

OPTIMALISASI FUNGSI JDIHN DALAM MENJAMIN KETERSEDIAAN DAN KEAUTENTIKAN DOKUMENTASI DAN INFORMASI HUKUM YANG TERKONSOLIDASI DEMI KETAHANAN HUKUM NASIONAL

*OPTIMIZING THE FUNCTION OF JDIHN IN ENSURING THE AVAILABILITY AND AUTHENTICITY OF
CONSOLIDATED LEGAL DOCUMENTATION AND INFORMATION FOR NATIONAL LEGAL RESILIENCE*

Wicipto Setiadi

Fakultas Hukum Universitas Pembangunan Nasional
Jl. RS. Fatmawati, Pondok Labu, Jakarta Selatan, 12450
e-mail: wiciptos@gmail.com

Kaharuddin

Fakultas Hukum Universitas Pembangunan Nasional
Jl. RS. Fatmawati, Pondok Labu, Jakarta Selatan, 12450
e-mail: kaharuddin@upnvj.ac.id

Ahmad Haris Junaidi

Badan Pembinaan Hukum Nasional
Jl. Mayjen Soetoyo, No. 10, Cililitan, Jakarta Timur, 13640
e-mail: ahmadharis.bphn@gmail.com

Abstrak

Transformasi digital dalam penyelenggaraan pemerintahan menuntut adanya sistem informasi hukum yang terintegrasi, valid, dan aman. Jaringan Dokumentasi dan Informasi Hukum Nasional (JDIHN), yang dibentuk berdasarkan Peraturan Presiden Nomor 33 Tahun 2012, memiliki peran strategis sebagai sarana penghimpunan, pengelolaan, dan penyebarluasan dokumentasi hukum nasional yang sah dan terkonsolidasi. Namun, implementasinya masih menghadapi tantangan serius, antara lain belum meratanya kapasitas teknis antaranggota, keterbatasan kelembagaan, serta belum diterapkannya standar pengelolaan informasi hukum digital yang mengacu pada praktik terbaik internasional. Penelitian ini menggunakan pendekatan yuridis normatif dengan metode deskriptif-kualitatif melalui studi literatur terhadap peraturan perundang-undangan, publikasi resmi, dan literatur akademik. Hasil kajian menunjukkan perlunya reformasi regulasi terhadap Perpres 33/2012 agar selaras dengan kebijakan Sistem Pemerintahan Berbasis Elektronik (SPBE), Perpres tentang Pelindungan Infrastruktur Informasi Vital, Perpres Satu Data Indonesia, serta Strategi Keamanan Siber Nasional. Selain itu, penguatan tata kelola JDIHN perlu diarahkan pada penerapan dokumen hukum digital-native dengan standar metadata yang seragam, adopsi standar keamanan informasi internasional (ISO/IEC 27001), serta peningkatan koordinasi kelembagaan. Optimalisasi ini diharapkan dapat menjamin keterlacakan, integritas, dan keautentikan dokumen hukum digital, sekaligus memperkuat ketahanan hukum nasional di tengah dinamika transformasi digital.

Kata kunci: JDIHN, dokumentasi hukum, *digital native*, keamanan informasi, ketahanan hukum nasional

Abstract

The digital transformation of governance requires an integrated, valid, and secure legal information system. The National Legal Documentation and Information Network (JDIHN), established under Presidential Regulation No. 33 of 2012, plays a strategic role as a platform for collecting, managing, and disseminating authentic and consolidated legal documentation. Nevertheless, its implementation still faces serious challenges, including uneven technical capacities among members, institutional limitations, and the absence of internationally recognized standards for managing digital legal information. This study applies a normative juridical approach with a descriptive-qualitative method through a review of legislation, official publications, and academic literature. The findings indicate the need for regulatory reform of Presidential Regulation No. 33/2012 to align with the Electronic-Based Government System (SPBE) policy, the Presidential Regulation on the Protection of Critical Information Infrastructure, the Presidential Regulation on One Data Indonesia, and the National Cybersecurity Strategy. Furthermore, strengthening JDIHN governance requires the adoption of digital-native legal documents with standardized metadata, the implementation of international information security standards (ISO/IEC 27001), and enhanced institutional coordination. This optimization is expected to ensure the traceability, integrity, and authenticity of digital legal documents while reinforcing national legal resilience in the context of digital transformation.

Keywords: JDIHN, legal documentation, *digital native*, information security, national legal resilience

A. Pendahuluan

Hak atas informasi merupakan salah satu hak asasi manusia yang dijamin dalam konstitusi. Pasal 28F Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 menegaskan bahwa setiap orang berhak untuk berkomunikasi dan memperoleh informasi guna mengembangkan pribadi dan lingkungan sosialnya, serta berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah, dan menyampaikan informasi dengan menggunakan segala jenis saluran yang tersedia.¹ Hak konstitusional ini menjadi fondasi penting bagi terselenggaranya kehidupan demokratis, karena akses terhadap informasi memungkinkan partisipasi masyarakat dalam pengambilan keputusan publik dan memperkuat akuntabilitas penyelenggara negara.

Sejalan dengan amanat konstitusi, pemerintah menetapkan Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (KIP). Undang-undang ini menegaskan empat prinsip utama: pertama, hak setiap orang untuk memperoleh informasi; kedua, kewajiban badan publik untuk menyediakan dan melayani permintaan informasi secara cepat, tepat, berbiaya ringan, dan sederhana; ketiga, pengecualian informasi yang bersifat ketat dan terbatas; dan keempat, kewajiban badan publik untuk membenahi sistem dokumentasi dan pelayanan informasi.² Prinsip-prinsip tersebut menegaskan bahwa keterbukaan informasi publik tidak sekadar pemenuhan hak warga negara, tetapi juga konsekuensi logis dari pelaksanaan pemerintahan yang baik (*good governance*). Dengan akses informasi yang luas, publik

dapat melakukan pengawasan, memperkuat legitimasi kebijakan, serta mencegah praktik korupsi, kolusi, dan nepotisme (KKN).

Dalam konteks penyelenggaraan negara hukum, keterbukaan informasi hukum memiliki posisi yang sangat strategis. Informasi hukum termasuk kategori informasi publik yang wajib tersedia setiap saat, karena menyangkut langsung hak warga negara untuk mengetahui dan memahami aturan yang berlaku. Tanpa akses yang mudah, cepat, dan otentik terhadap dokumen hukum, partisipasi masyarakat dalam kehidupan berbangsa akan melemah, kepastian hukum terancam, dan legitimasi kebijakan publik berpotensi terganggu. Dengan demikian, pengelolaan dokumentasi dan informasi hukum yang terkonsolidasi dan otentik bukan sekadar urusan teknis administrasi, melainkan bagian integral dari pemenuhan hak asasi manusia dan penguatan negara hukum demokratis.

Sebagai wujud implementasi prinsip keterbukaan informasi publik di bidang hukum, pemerintah membentuk Jaringan Dokumentasi dan Informasi Hukum Nasional (JDIHN) melalui Peraturan Presiden Nomor 33 Tahun 2012.³ Peraturan ini menugaskan Badan Pembinaan Hukum Nasional (BPHN) sebagai Pusat JDIHN yang bertanggung jawab membina, mengoordinasikan, dan mengintegrasikan pengelolaan dokumentasi hukum di seluruh kementerian, lembaga, dan pemerintah daerah. JDIHN dirancang sebagai sarana *single access point* bagi masyarakat untuk mengakses dokumen hukum yang otentik, valid, dan mutakhir. Dengan kehadiran JDIHN, diharapkan fragmentasi pengelolaan dokumentasi hukum dapat diatasi, sehingga publik memperoleh

¹ Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Pasal 28F.

² Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Penjelasan Umum.

³ Peraturan Presiden Nomor 33 Tahun 2012 tentang Jaringan Dokumentasi dan Informasi Hukum Nasional.

kepastian dan konsistensi dalam mengakses peraturan perundang-undangan.

