

Artikel Penelitian

## Fragmentasi Penegakan Hukum Pelindungan Data Pribadi dan Desain Kelembagaan Otoritas Pelindungan Data Pribadi di Indonesia

*Indrawan Yoswanda Saputra*<sup>\*</sup>, *Paltiada Saragi*, *Andrew Betlehn**Fakultas Hukum, Magister Hukum, Universitas Kristen Indonesia, Jakarta, Indonesia*

### INFORMASI ARTIKEL

Diterima Redaksi: 10 Januari 2026  
Revisi Akhir: 21 Februari 2026  
Diterbitkan *Online*: 27 Februari 2026

### KATA KUNCI

Fragmentasi Kewenangan  
Functional Vacuum of Enforcement  
Huband-Spoke  
Kepastian Hukum  
Otoritas Pelindungan Data Pribadi

### KORESPONDENSI

Phone: +62 878 8886 4656  
E-mail: [yoswanda@gmail.com](mailto:yoswanda@gmail.com)

### A B S T R A K

Kehadiran Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) menandai unifikasi norma substantif pelindungan data di Indonesia. Namun, maraknya insiden kebocoran data siber lintas sektor menunjukkan adanya kesenjangan struktural yang tajam antara kondisi normatif (*das sollen*) dengan implementasi empiris (*das sein*). Artikel ini bertujuan menganalisis bagaimana fragmentasi kewenangan kelembagaan eksisting memicu ketidakterintegrasian penegakan hukum dan merumuskan rekonstruksi desain Otoritas Pelindungan Data Pribadi (OPDP) yang ideal. Dengan metode penelitian yuridis normatif melalui pendekatan perundang-undangan, konseptual, dan perbandingan yurisdiksi European Data Protection Board (EDPB), kajian ini mengidentifikasi terjadinya fenomena *functional vacuum of enforcement* (kevakuman fungsional penegakan hukum). Kondisi ini disebabkan oleh tumpang tindih yurisdiksi sektoral antara Kementerian Komunikasi dan Digital, Badan Siber dan Sandi Negara, Otoritas Jasa Keuangan, dan Kepolisian Negara Republik Indonesia yang bergerak secara parsial tanpa mekanisme interkoneksi formal. Hasil penelitian merekomendasikan rekonstruksi OPDP sebagai Independent Regulatory Agency yang mengadopsi Integrated Network Governance Model berbasis struktur Hub-and-Spoke. Model ini memposisikan OPDP sebagai pusat jaringan komando tertinggi (*hub*) berkewenangan quasi-judicial, yang terintegrasi dengan instansi sektoral sebagai pengawas teknis spesifik (*spokes*). Hubungan kerja ini dikunci dalam instrumen Hukum Administrasi Negara berupa Peraturan Presiden yang mengoperasionalkan tiga pilar utama: parameter prosedural tenggat lapor tunggal 3x24 jam, parameter tingkat keparahan insiden, dan protokol klasifikasi pembagian data (*data sharing*). Rekonstruksi ini terbukti secara teoretis mampu menguatkan prediktabilitas hukum, konsistensi penegakan sanksi, dan mengembalikan kepercayaan publik dalam ekosistem transaksi daring nasional.

### PENDAHULUAN

Transformasi digital telah mendorong perubahan mendasar dalam berbagai sektor kehidupan masyarakat di Indonesia, khususnya dalam aktivitas ekonomi, pelayanan publik, dan transaksi daring. Kecepatan arus pertukaran informasi ini menempatkan data pribadi sebagai komoditas strategis bernilai tinggi di era kapitalisme informasi modern. Namun, akselerasi pemrosesan data pribadi tersebut tidak selalu diikuti dengan kesiapan sistem pelindungan data dan infrastruktur hukum yang memadai. Dalam beberapa tahun terakhir, rangkaian insiden kebocoran data berskala makro—seperti kebocoran data Pusat Data Nasional Sementara (PDNS) tahun 2024, data kepesertaan jaminan kesehatan nasional, hingga data nasabah institusi perbankan—menjadi bukti kerentanan ekosistem siber di Indonesia. Dampak dari kebocoran data tersebut tidak hanya bersifat teknis-digital, melainkan menimbulkan kerugian nyata bagi masyarakat luas, mulai dari eksploitasi kejahatan siber berupa penipuan finansial, pencurian identitas, hingga ancaman runtuhnya kepercayaan publik terhadap keandalan transaksi daring.

