muncul dalam bentuk pelanggaran prosedur, kelalaian, maupun tidak terpenuhinya kewajiban pelayanan.

Sementara itu, kontribusi disiplin Teknik Informatika terbukti esensial dalam memastikan bahwa kewajiban hukum tersebut dapat diterapkan secara nyata. Melalui *risk assessment*, penetration testing, incident response, enkripsi, dan tata kelola keamanan informasi, keilmuan TI memungkinkan pemerintah membangun sistem yang aman dan tahan terhadap ancaman. Integrasi kedua disiplin ilmu ini tidak hanya memperkecil risiko insiden, tetapi juga mencegah potensi pelanggaran administratif yang dapat merugikan negara dan masyarakat.

Dari analisis keseluruhan, dapat disimpulkan bahwa peningkatan keamanan siber pemerintah harus dilakukan melalui pendekatan kolaboratif yang menggabungkan norma hukum, mekanisme teknis, serta komitmen kelembagaan. Pemerintah perlu memperkuat kebijakan keamanan informasi, meningkatkan kompetensi sumber daya manusia, serta memastikan bahwa seluruh sistem elektronik mengikuti standar keamanan yang dapat dipertanggungjawabkan secara hukum maupun teknis. Dengan demikian, pembangunan tata kelola SPBE yang aman, akuntabel, dan berkelanjutan dapat tercapai, sekaligus meningkatkan kepercayaan publik terhadap layanan digital negara.

Referensi

Amsori, Y. (2018). Maladministrasi dan upaya hukum pencegahannya dalam pelayanan publik. *Jurnal Hukum dan Peradilan*, *7*(2), 339–354. https://doi.org/10.25216/JHP.7.2.339-354

Arsil, F. (2019). Tanggung jawab hukum administrasi negara dalam menghadapi ancaman siber. *Jurnal Hukum Ius Quia Iustum*, *26*(4), 677–695. https://doi.org/10.20473/iqij.v26i4.17062

Bachmid, F. (2023). Urgensi perlindungan data pribadi dalam kerangka hukum administrasi negara di era digital. *Jurnal Penelitian Hukum De Jure, 23*(1), 57–73. https://doi.org/10.30641/dejure.2023.V23.57-73

Bhakti, R. S. (2020). Akuntabilitas pemerintah dalam pengelolaan Sistem Pemerintahan Berbasis Elektronik (SPBE). *Jurnal Ilmu Administrasi Publik, 7*(2).

Darmawan, R. (2021). Peran Badan Siber dan Sandi Negara (BSSN) dalam implementasi keamanan siber nasional. *Jurnal Pertahanan dan Bela Negara, 11*(3).

Dewi, S. T., & Arjuni, A. (2022). Tinjauan hukum administrasi terhadap kewajiban pejabat publik dalam pengamanan data elektronik pemerintah. *Jurnal Hukum dan Pembangunan, 52*(3), 677–695. https://doi.org/10.21143/jhp.vol52.no3.3855

Fernando, M. (2023). Pertanggungjawaban administratif atas kegagalan sistem informasi publik: Analisis perspektif maladministration. *Jurnal Ilmu Hukum, 14*(2).

Gultom, E. (2021). Prinsip kehati-hatian dalam kebijakan publik berbasis teknologi informasi: Perspektif hukum administrasi. *Jurnal Hukum Administrasi Negara (JHAN), 1*(2).

Hidayat, S. (2020). Sinkronisasi regulasi SPBE dan UU ITE: Mewujudkan tata kelola pemerintahan digital yang aman. *Jurnal Konstitusi, 17*(3), 573–596. https://doi.org/10.31078/jk1732

Ibrahim, J. (2022). Penerapan asas umum pemerintahan yang baik (AUPB) dalam kebijakan keamanan siber pemerintah daerah. *Jurnal Hukum Tata Negara, 13*(1).

Indra, J., & Harjono, P. (2023). Kewajiban pemerintah dalam pemulihan pasca-serangan siber (Incident Response) ditinjau dari asas pelayanan publik yang berkelanjutan. *Jurnal Hukum Responsif, 11*(1).

Jaya, N. W. A. (2019). Konsep tanggung jawab negara dalam perlindungan data pribadi warga negara. *Jurnal Hukum Internasional, 16*(4).