Namun, implementasi JDIHN hingga kini masih menghadapi sejumlah tantangan mendasar. Pertama, belum semua anggota JDIHN memiliki kapasitas teknis, infrastruktur, maupun sumber daya manusia yang memadai untuk mengelola dokumentasi hukum digital secara efektif. Penelitian di beberapa daerah menunjukkan bahwa perbedaan kapasitas teknis antaranggota menyebabkan kualitas layanan yang tidak seragam, sehingga masyarakat di tingkat daerah sering mengalami keterbatasan dalam memperoleh dokumen hukum yang akurat dan terkini.⁴ Kedua, aspek keamanan informasi hukum digital belum mendapat perhatian memadai. Padahal, dalam era transformasi digital, dokumen hukum berpotensi menjadi target serangan siber, baik berupa peretasan, manipulasi isi dokumen, maupun sabotase sistem informasi. Tanpa sistem keamanan yang memadai, keaslian dan integritas dokumen hukum rentan dipertanyakan, yang pada gilirannya dapat menimbulkan ketidakpastian hukum.

Ketiga, penataan standar pengelolaan dokumen hukum digital yang digital native belum optimal. Sebagian besar dokumen hukum masih dikelola melalui digitalisasi pasca-fisik (pemindaian), bukan berbasis digital sejak penciptaan hingga pengundangan. Kondisi ini berimplikasi pada inkonsistensi metadata, fragmentasi basis data, serta kesulitan dalam menjamin validitas dan keterlacakan dokumen hukum. Padahal, praktik terbaik internasional seperti standar Akoma Ntoso menekankan

pentingnya interoperabilitas dokumen hukum digital dengan format terbuka untuk memastikan konsolidasi yang efektif di tingkat nasional maupun global.⁵

Keempat, tingkat literasi digital masyarakat dalam mengakses informasi hukum juga masih relatif rendah. Hasil kajian Majalah Hukum Nasional tahun 2024 menunjukkan bahwa banyak masyarakat lebih percaya pada dokumen hukum yang beredar di media sosial atau sumber tidak resmi, dibandingkan merujuk pada portal JDIHN.⁶ Rendahnya literasi ini menyebabkan peran strategis JDIHN dalam menjamin akses informasi hukum yang sah belum dimanfaatkan secara optimal. Dengan demikian, penguatan JDIHN tidak hanya menyangkut aspek teknis dan kelembagaan, tetapi juga menuntut strategi edukasi publik dan peningkatan literasi hukum digital.

Keterbatasan-keterbatasan tersebut menunjukkan adanya kesenjangan antara idealitas JDIHN sebagai pusat informasi hukum nasional dengan realitas implementasi di lapangan. Oleh karena itu, pemerintah merencanakan revisi Perpres 33 Tahun 2012 untuk menyesuaikan dengan perkembangan teknologi dan kebutuhan pengelolaan informasi hukum di era digital. Reformasi regulasi ini diarahkan pada integrasi JDIHN dengan kebijakan nasional lain seperti Perpres 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE), Perpres 39 Tahun 2019 tentang Satu Data Indonesia, Perpres 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital, serta Perpres 47 Tahun 2023

⁴ Badan Pembinaan Hukum Nasional, Laporan Tahunan JDIHN (Jakarta: BPHN, 2023).

⁵ UN Department of Economic and Social Affairs, Akoma Ntoso: Open Standards for Legal Documents (New York: UNDESA, 2018).

⁶ Ricca Anggraeni, JDIH dan Tantangan Literasi Digital, Majalah Hukum Nasional, (Jakarta: BPHN, 2024).

tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber.⁷

Selain reformasi regulasi, optimalisasi JDIHN juga harus mengadopsi standar keamanan informasi internasional seperti ISO/IEC 27001 guna menjamin kerahasiaan, integritas, dan ketersediaan data hukum. Adopsi standar ini sejalan dengan amanat PP Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, yang mewajibkan instansi pemerintah mengelola sistem elektronik strategis dengan standar keamanan minimum.⁸ Dengan demikian, penguatan tata kelola JDIHN tidak hanya berorientasi pada ketersediaan dokumen hukum, tetapi juga pada keandalan sistem pengamanan digital sebagai prasyarat legitimasi dan kepercayaan publik.

Lebih jauh, JDIHN harus dipandang sebagai bagian dari infrastruktur informasi vital nasional, mengingat dokumen hukum merupakan data strategis yang menentukan stabilitas sistem hukum, sosial, dan ekonomi negara. Gagalnya pengelolaan JDIHN dapat berimplikasi serius, mulai dari terganggunya akses publik terhadap regulasi hingga melemahkan legitimasi kebijakan negara. Oleh karena itu, optimalisasi JDIHN harus dilakukan dengan pendekatan multidimensional, mencakup aspek normatif, teknis, kelembagaan, serta literasi publik.

Dengan memperhatikan kerangka normatif serta tantangan praktis yang dihadapi, kajian ini diarahkan untuk menganalisis arah penguatan fungsi JDIHN dalam menjamin ketersediaan, keterkonsolidasian, dan keautentikan dokumen

hukum digital. Optimalisasi peran JDIHN penting karena dokumen hukum digital bukan hanya data administratif, melainkan aset informasi vital yang menopang kepastian hukum, legitimasi kebijakan, dan perlindungan hak konstitusional warga negara atas informasi. Dalam konteks ini, peran strategis JDIHN mencakup penyediaan akses publik terhadap dokumen hukum yang sah, mutakhir, dan terverifikasi, sehingga dapat mendorong transparansi penyelenggaraan negara, memperkuat kesadaran hukum masyarakat, serta memastikan tersedianya informasi hukum yang otoritatif. Namun, transformasi digital juga membawa tantangan serius berupa meningkatnya risiko serangan siber seperti peretasan, manipulasi data, atau ransomware, sementara kapasitas teknis antaranggota JDIHN masih belum merata. Kondisi ini menegaskan perlunya integrasi aspek keamanan siber dalam tata kelola dokumentasi hukum agar JDIHN tidak menjadi titik lemah dalam sistem pemerintahan berbasis elektronik.

Sejalan dengan itu, reformasi regulasi dan penataan kelembagaan JDIHN menjadi kebutuhan mendesak agar selaras dengan kebijakan Sistem Pemerintahan Berbasis Elektronik (SPBE), Satu Data Indonesia, serta Strategi Keamanan Siber Nasional. Revisi Peraturan Presiden Nomor 33 Tahun 2012 harus diarahkan pada penguatan pengelolaan dokumen hukum berbasis digital-native, penetapan standar interoperabilitas data, serta penegasan kewenangan lembaga dalam pengelolaan dokumentasi hukum nasional.

⁷ Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik; Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik; Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia; Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital; dan Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber.

⁸ International Organization for Standardization, ISO/IEC 27001:2022, Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements (Geneva: ISO, 2022).

Optimalisasi JDIHN juga memerlukan langkah strategis berupa penerapan standar keamanan informasi internasional (ISO/IEC 27001), pemanfaatan teknologi blockchain untuk menjaga integritas dokumen, pembentukan unit khusus keamanan siber di bawah koordinasi BPHN dan BSSN, serta pengembangan *maturity model* sebagai alat evaluasi kesiapan anggota JDIHN. Dengan demikian, JDIHN diharapkan mampu bertransformasi dari sekadar instrumen administratif menjadi elemen strategis dalam ketahanan hukum nasional sekaligus bagian integral dari infrastruktur keamanan siber Indonesia.

B. Metode Penelitian

Penelitian ini menggunakan metode yuridis normatif,⁹ yaitu penelitian hukum yang menitikberatkan pada kajian terhadap asas-asas, norma, dan peraturan perundang-undangan yang berlaku, serta doktrin hukum yang berkembang dalam literatur akademik. Metode ini dipilih karena fokus utama penelitian adalah menganalisis posisi, peran, dan tantangan Jaringan Dokumentasi dan Informasi Hukum Nasional (JDIHN) dalam sistem hukum nasional, khususnya dalam kaitannya dengan tata kelola informasi hukum digital dan keamanan siber.

Pendekatan yang digunakan adalah deskriptif-kualitatif.¹⁰ Data dikumpulkan melalui studi kepustakaan (*library research*) terhadap tiga sumber utama. Pertama, bahan hukum primer berupa peraturan perundang-undangan, antara lain Peraturan Presiden Nomor 33 Tahun 2012 tentang JDIHN, Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan

Berbasis Elektronik (SPBE), Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital, Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia, serta Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber.