Secara normatif, Pemerintah dan Dewan Perwakilan Rakyat telah mengundang Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) sebagai payung hukum komprehensif (unifikasi norma) yang mengatur tata kelola pemrosesan data, hak-hak subjek data, serta sanksi administratif dan pidana. Meskipun UU PDP dibentuk untuk menghadirkan unifikasi hukum, struktur kelembagaan penegakan hukum pelindungan data pribadi di Indonesia saat ini masih terperangkap dalam ego-sektoral yang terfragmentasi. Pasal 58 UU PDP mengamanatkan pembentukan lembaga pengawas pelindungan data pribadi yang ditetapkan oleh Presiden, namun dalam tataran empiris, belum beroperasinya lembaga tersebut secara independen mengakibatkan fungsi pengawasan dan penegakan hukum dijalankan secara parsial oleh berbagai instansi sektoral.

Fragmentasi kewenangan ini melibatkan Kementerian Komunikasi dan Digital (Komdigi) selaku pengawas Penyelenggara Sistem Elektronik (PSE), Badan Siber dan Sandi Negara (BSSN) selaku pengampu keamanan siber dan ketahanan infrastruktur kritis, Otoritas Jasa Keuangan (OJK) yang memegang yurisdiksi perlindungan konsumen di sektor finansial, serta Kepolisian Negara Republik Indonesia (Polri) di ranah penegakan hukum pidana siber. Ketiadaan koordinasi yang terlembaga secara formal di antara lembaga-lembaga ini menciptakan tumpang tindih yurisdiksi (*overlapping jurisdiction*) sekaligus kekosongan penegakan hukum operasional. Akibatnya, ketika terjadi insiden kebocoran data pribadi, masing-masing lembaga bertindak menggunakan instrumen sektoralnya sendiri tanpa adanya sinkronisasi data forensik digital dan standarisasi sanksi yang berkeadilan.

Permasalahan struktural tersebut menunjukkan adanya kesenjangan yang tajam antara kondisi normatif yang diharapkan (*das sollen*) dengan praktik implementasi hukum di lapangan (*das sein*). Dari perspektif sosiologi hukum dan teori penegakan hukum, ketiadaan mekanisme kelembagaan yang terkoordinasi melahirkan kondisi yang disebut sebagai *functional vacuum of enforcement* (kevakuman fungsional penegakan hukum). Kondisi ini merujuk pada situasi di mana undang-undang substantif yang progresif telah tersedia, namun efektivitas implementasinya mandek akibat absennya arsitektur kelembagaan yang solid, integratif, dan otoritatif. Permasalahan inilah yang melandasi urgensi dilakukannya penelitian ini.

Berdasarkan latar belakang tersebut, artikel ini memfokuskan analisisnya pada dua rumusan masalah utama. Pertama, bagaimana fragmentasi kewenangan antar-lembaga memengaruhi integrasi penegakan hukum pelindungan data pribadi di Indonesia? Kedua, bagaimana konstruksi desain kelembagaan Otoritas Pelindungan Data Pribadi yang ideal dalam mendukung integrasi penegakan hukum pelindungan data pribadi demi mewujudkan kepastian hukum transaksi daring? Melalui pembahasan ini, diharapkan dapat dirumuskan sebuah draf solusi kelembagaan yang komprehensif, orisinal, dan preskriptif dalam kerangka hukum administrasi negara Indonesia.

## TINJAUAN PUSTAKA

### *Konsep Pelindungan Data Pribadi dalam Sistem Digital*

Perkembangan teknologi informasi telah menggeser paradigma hak atas privasi. Konsep privasi tradisional yang dirumuskan oleh Warren dan Brandeis sebagai "hak untuk dibiarkan sendiri" (*the right to be let alone*) tidak lagi memadai untuk menjawab tantangan era digital. Daniel J. Solove, Julie E. Cohen, dan Paul De Hert mengembangkan konsep pelindungan data pribadi sebagai hak aktif atas kendali informasi atau hak penentuan nasib sendiri secara informasional (*informational self-determination*). Dalam ekosistem digital yang digerakkan oleh mahadata (*big data*) dan kecerdasan buatan, data pribadi bukan sekadar identitas melekat, melainkan aset ekonomi digital yang rentan dieksploitasi oleh pengendali data (*data controller*) maupun pemroses data (*data processor*). Oleh karena itu, pelindungan data pribadi harus dikonstruksikan sebagai instrumen hukum yang memberikan kontrol penuh kepada subjek data untuk menentukan bagaimana informasinya dikumpulkan, diproses, disebarkan, dan dihapus, guna menjamin harkat dan martabat manusia dalam ruang siber.