Kusumadewi, R. (2021). Risk management dalam tata kelola SPBE sebagai upaya pencegahan maladministrasi. *Jurnal Ilmu Pemerintahan dan Politik Lokal, 3*(2).

Lestari, S. (2022). Analisis yuridis terhadap maladministrasi pelayanan publik digital akibat data breach. *Jurnal Analisis Hukum, 6*(1).

Manurung, M. L. (2019). Penegakan hukum administratif terhadap kelalaian pejabat dalam pengamanan sistem informasi pemerintah. *Jurnal Kajian Administrasi Publik, 5*(2).

Nugroho, R. (2020). Peran auditor teknologi informasi dalam menilai kepatuhan SPBE terhadap standar keamanan. *Jurnal Teknologi Informasi dan Komunikasi (TIK), 9*(1).

Oktaviani, D. (2023). Penetration testing sebagai instrumen kepatuhan hukum administrasi dalam pengadaan sistem elektronik pemerintah. *Jurnal Teknologi dan Hukum, 4*(2).

Pratama, D. A. (2021). Integrasi asas-asas umum pemerintahan yang baik (AUPB) dalam kebijakan keamanan siber pemerintah. *Jurnal Hukum Tata Negara, 12*(1).

Puspitawati, D. (2022). Tinjauan hukum perlindungan data pribadi dalam konteks maladministrasi layanan publik pemerintah. *Jurnal Hukum Prioris, 11*(3).

Rahardjo, M. (2019). Kebijakan disaster recovery plan (DRP) sebagai manifestasi kewajiban administrasi negara dalam continuity of public service. *Jurnal Kebijakan Publik, 10*(2).

Ramadhan, M. Z. (2020). Akuntabilitas dan transparansi pemerintah dalam penanggulangan serangan ransomware terhadap sistem informasi publik. *Jurnal Hukum dan Pembangunan Ekonomi, 3*(1).

Sari, N. (2021). Tanggung jawab administratif pejabat administrasi negara dalam pengelolaan data strategis pemerintah. *Jurnal Administrasi Hukum Indonesia (JAHI), 9*(4).

Sitorus, R. M. (2023). Pengujian konsep detournement de pouvoir dalam kebijakan pengamanan data di lingkungan pemerintah. *Jurnal Hukum Pidana dan Hukum Administrasi, 5*(2).

Wijaya, R. (2022). Standar minimum keamanan sistem informasi pemerintah: Perspektif hukum dan teknis. *Jurnal Informatika dan Sistem Informasi, 1*(1).

Yulianti, R. (2018). Perlindungan hukum terhadap data kependudukan sebagai bagian dari pelayanan publik digital. *Jurnal Hukum Tata Usaha Negara, 4*(1).

Asshiddiqie, J. (2014). *Hukum administrasi negara dan prinsip-prinsip good governance. Sinar Grafika.*

Kadir, A. (2004). *Hukum dan penelitian hukum*. Citra Aditya Bhakti.

Marbun, B. N. (2017). *Dimensi-dimensi administrasi negara*. Ghalia Indonesia.

Santoso, L. Y. (2020). *Cyber security governance: Implementasi tata kelola keamanan siber di sektor publik.* Elex Media Komputindo.

Simbolon, R. M. (2023). *Hukum perlindungan data pribadi di Indonesia: Isu dan tantangan implementasi*. Prenada Media.

Badan Siber dan Sandi Negara (BSSN). (2023). Laporan monitoring dan analisis insiden siber Indonesia 2023. Retrieved from https://www.bssn.go.id/laporan-tahunan-2023

Kementerian Komunikasi dan Informatika (Kominfo RI). (2022). Pedoman teknis dan prosedur keamanan informasi SPBE. Retrieved from https://www.kominfo.go.id/spbe/pedoman-teknis

Ombudsman RI. (2024). Hasil kajian maladministrasi dalam layanan publik digital. Retrieved from https://www.ombudsman.go.id/kajian/maladministrasi-digital

Pusat Studi Hukum dan Kebijakan Indonesia (PSHK). (2023). Analisis kepatuhan hukum administrasi dalam pengamanan data pemerintah. Retrieved from https://www.pshk.or.id/publikasi/analisis-data-pemerintah

Setiadi, R. (2023, Oktober 10). Pentingnya koordinasi lintas sektoral dalam penanganan krisis siber pemerintah. Kompas.id. Retrieved from https://www.kompas.id/baca/analisis/2023/10/10/koordinasi-krisis-siber