Kedua, bahan hukum sekunder berupa dokumen resmi pemerintah dan lembaga terkait, seperti Laporan Tahunan JDIHN yang diterbitkan oleh BPHN, laporan Badan Siber dan Sandi Negara (BSSN) mengenai ancaman siber nasional, serta publikasi dari Kementerian Komunikasi dan Informatika mengenai tata kelola sistem elektronik strategis.

Ketiga, bahan hukum tersier berupa kajian literatur ilmiah, baik nasional maupun internasional, yang membahas teori sistem informasi hukum, prinsip manajemen keamanan informasi, serta praktik dokumentasi hukum digital dan praktik terbaik pengelolaan dokumentasi hukum digital di negara lain.

Data yang diperoleh dianalisis menggunakan teknik analisis isi (*content analysis*), yakni dengan mengidentifikasi tema-tema utama, pola hubungan antarregulasi, serta kesenjangan antara norma dan praktik dalam pengelolaan informasi hukum dan pengamanan digital. Pendekatan ini juga didukung dengan teknik normatif-komparatif, guna membandingkan ketentuan yang ada dengan praktik baik (*best practices*) pengelolaan sistem dokumentasi hukum di negara lain atau standar internasional, mengenai manajemen keamanan informasi.¹¹

Dengan metode ini, penelitian diharapkan mampu memberikan analisis yang mendalam

⁹ Soerjono dan Sri Mamudji Soekanto, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat* (Jakarta: Rajawali Pers, 2012), hlm. 14.

¹⁰ Moleong, Lexy J., *Metodologi Penelitian Kualitatif*, Bandung: Remaja Rosdakarya, 2018, hlm. 6–7.

¹¹ Zuchri Abdussamad, *Metode Penelitian Kualitatif*, CV. syakir Media Press, Makassar, 2021, hlm. 186.

dan argumentasi normatif yang kuat mengenai arah optimalisasi fungsi JDIHN, baik dari sisi regulasi, kelembagaan, maupun pengelolaan teknologi informasi hukum nasional.

C. Pembahasan

1. Peran Sentral JDIHN dalam Ekosistem Informasi Hukum Nasional

Jaringan Dokumentasi dan Informasi Hukum Nasional (JDIHN) merupakan infrastruktur kelembagaan yang memiliki posisi strategis dalam pembangunan sistem hukum nasional yang transparan, akuntabel, dan partisipatif. Dibentuk melalui Peraturan Presiden Nomor 33 Tahun 2012, JDIHN hadir untuk menjawab kebutuhan masyarakat terhadap dokumentasi hukum yang lengkap, akurat, mudah diakses, dan dapat dimanfaatkan untuk berbagai tujuan, mulai dari perumusan kebijakan, penelitian ilmiah, pendidikan hukum, hingga penegakan hukum.¹² Keberadaan JDIHN sekaligus menjadi representasi komitmen negara dalam mewujudkan sistem hukum yang terbuka dan inklusif, sejalan dengan amanat Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik yang menegaskan hak publik atas informasi hukum.¹³

Informasi hukum merupakan salah satu bentuk informasi publik yang wajib tersedia setiap saat karena menyangkut langsung dengan hak warga negara untuk mengetahui aturan yang mengikat dirinya. Akses luas dan setara terhadap dokumen hukum menjadi elemen penting dalam menjamin kepastian hukum (*legal certainty*), mendorong partisipasi

masyarakat dalam proses legislasi, serta memperkuat kontrol publik terhadap kebijakan pemerintah.¹⁴ Dengan demikian, penguatan peran JDIHN tidak sekadar fungsi teknis, melainkan bentuk aktualisasi perlindungan hak asasi manusia, khususnya hak atas informasi.

Dalam kerangka teoritis, Mahfud MD menegaskan bahwa informasi hukum yang tersebar luas akan memperkuat budaya hukum dan meningkatkan kesadaran hukum masyarakat.¹⁵ Satjipto Rahardjo juga mengingatkan bahwa hukum tidak cukup hanya hadir dalam norma tertulis, melainkan harus disosialisasikan dan diinternalisasikan agar hidup dalam masyarakat.¹⁶ Hal ini menunjukkan JDIHN berfungsi sebagai jembatan antara pembentukan hukum dan kesadaran hukum publik.

Seiring perkembangan teknologi informasi, peran JDIHN semakin strategis dalam mendukung sistem pemerintahan berbasis elektronik (e-Government). Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) menekankan pentingnya integrasi sistem informasi, termasuk di bidang hukum. Dalam konteks ini, JDIHN bukan hanya repositori hukum digital, tetapi juga *information backbone* yang menopang layanan publik berbasis regulasi.¹⁷ Integrasi ini memungkinkan interoperabilitas data hukum antarinstansi, menghindari duplikasi dokumen, dan meningkatkan efektivitas pengambilan keputusan berbasis hukum.

Secara kelembagaan, JDIHN juga mendukung proses legislasi nasional, terutama dalam

¹² Peraturan Presiden Nomor 33 Tahun 2012 tentang Jaringan Dokumentasi dan Informasi Hukum Nasional.

¹³ Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik.

¹⁴ Ridwan Khairandy, *Hukum Informasi dan Transaksi Elektronik* (Yogyakarta: FH UII Press, 2018), hlm. 44.

¹⁵ Mahfud MD, *Politik Hukum di Indonesia* (Jakarta: Rajawali Pers, 2009), hlm. 121.

¹⁶ Satjipto Rahardjo, *Ilmu Hukum* (Bandung: Citra Aditya Bakti, 2006), hlm. 215.

¹⁷ Republik Indonesia, Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.

harmonisasi peraturan perundang-undangan dan pengawasan regulasi. Akses dokumen hukum dari berbagai instansi memungkinkan identifikasi tumpang tindih regulasi, disharmoni norma, hingga menjadi basis informasi dalam uji materiil atau judicial review di Mahkamah Konstitusi dan Mahkamah Agung.¹⁸ Dengan ketersediaan dokumen hukum yang terdigitalisasi dan tervalidasi, proses legislasi dapat berjalan lebih efisien, konsisten, dan terhindar dari konflik normatif.

Namun, realisasi peran sentral JDIHN belum sepenuhnya terwujud. Tantangan utama antara lain:

- a. Fragmentasi database hukum: setiap instansi masih mengelola basis data hukum secara mandiri, dengan standar berbeda, sehingga sering terjadi perbedaan jumlah, jenis, atau isi dokumen hukum.¹⁹
- b. Ketiadaan sistem terpadu: belum ada *single national database* yang utuh, terkini, dan real-time, sehingga pencarian dokumen hukum sering tidak efisien.
- c. Rendahnya literasi digital: masyarakat sering lebih percaya pada dokumen yang beredar di media sosial dibanding portal resmi JDIHN. Kajian Majalah Hukum Nasional 2024 menunjukkan literasi digital hukum masih rendah, menyebabkan informasi hukum resmi kurang optimal dimanfaatkan.²⁰
- d. Standar digital-native: sebagian besar dokumen hukum masih berbasis *scan*, belum

seluruhnya digital-native dengan metadata terstandar seperti praktik internasional *Akoma Ntoso*.²¹

Di era digital yang sarat ancaman siber, JDIHN juga harus memastikan aspek authenticity, integrity, dan resilience dari dokumen hukum digital.²² Hal ini penting untuk menjaga kepercayaan publik, mengingat dokumen hukum menjadi dasar administrasi dan kebijakan negara. Karena itu, penguatan JDIHN memerlukan dukungan regulasi, SDM, infrastruktur digital, serta penerapan standar keamanan internasional seperti ISO/IEC 27001.²³

Dengan memperhatikan seluruh aspek tersebut, JDIHN tidak lagi dapat dipandang sebagai fungsi administratif semata, melainkan pilar utama dalam membangun tata kelola hukum nasional yang modern, transparan, dan akuntabel. Optimalisasi JDIHN harus menjadi agenda strategis nasional yang didukung oleh regulasi yang kuat, sumber daya yang memadai, dan komitmen politik yang konsisten.

2. Analisis Risiko dan Ancaman Siber terhadap Informasi Hukum Nasional

Transformasi digital dalam penyelenggaraan pemerintahan telah membawa manfaat besar bagi keterbukaan informasi publik. Namun, digitalisasi juga menghadirkan risiko baru berupa ancaman siber terhadap keberlangsungan layanan publik, termasuk sistem dokumentasi

¹⁸ Tryavena Martha Adhiasti dan Yuwanto, "Legal Documentation and Information Network (JDIH) as an Implementation of e-Government System in the Regional Representative Council of the Republic of Indonesia," *Jurnal Politik dan Pemerintahan* 15, no. 2 (2024): 145–163.