### *Teori Penegakan Hukum dan Efektivitas Regulasi*

Analisis terhadap ketidakefektifan penegakan hukum pelindungan data pribadi memerlukan pisau analisis Teori Penegakan Hukum yang dirumuskan oleh Soerjono Soekanto. Menurut Soekanto, efektivitas penegakan hukum dipengaruhi secara simultan oleh lima faktor, yaitu: (1) faktor undang-undang/norma, (2) faktor aparat penegak hukum/kelembagaan, (3) faktor sarana dan fasilitas, (4) faktor masyarakat, dan (5) faktor kebudayaan. Ditinjau dari teori ini, problem utama pelindungan data pribadi di Indonesia berpusat pada faktor aparat dan struktur kelembagaan, bukan pada kelangkaan norma substantif. Sejalan dengan hal tersebut, Satjipto Rahardjo menekankan konsep *law in action* yang menyatakan bahwa hukum tidak boleh dipandang sebatas teks tertulis (*law in books*), melainkan bagaimana hukum tersebut dioperasionalkan oleh institusi penegak hukum dalam merespons

realitas sosial. Ketiadaan institusi pengawas yang terintegrasi menurunkan apa yang disebut Baldwin, Cave, dan Lodge sebagai enforcement capacity, yaitu kapasitas kelembagaan untuk melakukan investigasi forensik digital, memonitor kepatuhan, dan menegakkan sanksi secara kredibel guna memaksa kepatuhan pelaku industri.

### ***Teori Kepastian Hukum dan Nilai Dasar Hukum***

Kepastian hukum merupakan pilar utama dalam penyelenggaraan negara hukum dan aktivitas ekonomi digital. Hans Kelsen melalui Teori Hukum Murni (Pure Theory of Law) dan hierarki norma (Stufenbaulehre) menegaskan bahwa setiap tindakan organ negara harus bersumber pada pelimpahan kewenangan yang sah (legalitas kewenangan) dari norma hukum yang lebih tinggi. Kepastian hukum menghendaki konsistensi, kejelasan prosedur, dan tidak adanya kontradiksi internal dalam sistem hukum positif. Sementara itu, Gustav Radbruch menyatakan adanya tiga nilai dasar hukum yang saling melengkapi namun kerap berbenturan, yaitu keadilan (*gerechtigkeits*), kemanfaatan (*zweckmassigkeit*), dan kepastian hukum (*rechtssicherheit*). Dalam konteks transaksi daring, kepastian hukum mewujudkan dalam bentuk prediktabilitas penerapan hukum (*legal predictability*), di mana pelaku usaha memiliki kepastian mengenai kewajiban hukumnya dan subjek data memiliki jaminan perlindungan yang setara tanpa dibayangi oleh ketidakpastian yurisdiksi lembaga pengawas.

### ***Konsep Fragmentasi Kelembagaan dan Independent Regulatory Agency (IRA)***

Fenomena tumpang tindih kewenangan lintas sektoral dipelajari melalui konsep *decentered regulation* oleh Julia Black dan *post-regulatory state* oleh Colin Scott. Black menjelaskan bahwa regulasi di era modern tidak lagi bersifat sentralistik-hierarkis (berpusat pada satu lembaga negara saja), melainkan terdesentralisasi, polisentris, dan melibatkan jaringan tata kelola yang kompleks (*governance network*). Ketika jaringan ini gagal dikoordinasikan secara formal, maka akan terjadi kegagalan koordinasi (*coordination failure*) dan benturan yurisdiksi. Guna mengatasi hal ini, Giandomenico Majone dan Mark Thatcher menawarkan doktrin Independent Regulatory Agency (IRA). Doktrin ini menyatakan bahwa fungsi pengawasan terhadap sektor teknis yang dinamis dan berisiko tinggi seperti ranah siber harus diserahkan kepada lembaga regulatori independen yang memiliki kemandirian fungsional dari intervensi politik dan birokrasi, namun tetap akuntabel dalam koridor hukum administrasi negara.