¹⁹ Rahmat Trijono, "Pushing the Improvement of the Indonesian Legal Database for Law Research and Economic Research," *Indonesian Law Journal* 12 (2019): 75–95.

²⁰ Op. Cit, Ricca Anggraeni, *JDIH dan Tantangan Literasi Digital*, Majalah Hukum Nasional, Jakarta, BPHN, 2024.

²¹ UN Department of Economic and Social Affairs, *Akoma Ntoso: Open Standards for Legal Documents* (New York: UNDESA, 2018).

²² Moch. Syaiful Bakhri, *Pengantar Hukum Keamanan Siber* (Jakarta: Prenada Media, 2021), hlm. 97.

²³ International Organization for Standardization, *ISO/IEC 27001:2022, Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements* (Geneva: ISO, 2022).

hukum nasional. Dalam konteks ini, Jaringan Dokumentasi dan Informasi Hukum Nasional (JDIHN) memiliki posisi yang rawan karena menyimpan dan mendistribusikan dokumen hukum resmi yang memiliki nilai strategis bagi negara dan masyarakat.

Ancaman terhadap sistem dokumentasi hukum dapat diklasifikasikan ke dalam beberapa bentuk utama. Pertama, peretasan (hacking), yakni upaya memperoleh akses ilegal untuk mengubah, mencuri, atau merusak data hukum. Ancaman ini berpotensi menimbulkan kebocoran data regulasi penting maupun manipulasi substansi dokumen.²⁴ Kedua, modifikasi ilegal (tampering), yaitu perubahan isi dokumen hukum tanpa otorisasi. Praktik semacam ini sangat berbahaya karena dapat menciptakan versi hukum digital yang berbeda dengan naskah otentik, sehingga menyesatkan publik dan berimplikasi pada legitimasi hukum.²⁵ Ketiga, serangan ransomware, yakni upaya mengenkripsi dokumen hukum dan menuntut tebusan, yang dapat melumpuhkan layanan JDIHN jika tidak disertai sistem cadangan data yang memadai.²⁶ Keempat, pencurian kredensial (phishing) yang menasar akun administrator atau pengelola sistem, sehingga membuka peluang eksploitasi dari dalam. Kelima, eksploitasi perangkat lunak usang yang tidak diperbarui secara berkala, menjadikan sistem lebih rentan terhadap serangan siber.²⁷

Secara empiris, sistem JDIHN rata-rata mengalami sekitar 10 percobaan peretasan per tahun.²⁸ Jumlah ini relatif rendah bila dibandingkan dengan skala ancaman siber nasional. Menurut laporan Badan Siber dan Sandi Negara (BSSN), pada tahun 2022 saja terdeteksi lebih dari 700 juta anomali lalu lintas siber di sektor pemerintahan, termasuk sistem layanan hukum digital.²⁹ Rendahnya angka serangan yang tercatat terhadap JDIHN dapat dijelaskan oleh dua faktor. Pertama, jumlah pengguna JDIHN masih terbatas. Survei BPHN tahun 2023 menunjukkan bahwa rata-rata pengunjung situs JDIHN hanya sekitar 60.000 pengguna per tahun, meskipun indeks kepuasan pengguna mencapai 93,21, jauh di atas target nasional sebesar 77.³⁰ Kedua, infrastruktur JDIHN masih tersebar di berbagai situs kementerian/lembaga dan pemerintah daerah. Hingga Oktober 2023, baru 1.232 situs JDIH yang terintegrasi dari total 1.662 anggota JDIHN, dengan jumlah koleksi sekitar 557.509 dokumen hukum.³¹ Fragmentasi ini membuat lalu lintas di masing-masing situs relatif kecil, sehingga mengurangi insentif bagi pelaku siber untuk melakukan serangan berskala besar.

Namun, kondisi ini tidak berarti JDIHN aman. Justru sebaliknya, rendahnya serangan bukan indikator kekuatan sistem, melainkan mencerminkan rendahnya eksposur publik terhadap JDIHN. Apabila pengguna meningkat

²⁴ Andi Hamzah, *Hukum Siber Indonesia* (Jakarta: Sinar Grafika, 2015), hlm. 77.

²⁵ Op. Cit. Rahmat Trijono, "Pushing the Improvement of the Indonesian Legal Database for Law Research and Economic Research," *Indonesian Law Journal* 12 (2019): 75–95.

²⁶ Herbert J. Mattord and Michael E. Whitman, *Principles of Information Security*, 6th ed. (Boston: Cengage Learning, 2018), hlm. 241.

²⁷ Abdul Yusriyadi, *Hukum dan Teknologi Informasi* (Malang: Setara Press, 2020), hlm. 92.

²⁸ Hasil wawancara dengan pejabat Badan Pembinaan Hukum Nasional (BPHN), Jakarta, Juli 2025.

²⁹ Badan Siber dan Sandi Negara, *Statistik Ancaman Siber Indonesia Tahun 2022* (Jakarta: BSSN, 2023).

³⁰ Badan Pembinaan Hukum Nasional, *Laporan Kinerja Tahunan BPHN 2023* (Jakarta: BPHN, 2024), hlm. 51.

³¹ <https://www.hukumonline.com>, "Kemenkumham Anugerahkan 57 Anggota JDIHN Terbaik Tahun 2023," diakses 25 Agustus 2025,

seiring transformasi digital hukum nasional, maka JDIHN berpotensi menjadi target serangan yang jauh lebih serius.

Dari perspektif hukum, dokumen hukum digital merupakan bagian dari informasi elektronik strategis sebagaimana diatur dalam PP Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Regulasi ini mewajibkan setiap penyelenggara sistem elektronik pemerintah untuk menjamin kerahasiaan, integritas, ketersediaan, dan autentikasi data.³² Selain itu, Perpres Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber secara eksplisit mengklasifikasikan informasi hukum sebagai infrastruktur informasi vital (IIV) yang harus mendapat perlindungan ekstra.³³ Namun demikian, Perpres Nomor 33 Tahun 2012 tentang JDIHN maupun Permenkumham Nomor 2 Tahun 2013 belum mengatur secara detail mengenai standar pengamanan digital, seperti enkripsi, *access control*, *audit trail*, maupun prosedur penanganan insiden (*incident response protocol*).³⁴

Sejumlah pakar hukum menekankan pentingnya penguatan keamanan informasi hukum. Ridwan Khairandy menilai bahwa sistem hukum digital tanpa manajemen keamanan informasi berpotensi melanggar prinsip kehati-hatian administrasi negara.³⁵ Sementara itu, Moch. Syaiful Bakhri menegaskan bahwa dokumen hukum digital merupakan objek vital strategis yang memerlukan perlindungan

setara dengan data intelijen negara.³⁶ Literatur internasional, seperti Cybersecurity Framework dari National Institute of Standards and Technology (NIST) dan standar internasional ISO/IEC 27001, mendorong penerapan pendekatan risk-based governance yang mencakup identifikasi risiko, pengukuran dampak, mitigasi, serta evaluasi berkelanjutan.³⁷

Dengan demikian, analisis terhadap ancaman siber menunjukkan bahwa meskipun serangan langsung terhadap JDIHN masih relatif rendah, hal itu bukan indikator keamanan yang memadai. Rendahnya jumlah pengguna dan fragmentasi sistem justru membuat potensi ancaman siber belum terekspos secara penuh. Jika tidak diperkuat dengan standar keamanan yang ketat, peningkatan jumlah pengguna di masa depan dapat mengubah JDIHN menjadi target utama serangan siber. Oleh karena itu, penguatan aspek keamanan informasi hukum dalam JDIHN merupakan kebutuhan strategis yang mendesak.

3. Integrasi Keamanan Siber dalam Tata Kelola Sistem Informasi Hukum

Keamanan siber dalam tata kelola sistem informasi hukum tidak dapat dipandang sebagai aspek teknis tambahan, melainkan sebagai fondasi utama yang melekat dalam keseluruhan arsitektur Jaringan Dokumentasi dan Informasi Hukum Nasional (JDIHN). Sistem hukum digital yang tidak dilindungi dengan baik berisiko menimbulkan keraguan publik terhadap

³² Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

³³ Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber.

³⁴ Peraturan Presiden Nomor 33 Tahun 2012 tentang JDIHN; Permenkumham Nomor 2 Tahun 2013 tentang JDIHN.

³⁵ Ridwan Khairandy, *Hukum Informasi dan Transaksi Elektronik* (Yogyakarta: FH UII Press, 2018), hlm. 44.

³⁶ Moch. Syaiful Bakhri, *Pengantar Hukum Keamanan Siber* (Jakarta: Prenada Media, 2021), hlm. 97.

³⁷ International Organization for Standardization, *ISO/IEC 27001:2022, Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements* (Geneva: ISO, 2022); National Institute of Standards and Technology (NIST), *Cybersecurity Framework* (Gaithersburg: NIST, 2018).

validitas dokumen hukum yang dipublikasikan, dan pada gilirannya melemahkan legitimasi negara hukum.³⁸ Oleh karena itu, integrasi keamanan siber harus dirancang *by design*, yakni sebagai bagian integral dari siklus hidup sistem informasi hukum sejak tahap perencanaan, pengembangan, hingga operasionalisasi.

Standar minimum keamanan informasi dikenal dengan CIA triad, yaitu confidentiality (kerahasiaan), integrity (integritas), dan availability (ketersediaan).³⁹ Dalam konteks JDIHN, prinsip ini bermakna bahwa:

- a. Kerahasiaan harus dijaga agar dokumen hukum tidak dapat dimanipulasi oleh pihak yang tidak berwenang.
- b. Integritas harus dipastikan sehingga setiap dokumen hukum yang diakses publik adalah versi otentik yang sesuai dengan naskah resmi.
- c. Ketersediaan harus dijamin agar akses publik terhadap dokumen hukum tidak terganggu akibat serangan siber maupun kegagalan sistem.

Ketiga prinsip ini sejalan dengan mandat Pasal 15 Undang-Undang Nomor 11 Tahun 2008 jo. UU Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE) yang mewajibkan setiap penyelenggara sistem elektronik menjamin keandalan dan keamanan sistem.⁴⁰

Untuk memastikan tata kelola keamanan yang adaptif, JDIHN perlu mengadopsi standar

internasional seperti ISO/IEC 27001 yang mengatur sistem manajemen keamanan informasi (Information Security Management System/ISMS). Standar ini mencakup kebijakan keamanan, manajemen risiko, pengendalian akses, audit berkala, hingga pelatihan siber bagi pengelola sistem.⁴¹ Adopsi ISO/IEC 27001 juga didukung oleh PP Nomor 71 Tahun 2019 yang mewajibkan instansi pemerintah menggunakan standar keamanan dalam penyelenggaraan sistem elektronik strategis.⁴²

Selain itu, integrasi teknologi baru seperti blockchain dapat digunakan untuk menjamin keaslian dokumen hukum melalui sistem pencatatan yang tidak dapat diubah (*immutable ledger*). Pengalaman Estonia dan Uni Emirat Arab menunjukkan bahwa blockchain mampu meningkatkan kepercayaan publik terhadap dokumen digital.⁴³ Cloud computing dengan lapisan keamanan berlapis juga dapat mendukung aksesibilitas dokumen hukum yang lebih luas, meski tetap memerlukan kebijakan enkripsi dan proteksi data yang ketat.

Meski kebutuhan integrasi keamanan siber sudah mendesak, regulasi yang ada belum sepenuhnya mengakomodasi kebutuhan ini. Perpres Nomor 33 Tahun 2012 hanya menekankan aspek koordinasi kelembagaan tanpa mengatur standar pengamanan digital. Demikian pula Permenkumham Nomor 2 Tahun 2013 tidak menyertakan klausul mengenai protokol keamanan siber.⁴⁴

³⁸ Andi Hamzah, *Hukum Siber Indonesia* (Jakarta: Sinar Grafika, 2015), hlm. 77.

³⁹ Herbert J. Mattord and Michael E. Whitman, *Principles of Information Security*, 6th ed. (Boston: Cengage Learning, 2018), hlm. 33.

⁴⁰ Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, diubah dengan UU Nomor 19 Tahun 2016.

⁴¹ Op Cit, International Organization for Standardization, ISO/IEC 27001:2022.

⁴² Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

⁴³ Ahmed Alketbi, Qusay H. Mahmoud, dan Mahmoud Nasralla, "Blockchain for Government Services—Use Cases, Security Benefits and Challenges," 2018 IEEE International Conference on Internet of Things and Intelligence System (IOTAIS).

⁴⁴ Peraturan Presiden Nomor 33 Tahun 2012 tentang JDIHN; Permenkumham Nomor 2 Tahun 2013 tentang JDIHN.

Dari sisi kelembagaan, Badan Pembinaan Hukum Nasional (BPHN) sebagai Pusat JDIHN belum memiliki unit khusus yang menangani keamanan informasi hukum. Padahal, sebagai national legal backbone, JDIHN memerlukan struktur organisasi yang mampu melakukan monitoring keamanan secara real time, menyusun incident response protocol, serta menjalin koordinasi dengan Badan Siber dan Sandi Negara (BSSN).⁴⁵

Integrasi JDIHN ke dalam Sistem Pemerintahan Berbasis Elektronik (SPBE) sebagaimana diatur dalam Perpres 95 Tahun 2018 harus dilihat sebagai momentum untuk memperkuat tata kelola keamanan hukum digital. SPBE menekankan interoperabilitas antar sistem pemerintah, yang berarti JDIHN tidak dapat berdiri sendiri, melainkan harus menjadi bagian dari arsitektur keamanan siber nasional.⁴⁶

Lebih jauh, Perpres 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber menempatkan informasi hukum dalam kategori infrastruktur informasi vital (IIV). Hal ini menuntut agar JDIHN tidak hanya dijaga pada level teknis, tetapi juga menjadi prioritas perlindungan nasional yang setara dengan sektor energi, pertahanan, dan keuangan.⁴⁷

Dengan memperhatikan aspek teknis, normatif, dan kelembagaan, integrasi keamanan siber dalam tata kelola JDIHN merupakan keharusan. Tanpa integrasi ini, JDIHN hanya akan menjadi repositori hukum yang rentan diserang dan diragukan validitasnya. Sebaliknya, dengan mengadopsi standar internasional,

memanfaatkan teknologi baru, dan memperkuat koordinasi kelembagaan, JDIHN dapat berfungsi sebagai sumber kebenaran tunggal (single source of truth) dalam sistem hukum digital Indonesia.

4. Reformasi Regulasi dan Penataan Sistem Digitalisasi JDIHN

Dalam rangka menjawab tantangan transformasi digital dan keamanan informasi hukum, pembaruan regulasi Jaringan Dokumentasi dan Informasi Hukum Nasional (JDIHN) menjadi keharusan strategis. Kerangka hukum yang ada saat ini, yakni Peraturan Presiden Nomor 33 Tahun 2012, masih berfokus pada struktur kelembagaan dan koordinasi, tanpa secara eksplisit mengatur pengelolaan dokumen hukum berbasis digital dan sistem pengamanan siber. Hal ini menyebabkan kesenjangan antara tuntutan era digital dan kapasitas kelembagaan yang ada.

Rencana revisi Perpres tersebut menjadi momentum penting untuk melakukan reformasi regulatif yang mencakup pembaruan teknis, tata kelola, dan integrasi sistem. Setidaknya terdapat empat arah utama reformasi yang mendesak untuk dilakukan:

a. Penegasan Sistem Dokumentasi Hukum Digital yang Valid

Regulasi baru perlu menegaskan bahwa pengelolaan dokumentasi hukum dilakukan secara digital-native, yakni berbasis digital sejak proses penciptaan hingga diseminasi, bukan sekadar digitalisasi pasca-fisik. Ini termasuk kewajiban penggunaan tanda tangan elektronik tersertifikasi, sistem metadata standar, serta

⁴⁵ Op Cit, Laporan Kinerja Tahunan BPHN 2023 (Jakarta: BPHN, 2024), hlm. 62.

⁴⁶ Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.