## **METODOLOGI**

Penelitian ini menggunakan metode penelitian hukum yuridis normatif, yang menempatkan hukum sebagai sebuah sistem norma tertutup yang terdiri atas asas-asas, kaidah-kaidah, doktrin, dan peraturan perundangundangan. Isu hukum yang diteliti difokuskan pada problem ketidaksinkronan struktur hukum administrasi siber dalam penegakan hukum perlindungan data pribadi di Indonesia. Guna memecahkan isu hukum tersebut, digunakan tiga pendekatan utama: (1) Pendekatan perundang-undangan (*statute approach*), yang diterapkan dengan menelaah UU PDP (UU No. 27/2022), UU ITE (UU No. 11/2008 jo. UU No. 1/2024), UU OJK (UU No. 21/2011), UU P2SK (UU No. 4/2023), serta PP No. 71/2019; (2) Pendekatan konseptual (*conceptual approach*), yang merujuk pada doktrin-doktrin hukum administrasi negara, teori penegakan hukum, serta konsep *functional vacuum of enforcement*; dan (3) Pendekatan perbandingan (*comparative approach*), yang dilakukan dengan mengkaji kerangka kelembagaan European Data Protection Board (EDPB) di Uni Eropa untuk diambil saripati konseptualnya (*lessons learned*) yang relevan.

Sumber data yang dipergunakan sepenuhnya berupa data sekunder yang diklasifikasikan ke dalam tiga jenis bahan hukum. Bahan hukum primer meliputi instrumen regulasi nasional dan traktat internasional terkait. Bahan hukum sekunder terdiri atas buku literatur hukum teks, jurnal ilmiah bereputasi, tesis, serta pandangan doktrinal para yuris. Bahan hukum tersier mencakup kamus hukum dan ensiklopedia penunjang. Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*) berbasis penelusuran dokumentasi digital dan fisik secara selektif dan sistematis. Selanjutnya, teknik analisis data dilakukan secara kualitatif yuridis dengan metode penafsiran hukum (*penafsiran sistematis dan teleologis*).

Tahapan yang dilalui dalam penelitian, pembangunan konsep, atau penyelesaian kasus, dituliskan pada bagian metodologi. serta analisis preskriptif, guna merumuskan argumentasi hukum yang kokoh dan konklusif dalam menjawab kedua rumusan masalah penelitian.

## HASIL DAN PEMBAHASAN

### *Fragmentasi Kewenangan dan Implikasinya: Refleksi Fenomena Functional Vacuum of Enforcement*

Pengesahan UU PDP pada tahun 2022 semula digadang-gadang sebagai tonggak sejarah baru yang akan menghadirkan kepastian hukum dalam perlindungan privasi warga negara. Namun, analisis mendalam terhadap struktur penegakan hukum digital di Indonesia saat ini menunjukkan adanya realitas yang kontradiktif. Penegakan hukum perlindungan data pribadi mengalami ketidakterintegrasian kronis akibat struktur pengawasan yang terfragmentasi ke dalam berbagai sektor hukum eksisting (fragmented supervision). Masing-masing lembaga pengawas siber bergerak secara partial berdasarkan mandat undang-undang sektoralnya sendiri, tanpa adanya jembatan interkoneksi operasional yang mengikat secara hukum.

Kementerian Komunikasi dan Digital (Komdigi) memiliki kewenangan administratif yang luas berdasarkan PP No. 71/2019 tentang PSTE dan UU ITE untuk melakukan pengawasan terhadap Penyelenggara Sistem Elektronik (PSE), termasuk menjatuhkan sanksi administratif berupa pemutusan akses (blokir) atau denda. Namun, dalam menghadapi insiden kebocoran data yang masif, Komdigi kerap terhambat oleh keterbatasan kapasitas investigasi siber forensik yang mendalam, serta tidak memiliki taji regulatori yang kuat ketika berhadapan dengan pelanggaran yang dilakukan oleh badan publik atau instansi pemerintah sendiri. Di sisi lain, Badan Siber dan Sandi Negara (BSSN) berdasarkan Perpres No. 53/2017 bertindak sebagai pengampu keamanan siber nasional dan ketahanan infrastruktur kritis. BSSN memiliki instrumen teknis penanganan insiden siber (seperti CSIRT) dan kapabilitas melakukan forensik digital pascakebocoran, namun BSSN sama sekali tidak dibekali kewenangan yustisial untuk menjatuhkan sanksi administratif, denda siber, maupun melakukan penegakan hukum koersif terhadap pengendali data yang lalai.