⁴⁷ Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber.

integrasi dengan sistem keamanan informasi berbasis ISO/IEC 27001. Ketentuan ini juga harus memperkuat legalitas dokumen hukum elektronik sebagai dokumen otentik sesuai Pasal 5 dan Pasal 6 Undang-Undang ITE.⁴⁸

b. Penataan standar dokumen dan informasi yang dikelola kementerian/lembaga dan daerah

Salah satu tantangan fundamental dalam pengelolaan informasi hukum nasional dewasa ini adalah belum optimalnya penataan standar pengelolaan dokumen dan informasi hukum yang dilakukan oleh kementerian, lembaga, dan pemerintah daerah. Permasalahan ini muncul akibat belum adanya pedoman yang tegas dan seragam mengenai batasan kewenangan serta cakupan tanggung jawab masing-masing entitas dalam pengelolaan dokumen hukum. Ketidakteraturan ini berimplikasi pada terjadinya ketidaksinkronan data, duplikasi dokumen, serta penyebaran informasi hukum yang tidak valid di ruang publik.

Idealnya, pengelolaan informasi hukum oleh setiap instansi pemerintah harus diselaraskan dengan lingkup kewenangan penerbitan peraturan perundang-undangan yang dimiliki oleh instansi yang bersangkutan. Keselarasan tersebut sangat penting untuk menjamin validitas hukum dari setiap dokumen yang disebarluaskan kepada publik, sekaligus mencegah terjadinya disinformasi atau kekeliruan dalam pemahaman hukum oleh masyarakat. Namun demikian, dalam praktiknya, desentralisasi pengelolaan informasi hukum tanpa mekanisme pengendalian dan koordinasi yang ketat justru berkontribusi terhadap fragmentasi data hukum nasional.

Kebijakan yang memberikan keleluasaan kepada kementerian/lembaga dan pemerintah daerah untuk mengelola sendiri dokumen dan informasi hukum yang berkaitan dengan bidang tugas dan fungsinya, meskipun memiliki semangat desentralisasi informasi, ternyata turut menimbulkan konsekuensi negatif berupa redundansi dan ketidakseragaman data. Fenomena duplikasi dokumen, perbedaan jumlah data peraturan, bahkan perbedaan substansi dokumen hukum yang diunggah oleh berbagai instansi, telah menjadi permasalahan serius yang menimbulkan kebingungan bagi publik. Dalam sejumlah temuan, diketahui bahwa dokumen hukum yang sama dapat diakses melalui berbagai laman resmi instansi pemerintah, namun dengan versi redaksional dan muatan normatif yang berbeda. Situasi ini tidak hanya merugikan pengguna informasi hukum, tetapi juga melemahkan kredibilitas negara dalam menjamin kepastian hukum.

Lebih jauh, terdapat indikasi ketidaksesuaian antara data peraturan perundang-undangan yang tersimpan dalam database satu instansi dengan database instansi lainnya. Misalnya, terdapat perbedaan jumlah Peraturan Pemerintah atau Peraturan Presiden yang tercantum dalam portal kementerian tertentu dibandingkan dengan data yang tersedia di instansi pusat seperti Sekretariat Negara. Bahkan dalam beberapa kasus, substansi normatif dari dokumen yang diunggah menunjukkan ketidaksesuaian, baik dalam aspek sistematika maupun materi muatan. Hal ini menunjukkan bahwa tidak seluruh instansi memiliki kapasitas, standar teknis, maupun mekanisme validasi yang memadai dalam pengelolaan data hukum.

⁴⁸ Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo. Undang-Undang Nomor 19 Tahun 2016, Pasal 5-6.

Menyikapi permasalahan tersebut, diperlukan langkah strategis untuk memperjelas delineasi kewenangan pengelolaan informasi hukum. JDIHN, sebagai simpul koordinasi nasional dalam bidang dokumentasi dan informasi hukum, perlu menegaskan bahwa setiap instansi hanya diperkenankan untuk mengelola dan menyebarkan dokumen hukum yang merupakan produk dari kewenangannya sendiri. Artinya, kementerian, lembaga, dan pemerintah daerah hanya berhak untuk mempublikasikan dokumen hukum yang secara sah mereka terbitkan sebagai bagian dari output kelembagaan mereka. Dengan demikian, dokumen hukum yang bersumber dari tingkat nasional seperti Undang-Undang, Peraturan Pemerintah, dan Peraturan Presiden harus dikelola secara eksklusif oleh Sekretariat Negara sebagai lembaga yang memiliki mandat resmi dalam pengundangan dan penyebaran regulasi nasional.

Adapun untuk produk hukum yang bersifat teknis dan berada di bawah hirarki Undang-Undang, seperti Peraturan Menteri, Keputusan Presiden, Keputusan Menteri, maupun regulasi sektoral lainnya, pengelolaan informasinya seyogianya dipusatkan pada Kementerian Hukum dan Hak Asasi Manusia, khususnya oleh Direktorat Jenderal Peraturan Perundang-Undangan. Lembaga ini memiliki otoritas konstitusional untuk memastikan keabsahan substansi normatif, serta memiliki mekanisme verifikasi dan harmonisasi regulasi yang lebih sistematis. Sementara itu, untuk peraturan daerah, pengelolaan dan penyebaran dokumennya tetap menjadi kewenangan pemerintah daerah yang menerbitkan, dengan ketentuan bahwa setiap data tersebut tetap harus terhubung dengan sistem JDIHN secara interoperabel dan tersinkronisasi secara berkala.

Penataan ini tidak hanya penting dari perspektif ketertiban administratif, tetapi juga menjadi prasyarat mutlak bagi terciptanya sistem informasi hukum nasional yang akuntabel dan terpercaya. Standardisasi pengelolaan data hukum antar instansi akan meminimalkan kesenjangan informasi, meningkatkan efisiensi pencarian dokumen, serta memperkuat posisi JDIHN sebagai basis data hukum nasional yang otoritatif. Dalam jangka panjang, penataan ini akan berkontribusi pada penguatan prinsip legal certainty, mendorong konsistensi kebijakan lintas sektor, serta mendukung transformasi digital di bidang hukum sebagaimana diamanatkan dalam kebijakan Sistem Pemerintahan Berbasis Elektronik (SPBE).

Dengan demikian, penataan standar dokumen dan informasi hukum oleh kementerian, lembaga, dan pemerintah daerah merupakan bagian dari agenda reformasi hukum nasional yang harus segera diimplementasikan secara sistemik. Langkah ini memerlukan dukungan regulasi yang kuat, koordinasi antar lembaga yang efektif, serta penguatan kapasitas kelembagaan dalam pengelolaan sistem informasi hukum. Sebab, tanpa adanya arsitektur kelembagaan yang rapi dan berbasis pada pembagian peran yang jelas, maka cita-cita untuk mewujudkan keterpaduan informasi hukum nasional melalui JDIHN hanya akan menjadi wacana tanpa realisasi yang bermakna.

c. Penetapan Standar Teknis Keamanan dan Interoperabilitas Sistem

Dokumen hukum tidak hanya harus aman, tetapi juga dapat dibagikan, dicocokkan, dan diverifikasi oleh sistem instansi lain. Oleh karena itu, diperlukan penetapan standar interoperabilitas dalam bentuk format terbuka (open legal data standards) yang sesuai dengan pedoman Arsitektur SPBE Nasional. Hal ini

selaras dengan ketentuan Pasal 4 dan 5 Perpres Nomor 95 Tahun 2018, yang menekankan pentingnya integrasi dan keterpaduan dalam sistem elektronik pemerintahan.⁴⁹

Selain interoperabilitas, perlu juga diatur standar keamanan minimum, seperti enkripsi end-to-end, pemisahan akses berdasarkan peran, sistem cadangan dan pemulihan bencana (disaster recovery), serta prosedur respons insiden siber (incident response protocol).

d. Restrukturisasi Kelembagaan dan Peningkatan Koordinasi Nasional

Badan Pembinaan Hukum Nasional (BPHN) sebagai Pusat JDIHN perlu diperkuat perannya dalam standarisasi, pembinaan teknis, dan pemantauan terhadap seluruh anggota JDIHN. Regulasi baru dapat menetapkan pembentukan unit khusus keamanan siber dokumentasi hukum di bawah BPHN yang bekerja sama langsung dengan Badan Siber dan Sandi Negara (BSSN).