Kondisi ini semakin diperumit di sektor industri jasa keuangan. Otoritas Jasa Keuangan (OJK) memiliki kewenangan absolut berdasarkan UU OJK dan UU P2SK, yang diturunkan ke dalam POJK No. 6/ POJK.07/2022, untuk menyelenggarakan pengawasan kepatuhan perilaku pelaku usaha jasa keuangan, termasuk dalam hal perlindungan data konsumen perbankan dan teknologi finansial (fintech). Ketika terjadi kebocoran data nasabah di perbankan digital yang terhubung dengan ekosistem e-commerce, benturan kewenangan (overlapping jurisdiction) tidak terhindarkan. OJK melakukan investigasi dari sudut pandang prudensial dan perlindungan konsumen keuangan, Komdigi bergerak memeriksa kepatuhan sistem elektronik PSE, BSSN mendeteksi anomali siber infrastruktur, sedangkan Direktorat Tindak Pidana Siber Kepolisian Negara Republik Indonesia (Polri) melakukan penyelidikan hilir untuk mencari delik pidana siber. Ketiadaan interkoneksi formal di antara keempat lembaga ini melahirkan coordination gap yang melumpuhkan efektivitas hukum.

Fenomena tidak terintegrasinya penegakan hukum ini secara akademis memicu terjadinya functional vacuum of enforcement (kevakuman fungsional penegakan hukum). Aturan substantif dalam UU PDP sangat progresif dan memuat ancaman sanksi denda administratif yang tinggi (mencapai 2% dari pendapatan tahunan terhadap pengendali data swasta), namun mesin penegakan hukumnya mandek berputar. Kondisi ini membawa tiga dampak destruktif bagi ekosistem hukum digital nasional. Pertama, terjadinya enforcement inconsistency (inkonsistensi penegakan hukum), di mana standardisasi parameter pemenuhan kepatuhan dan pengenaan sanksi berbeda-beda antar-sektor. Kedua, timbulnya ketidakpastian hukum bagi pelaku usaha (PSE) yang dibebani kewajiban pelaporan ganda (multi-reporting burden) dengan format dan batas waktu yang saling bertentangan. Ketiga, melorotnya kepercayaan publik (public trust) terhadap keamanan transaksi daring, karena negara terkesan absen dan gagap dalam mengeksekusi keadilan ketika hak fundamental atas data pribadi warga negara dilanggar secara berulang tanpa ada kejelasan pertanggungjawaban hukum yang tuntas.

Aspek Perbandingan	Penelitian Terdahulu (HTN / Sektoral)	Kondisi Eksisting (Pasca UU PDP)	Penelitian Tesis ini (Novelty)
<b>Fokus Kajian</b>	Urgensi pembentukan lembaga independen perspektif tata negara (Mahardika) atau perlindungan sektor perbankan (Ervian).	Lembaga pengawas Pasal 58 belum operasional; lembaga eksisting (Komdigi, BSSN, OJK) berjalan parsial.	Analisis hubungan kausalitas fragmentasi kelembagaan terhadap kegagalan fungsi penegakan hukum secara operasional.
<b>Pendekatan Teoretis</b>	Menyoroti ketiadaan lembaga sebagai bentuk <i>rechtsvacuum</i> tradisional.	Norma hukum substantif tersedia (UU PDP), namun roda penegakan hukum di lapangan mandek.	Mengembangkan pendekatan konseptual baru melalui pisau analisis <i>functional vacuum of enforcement</i> .
<b>Model Solusi</b>	Menawarkan pembentukan lembaga baru yang terisolasi tanpa meredefinisikan hubungan antar-instansi.	Koordinasi ad-hoc dan saling menunggu antar-lembaga saat insiden kebocoran siber terjadi.	Merumuskan <i>Integrated Network Governance Model</i> berstruktur <i>Hub-and-Spoke</i> terikat hukum administrasi.

### ***Rekonstruksi Desain Kelembagaan OPDP: Penerapan Integrated Network Governance Model Berstruktur Hub-and-Spoke***

Guna menyembuhkan fenomena *functional vacuum of enforcement* dan menghentikan tumpang tindih yurisdiksi lintas sektor, diperlukan rekonstruksi fundamental terhadap arsitektur hukum administrasi siber nasional. Otoritas Pelindungan Data Pribadi (OPDP) yang diamanatkan oleh Pasal 58 UU PDP harus dikonstruksikan sebagai sebuah Independent Regulatory Agency (IRA). Lembaga ini wajib diletakkan langsung bertanggung jawab kepada Presiden demi menjamin legitimasi politik tertinggi, namun memiliki kemandirian fungsional (*functional independence*) yang mutlak dari pengaruh dan intervensi birokrasi kementerian sektoral maupun kepentingan pelaku industri pasar digital.