Selain itu, untuk meningkatkan efektivitas koordinasi, perlu dibentuk forum koordinasi nasional JDIHN berbasis digital, dengan dashboard pengawasan terpadu, pelaporan berkala, serta sistem peringatan dini terhadap gangguan siber.

e. Integrasi JDIHN dengan Platform Hukum Digital Nasional

Saat ini berbagai sistem hukum digital berkembang secara terpisah, seperti sistem legislasi DPR, SIMPONI di Kementerian Keuangan, atau platform peraturan daerah di Kemendagri. Reformasi JDIHN harus diarahkan

untuk menjadi pusat agregator hukum nasional (national legal integrator) yang menghubungkan seluruh repositori hukum dengan satu format dan satu standar validasi.

Integrasi ini sejalan dengan konsep “single source of truth” dalam sistem informasi, yang menekankan bahwa semua data hukum yang sah harus dapat diverifikasi dari satu sumber utama dalam hal ini adalah JDIHN.⁵⁰

Dari sisi literatur, Lawrence Lessig dalam teori *code as law* menekankan bahwa arsitektur sistem digital menentukan bagaimana norma dijalankan. Oleh karena itu, sistem digital JDIHN harus dirancang tidak hanya sebagai platform penyimpanan, tetapi juga sebagai sistem yang menegakkan validitas, transparansi, dan aksesibilitas hukum.⁵¹

Transformasi regulasi ini juga perlu mengadopsi prinsip adaptive governance, yaitu pendekatan regulasi yang mampu menyesuaikan dengan dinamika teknologi dan risiko baru, sebagaimana dikembangkan oleh Anne-Marie Slaughter dalam teori *_networked governance*.⁵²

f. Rekomendasi Penguatan Keamanan Siber dalam Sistem JDIHN

Sebagai sistem dokumentasi hukum nasional, JDIHN memiliki posisi strategis dalam membangun ekosistem hukum digital yang akuntabel, terbuka, dan adaptif terhadap dinamika teknologi. Untuk menjamin keberlanjutan peran tersebut di tengah meningkatnya ancaman siber, diperlukan langkah-langkah penguatan secara simultan pada aspek regulatif, teknis, dan kelembagaan.

⁴⁹ Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, Pasal 4–5.

⁵⁰ BPHN, Rencana Strategis JDIHN 2020–2024, (Jakarta: BPHN, 2020), hlm. 22–24.

⁵¹ Lawrence Lessig, *Code and Other Laws of Cyberspace*, (New York: Basic Books, 1999), hlm. 39–40.

⁵² Anne-Marie Slaughter, *The Chessboard and the Web: Strategies of Connection in a Networked World*, (New Haven: Yale University Press, 2017), hlm. 89–90.

1) Penyusunan Standar Nasional Pengamanan Dokumen Hukum

Pemerintah, melalui BPHN dan BSSN, perlu menyusun Pedoman Nasional Keamanan Dokumen Hukum Digital, yang mengatur standar minimum pengamanan dokumen hukum, baik dari sisi teknis, prosedural, maupun kelembagaan. Pedoman ini dapat merujuk pada praktik internasional seperti *National Institute of Standards and Technology (NIST) Cybersecurity Framework* atau ISO/IEC 27001.

Pedoman ini harus mencakup:

- a) Prosedur klasifikasi tingkat sensitivitas dokumen hukum;
- b) Sistem autentikasi pengguna berlapis (multi-factor authentication);
- c) Kebijakan backup dan pemulihan data hukum;
- d) Ketentuan pemantauan sistem dan pelaporan insiden;
- e) Penanganan insiden siber dan mitigasi gangguan operasional.

Langkah ini sejalan dengan prinsip keamanan informasi pada Pasal 20–21 PP Nomor 71 Tahun 2019, yang mengatur penyelenggaraan sistem elektronik strategis.⁵³

2) Peningkatan Kapasitas SDM dan Asistensi Teknis Anggota JDIHN

Optimalisasi pengamanan siber tidak mungkin tercapai tanpa pembinaan teknis yang berkelanjutan. BPHN sebagai koordinator JDIHN harus menyediakan modul pelatihan keamanan informasi bagi seluruh pengelola dokumentasi hukum, khususnya di tingkat daerah yang masih menghadapi keterbatasan kapasitas.

Pelatihan ini mencakup pengenalan risiko siber, dasar-dasar keamanan digital, pemanfaatan perangkat lunak legal open source, serta simulasi penanganan insiden (table-top exercise). Asistensi teknis juga perlu diberikan melalui kunjungan langsung atau dukungan daring, terutama pada unit kerja yang berstatus “belum aktif” dalam sistem JDIHN.⁵⁴

3) Pemanfaatan Teknologi untuk Otomatisasi dan Validasi Dokumen

Teknologi seperti blockchain, digital watermarking, dan smart tagging perlu dipertimbangkan untuk meningkatkan keandalan sistem dokumentasi hukum.

- a) *Blockchain* dapat menjaga integritas dan histori revisi dokumen hukum secara transparan;
- b) *Watermarking digital* dapat menandai keaslian dokumen secara visual dan tersembunyi;
- c) *Smart tagging berbasis AI* memungkinkan klasifikasi dan pencarian hukum lebih cerdas.

Di sisi lain, sistem validasi dan verifikasi berbasis kode QR atau token digital dapat diterapkan agar setiap dokumen yang diakses publik dapat dicek langsung ke sumber resmi (single source of truth). Hal ini sejalan dengan pendekatan *regtech* (regulatory technology) yang telah banyak diterapkan di sektor keuangan dan kini mulai diadopsi dalam sistem hukum.⁵⁵

4) Integrasi dan Harmonisasi dengan Infrastruktur Keamanan Nasional

⁵³ Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Pasal 20–21.

⁵⁴ BPHN, Laporan Tahunan Kinerja JDIHN 2023, (Jakarta: BPHN, 2024), hlm. 15.

⁵⁵ Omarova, Saule T., "New Tech v. New Deal: Fintech as a Systemic Phenomenon," *Yale Journal on Regulation* 36, no. 3 (2019): 735–793.

Ke depan, pengamanan JDIHN tidak dapat berjalan sendiri. Perlu ada integrasi sistem peringatan dini dan audit keamanan dengan BSSN serta koordinasi insiden dengan Kementerian Kominfo. JDIHN juga harus terhubung dengan Pusat Operasi Keamanan Siber Nasional agar dapat mendeteksi dan merespons gangguan secara real time.

Revisi regulasi JDIHN dapat memuat ketentuan mengenai mekanisme koordinasi dengan BSSN dan instansi pemangku kepentingan lainnya dalam bidang keamanan siber. Konektivitas ini diperlukan guna memastikan bahwa sistem hukum nasional tidak menjadi titik lemah dalam arsitektur *national cybersecurity* secara keseluruhan.⁵⁶

5) Evaluasi Berkala dan Pengembangan Maturity Model

Sebagai langkah akhir, perlu disusun kerangka maturity model atau indeks ketahanan sistem dokumentasi hukum nasional. Setiap instansi anggota JDIHN dapat dinilai berdasarkan parameter keamanan, keterpaduan sistem, dan ketersediaan data. Evaluasi ini akan memacu peningkatan kualitas layanan dan pengelolaan keamanan informasi secara kompetitif dan berkelanjutan.

D. Penutup

Penguatan fungsi Jaringan Dokumentasi dan Informasi Hukum Nasional (JDIHN) dalam konteks pengamanan siber merupakan kebutuhan mendesak seiring meningkatnya ancaman terhadap integritas, ketersediaan, dan keaslian dokumen hukum di era digital. JDIHN memiliki posisi sentral dalam ekosistem hukum nasional sebagai simpul penyedia informasi

hukum resmi yang mendukung keterbukaan, kepastian hukum, dan pelayanan publik berbasis elektronik. Namun demikian, infrastruktur dan tata kelola JDIHN saat ini belum sepenuhnya dirancang untuk menjawab tantangan transformasi digital dan risiko keamanan siber yang semakin kompleks.

Analisis menunjukkan bahwa kelemahan utama terletak pada belum terintegrasinya standar keamanan informasi dalam sistem pengelolaan dokumen hukum nasional, belum meratanya kapasitas teknis antaranggota JDIHN, serta minimnya dukungan regulatif terhadap isu pengamanan data hukum. Selain itu, dokumen hukum digital belum sepenuhnya diakui dan dilindungi dalam kerangka perlindungan infrastruktur informasi vital negara, meskipun nilainya sangat strategis dalam proses legislasi, penegakan hukum, dan pelayanan publik.

Oleh karena itu, optimalisasi fungsi JDIHN dalam pengamanan siber perlu dilakukan secara menyeluruh melalui revisi Peraturan Presiden Nomor 33 Tahun 2012 yang menegaskan pengelolaan dokumentasi hukum secara digital-native, penerapan standar keamanan internasional (seperti ISO/IEC 27001), dan integrasi sistem JDIHN ke dalam arsitektur Sistem Pemerintahan Berbasis Elektronik (SPBE). Di samping itu, dibutuhkan peningkatan kapasitas sumber daya manusia, asistensi teknis bagi anggota JDIHN, serta kerja sama lintas sektoral, khususnya dengan Badan Siber dan Sandi Negara (BSSN), untuk menjamin perlindungan dokumen hukum sebagai aset informasi strategis nasional.

Reformasi ini penting untuk memastikan bahwa dokumen hukum tidak hanya tersedia dan mudah diakses, tetapi juga terjamin validitas,

⁵⁶ Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber, Pasal 6 dan 10.

integritas, dan keamanannya dari ancaman siber. Dengan demikian, JDIHN dapat benar-benar berfungsi sebagai fondasi digital sistem hukum Indonesia yang modern, terpercaya, dan berdaulat secara informasi.

Penguatan fungsi Jaringan Dokumentasi dan Informasi Hukum Nasional (JDIHN) tidak dapat dilepaskan dari kerangka besar pembangunan Sistem Pemerintahan Berbasis Elektronik (SPBE) dan Sistem Jaringan Dokumentasi dan Informasi Hukum Nasional (SJDIHN). JDIHN harus diposisikan sebagai simpul utama yang menjamin ketersediaan, keterpaduan, dan keautentikan informasi hukum, sekaligus sebagai bagian dari infrastruktur informasi vital yang perlu mendapatkan perlindungan setara dengan sektor lain dalam Strategi Keamanan Siber Nasional.

Analisis dalam tulisan ini menegaskan bahwa tanpa adanya reformasi regulasi, standar teknis keamanan, dan penguatan koordinasi kelembagaan, JDIHN akan sulit menjawab tuntutan era digital dan menghadapi ancaman siber yang semakin kompleks. Optimalisasi fungsi JDIHN harus diarahkan pada tiga hal utama:

1. Aspek regulatif, melalui revisi Perpres 33 Tahun 2012 agar selaras dengan Perpres SPBE, Perpres Satu Data Indonesia, dan Perpres Pelindungan Infrastruktur Informasi Vital;
2. Aspek teknis, dengan penerapan standar keamanan informasi internasional (ISO/IEC 27001) serta integrasi interoperabilitas antar-sistem hukum digital;
3. Aspek kelembagaan, berupa penguatan peran BPHN sebagai pusat JDIHN, pembentukan unit khusus keamanan siber, serta peningkatan koordinasi dengan Badan Siber dan Sandi Negara (BSSN).

Dengan demikian, optimalisasi JDIHN tidak hanya menjawab kebutuhan administratif dalam menyediakan dokumen hukum yang sah dan akurat, tetapi juga menjadi bagian integral dari ketahanan hukum nasional dan infrastruktur keamanan siber Indonesia. Reformasi menyeluruh ini diharapkan mampu memastikan bahwa sistem hukum Indonesia benar-benar modern, adaptif, dan berdaulat di tengah arus transformasi digital global.

DAFTAR PUSTAKA

Buku

- Abdussamad, Zuchri, Metode Penelitian Kualitatif (Makassar: Syakir Media Press, 2021).
- Bakhri, Moch. Syaiful, Pengantar Hukum Keamanan Siber (Jakarta: Prenada Media, 2021).
- Hamzah, Andi, Hukum Siber Indonesia (Jakarta: Sinar Grafika, 2015).
- Khairandy, Ridwan, Hukum Informasi dan Transaksi Elektronik (Yogyakarta: FH UII Press, 2018).
- Lessig, Lawrence, Code and Other Laws of Cyberspace (New York: Basic Books, 1999).
- Mahfud MD, Politik Hukum di Indonesia (Jakarta: Rajawali Pers, 2009).
- Mattord, Herbert J. and Michael E. Whitman, Principles of Information Security, 6th ed. (Boston: Cengage Learning, 2018).
- Moleong, Lexy J., Metodologi Penelitian Kualitatif (Bandung: Remaja Rosdakarya, 2018).
- Rahardjo, Satjipto, Ilmu Hukum (Bandung: Citra Aditya Bakti, 2006).
- Slaughter, Anne-Marie, The Chessboard and the Web: Strategies of Connection in a Networked World (New Haven: Yale University Press, 2017).
- Soekanto, Soerjono dan Sri Mamudji, Penelitian Hukum Normatif: Suatu Tinjauan Singkat (Jakarta: Rajawali Pers, 2012).
- Yusriyadi, Abdul, Hukum dan Teknologi Informasi (Malang: Setara Press, 2020).

Makalah/Artikel/Prosiding/Hasil Penelitian

- Adhiasti, Tryavena Martha dan Yuwanto, "Legal Documentation and Information Network (JDIH) as an Implementation of e-Government System in the Regional Representative Council

of the Republic of Indonesia,” *Jurnal Politik dan Pemerintahan* 15, no. 2 (2024): 145–163.

Alketbi, Ahmed, Qusay H. Mahmoud, dan Mahmoud Nasralla, “Blockchain for Government Services—Use Cases, Security Benefits and Challenges,” 2018 IEEE International Conference on Internet of Things and Intelligence System (IOTAIS).

Anggraeni, Ricca, JDIH dan Tantangan Literasi Digital, *Majalah Hukum Nasional* (Jakarta: BPHN, 2024).

Omarova, Saule T., “New Tech v. New Deal: Fintech as a Systemic Phenomenon,” *Yale Journal on Regulation* 36, no. 3 (2019): 735–793.

Trijono, Rahmat, “Pushing the Improvement of the Indonesian Legal Database for Law Research and Economic Research,” *Indonesian Law Journal* 12 (2019): 75–95

Internet

Badan Siber dan Sandi Negara, “Statistik Ancaman Siber Indonesia Tahun 2022,” <https://bssn.go.id/statistik-2022>

Hukumonline, “Kemenkumham Anugerahkan 57 Anggota JDIHN Terbaik Tahun 2023,” <https://www.hukumonline.com>

Laporan/Literatur Resmi

Badan Pembinaan Hukum Nasional, *Laporan Tahunan JDIHN* (Jakarta: BPHN, 2023).

Badan Pembinaan Hukum Nasional, *Laporan Kinerja Tahunan BPHN 2023* (Jakarta: BPHN, 2024).

Badan Pembinaan Hukum Nasional, *Rencana Strategis JDIHN 2020–2024* (Jakarta: BPHN, 2020).

Badan Siber dan Sandi Negara, *Pedoman Arsitektur Zero Trust untuk Pemerintah Indonesia* (Jakarta: BSSN, 2023).

UN Department of Economic and Social Affairs, Akoma Ntoso: *Open Standards for Legal Documents* (New York: UNDESA, 2018).

Standar Internasional

International Organization for Standardization, *ISO/IEC 27001:2022, Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements* (Geneva: ISO, 2022).

National Institute of Standards and Technology, *Cybersecurity Framework* (Gaithersburg: NIST, 2018).

Peraturan Perundang-undangan

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, diubah dengan Undang-Undang Nomor 19 Tahun 2016.

Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik.

Undang-Undang Nomor 32 Tahun 2004 tentang Pemerintahan Daerah.

Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Peraturan Presiden Nomor 33 Tahun 2012 tentang Jaringan Dokumentasi dan Informasi Hukum Nasional.

Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia.

Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital.

Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.

Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber.

Peraturan Menteri Hukum dan HAM Nomor 2 Tahun 2013 tentang Jaringan Dokumentasi dan Informasi Hukum Nasional.

Wawancara

Wawancara dengan pejabat Badan Pembinaan Hukum Nasional (BPHN), Jakarta, Juli 2025.