Melalui pendekatan perbandingan hukum (*comparative approach*), Indonesia dapat mengambil pelajaran berharga (*lessons learned*) dari keberhasilan Uni Eropa dalam mengelola pengawasan data lintas negara melalui European Data Protection Board (EDPB) berdasarkan General Data Protection Regulation (GDPR). EDPB menerapkan mekanisme tata kelola satu pintu yang dikenal sebagai *One-Stop-Shop* (OSS) dan mekanisme konsistensi (*consistency mechanism*). Di bawah mekanisme ini, terdapat pembagian peran yang tegas antara *Lead Supervisory Authority* (LSA)—otoritas utama di negara tempat pengendali data berdomisili—dengan *Concerned Supervisory Authorities* (CSA) selaku otoritas penunjang di negara tempat subjek data terdampak berada. Jika terjadi sengketa interpretasi hukum atau penegakan sanksi, EDPB bertindak sebagai dewan tertinggi yang mengeluarkan keputusan final yang mengikat (*binding decision*) demi menjamin konsistensi penerapan hukum di seluruh wilayah Uni Eropa.

Dalam merancang desain OPDP di Indonesia, penelitian ini menolak pendekatan penjiplakan mentah tanpa filter (*non-transplant approach*), mengingat perbedaan mendasar pada sistem ketatanegaraan. Penulis menawarkan metode adaptasi kontekstual (*contextual adaptation*) yang dituangkan ke dalam bentuk *Integrated Network Governance Model dengan Struktur Hub-and-Spoke*. Desain ini tidak membubarkan atau mengebiri kewenangan teknis lembaga pengawas sektoral eksisting yang telah memiliki keahlian dan infrastruktur matang, melainkan merajutnya ke dalam satu jaringan tata kelola yang terintegrasi di bawah satu pusat komando tunggal.

Dalam model ini, OPDP diposisikan sebagai HUB (Pusat Komando Tertinggi). OPDP memegang monopoli penuh terhadap kewenangan regulatori makro dan fungsi *quasi-judicial*. Kewenangan *quasi-judicial* ini mencakup

otoritas tunggal untuk memutus sengketa perlindungan data pribadi, menetapkan status terjadinya pelanggaran hukum, serta mengeksekusi sanksi administratif dan denda siber. Sebaliknya, *lembaga-lembaga eksisting (Komdigi, BSSN, OJK, dan Polri) diposisikan sebagai SPOKES (Jari-jari Jaringan Pengawas Teknis)*. Mereka bertindak sebagai perpanjangan tangan logis dan unit pelaksana teknis spesifik di bawah supervisi koordinatif dari OPDP selaku *hub*. Melalui integrasi ini, koordinasi tidak lagi bersifat sukarela atau ad-hoc, melainkan menjadi kewajiban struktural yang digerakkan oleh sistem hukum administrasi yang solid.

### ***Parameter Interkoneksi Hubungan Kerja Terintegrasi dan Pengujian Efektivitas Kepastian Hukum***

Agar struktur Hub-and-Spoke tidak jatuh menjadi macan kertas birokrasi, hubungan tata kerja koordinatif ini harus dikunci dan dioperasionalkan melalui instrumen Hukum Administrasi Negara yang memaksa dan mengikat, yaitu melalui *Peraturan Presiden tentang Tata Kerja Otoritas Pelindungan Data Pribadi* atau melalui penetapan *Surat Keputusan Bersama (SKB) tentang Single Window Enforcement Protocol dalam Penegakan Hukum Siber*. Mekanisme kerja operasional interkoneksi di dalam jaringan ini digerakkan melalui tiga pilar parameter strategis:

1. Parameter Prosedural (Tenggat Waktu Pelaporan Tunggal): Menyeragamkan aturan main pelaporan insiden. Seluruh pengendali data (baik korporasi swasta, platform e-commerce, maupun badan publik pemerintah) wajib melaporkan setiap adanya dugaan kegagalan perlindungan data pribadi secara satu pintu melalui *Single Window System* yang dikelola langsung oleh OPDP. Tenggat waktu pelaporan ditetapkan secara tegas maksimal 3 x 24 jam ( $T \leq 72$  jam) sejak insiden diketahui. Parameter ini menghapus dualisme prosedur pelaporan sektoral yang membingungkan pelaku usaha.
2. Parameter Tingkat Keparahan Insiden (Incident Severity Parameters): Membangun sistem eskalasi penanganan otomatis berbasis matriks risiko siber. Insiden diklasifikasikan ke dalam tiga tingkatan dampak, yaitu: (a) *Dampak Rendah*, jika kebocoran hanya melibatkan data umum non-sensitif dengan volume subjek data kecil; (b) *Dampak Sedang*, jika melibatkan kebocoran data umum skala besar; dan (c) *Dampak Tinggi*, jika insiden melibatkan kebocoran data pribadi spesifik/sensitif (data kesehatan, biometrik, keuangan, data anak) atau menyangkut Infrastruktur Informasi Kritis Nasional. Tingkat keparahan ini otomatis menentukan bauran dan aktivasi tim gabungan penanganan antara OPDP dengan *spokes* terkait.
3. Parameter Klasifikasi Pembagian Data (Data Sharing Protokol): Menstandardisasi protokol pertukaran informasi teknis dan intelijen siber. BSSN diwajibkan secara hukum untuk menyalurkan berkas *log file* forensik digital makro dan hasil analisis *root cause* insiden kepada OPDP secara rahasia dan aman (interkoneksi tersenkripsi). Data ini menjadi dasar bagi OPDP untuk menjalankan kewenangan *quasijudicial*-nya dalam menetapkan derajat kelalaian pengendali data dan menghitung proporsionalitas denda siber yang akan dijatuhkan.

Guna membuktikan validitas model solusi yang ditawarkan, dilakukan pengujian efektivitas kelembagaan melalui tiga indikator utama nilai dasar kepastian hukum siber modern. Indikator pertama adalah Prediktabilitas Hukum (Legal Predictability). Model *Hub-and-Spoke* memberikan jaminan kepastian bagi pelaku industri transaksi daring dalam memetakan kepatuhan hukumnya karena standar kepatuhan diunifikasi oleh OPDP, sehingga menghapus risiko pengenaan sanksi ganda (*double jeopardy*) dari kementerian yang berbeda. Indikator kedua adalah Konsistensi Penegakan Hukum (Enforcement Consistency). Putusan sanksi administratif dan denda siber dijatuhkan dengan parameter yang objektif, transparan, dan setara, baik terhadap korporasi multinasional, tekfin lokal, maupun instansi pemerintah penentu kebijakan. Indikator ketiga adalah Kepercayaan Publik (Public Trust). Integrasi pengawasan yang responsif dan berwibawa memastikan hak-hak konstitusional subjek data dilindungi secara nyata, yang pada gilirannya akan menumbuhkan iklim investasi yang sehat dan memperkokoh fondasi ekonomi digital nasional secara berkelanjutan.

## KESIMPULAN DAN SARAN

### *Kesimpulan*

Berdasarkan seluruh analisis mendalam dan kajian teoretis-komparatif yang telah dipaparkan pada bab-bab sebelumnya, penelitian ini menarik kesimpulan linier sebagai berikut:

Fragmentasi kewenangan antar-lembaga sektoral di Indonesia (Komdigi, BSSN, OJK, dan Polri) secara kausalitas terbukti melahirkan fenomena *functional vacuum of enforcement* (kevakuman fungsional penegakan hukum). Kehadiran UU PDP sebagai unifikasi norma substantif tidak diimbangi dengan integrasi aparatur penegak hukum operasional, sehingga menimbulkan *coordination gap*, tumpang tindih yurisdiksi dan ketidakkonsistenan penegakan yang merugikan kepastian hukum subjek data maupun pelaku transaksi digital.

Konstruksi desain kelembagaan Otoritas Pelindungan Data Pribadi (OPDP) yang paling ideal Adalah pembentukan Independent Regulatory Agency (IRA) yang diletakkan langsung di bawah koordinasi Presiden dengan menerapkan Integrated Network Governance Model berstruktur Hub-and-Spoke. Model inimemposisikan OPDP sebagai pusat jaringan komando tertinggi (hub) berkewenangan quasi-judicial tunggal, dengan mengoptimalkan peran instansi sektoral eksisting sebagai jari-jari jaringan teknis spesifik (spokes). Struktur ini menjamin tiga nilai dasar hukum, yakni prediktabilitas hukum, konsistensi penegakan sanksi siber, and pemulihan kepercayaan publik.

### *Saran*

Sebagai rekomendasi preskriptif dan aplikatif demi memperkuat tata kelola siber administrasi negara, penulis merumuskan saran-saran berikut:

1. Kepada Presiden Republik Indonesia: Disarankan untuk segera menggunakan mandat regulative Pasal 58 UU PDP untuk mempercepat penerbitan Peraturan Presiden tentang Organisasi dan Tata Kerja OPDP, dengan mengunci kemandirian fungsional otoritas secara absolut dari segala intervensi birokrasi maupun pasar digital korporasi swasta.
2. Kepada Jajaran Regulator Siber Nasional: Disarankan untuk segera menyusun draf Surat Keputusan Bersama (SKB) tentang Single Window Enforcement Protocol guna mengoperasionalkan tiga pilar parameter strategis interkoneksi: penyeragaman tenggat lapor wajib insiden maksimal *3 x 24 jam*, standardisasi parameter tingkat keparahan insiden siber, serta pembentukan protokol pertukaran intelijen log file forensik (data sharing) antara BSSN dan OPDP.
3. Kepada DPR dan Pemerintah: Disarankan untuk melakukan harmonisasi dan unifikasi hukum jangka panjang atas seluruh undang-undang digital sektoral (seperti UU ITE, UU OJK, dan UU P2SK) menggunakan metode Omnibus Law di masa mendatang guna mengeliminasi dualisme prosedur penegakan sanksi serta memperkokoh kedaulatan yurisdiksi digital nasional.

## DAFTAR PUSTAKA

- Asshiddiqie, Jimly. *Perkembangan dan Konsolidasi Lembaga Negara Pasca Reformasi*. Cetakan revisi 2016. Jakarta: Sinar Grafika, 2016.
- Baldwin, Robert, Martin Cave, and Martin Lodge. *Understanding Regulation: Theory, Strategy, and Practice*. 2nd ed. Oxford: Oxford University Press, 2012.
- Black, Julia. "Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'PostRegulatory' World." *Current Legal Problems* 54, no. 1 (2001): 103–146.
- Carey, David J. *Data Protection: A Practical Guide to UK and EU Law*. Oxford: Oxford University Press, 2018
- Cohen, Julie E. *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford: Oxford University Press, 2019.
- De Hert, Paul, and Vagelis Papakonstantinou. "Data Protection Authorities in the EU: The Power of Coordination and the Limits of Harmonisation." *Common Market Law Review* 55, no. 5 (2018): 1423– 1452.
- Hans Kelsen. *Teori Hukum Murni: Dasar-Dasar Ilmu Hukum Normatif*. Diterjemahkan oleh Raisul Muttaqien. Cetakan ke-9. Bandung: PT Citra Aditya Bakti, 2019
- Lobel, Orly. "The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought." *Minnesota Law Review* 89 (2004): 342–470.
- Majone, Giandomenico. *Regulating Europe*. London: Routledge, 2016.
- Marzuki, Peter Mahmud. *Penelitian Hukum: Edisi Revisi*. Jakarta: Prenadamedia Group, 2017.

- Mochtar, Zainal Arifin. *Lembaga Negara Independen: Dinamika Perkembangan dan Urgensi Penataannya Kembali Pasca-Amandemen*. Jakarta: Rajawali Pers, 2021.
- Radbruch, Gustav. *Legal Philosophy and Legal Theory*. Reprint ed. Cambridge: Harvard University Press, 2021.
- Rahardjo, Satjipto. *Masalah Penegakan Hukum: Suatu Tinjauan Sosiologis*. Bandung: Sinar Baru, 2018.
- Scott, Colin. "Regulation in the Age of Governance: The Rise of the Post-Regulatory State." In *The Politics of Regulation*, edited by Jacint Jordana and David Levi-Faur, 145–174. Cheltenham: Edward Elgar Publishing, 2004.
- Soekanto, Soerjono. *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*. Jakarta: Rajawali Pers, 2023.
- Solove, Daniel J. *Understanding Privacy*. Cambridge, MA: Harvard University Press, 2008.
- Thatcher, Mark, and Aleksandrs Cepilovs. "The Independence of Regulatory Agencies: Concept and Measurement." *Journal of European Public Policy* 23, no. 6 (2016): 790–805
- van Dijck, José, Thomas Poell, and Martijn de Waal. *The Platform Society: Public Values in a Connective World*. Oxford: Oxford University Press, 2018.