

Penalaran Argumentasi Hukum Terhadap Pengaturan Identitas Digital Sebagai Instrumen Perlindungan Hak Privasi Masyarakat Indonesia

Siti Nengsih Lestari, S.AP*¹, Dr. C. Aturkian Laia, S.H., M.H., CFHA., CHA., CEFT.*²

¹Tambusai Fakultas Hukum, Universitas Dirgantara Marsekal Suryadarma

e-mail: Nengsihlstr@gmail.com

Published: September, 2026

ABSTRAK

Transformasi digital yang masif telah menggeser paradigma identitas fisik menuju ekosistem identitas digital terintegrasi. Di satu sisi, identitas digital menawarkan efisiensi layanan publik dan komersial, namun di sisi lain memicu kerentanan eksponensial terhadap pelanggaran hak privasi dan kebocoran data pribadi warga negara. Penelitian ini bertujuan untuk menganalisis secara mendalam argumentasi hukum terhadap urgensi pengaturan identitas digital sebagai instrumen pelindung privasi masyarakat berdasarkan kerangka hukum positif di Indonesia, khususnya pasca berlakunya Undang-Undang Perlindungan Data Pribadi (UU PDP). Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan dan konseptual. Hasil penelitian menunjukkan bahwa eksistensi identitas digital tanpa regulasi yang rigid berpotensi mendistorsi hak konstitusional warga negara atas perlindungan diri pribadi yang dijamin oleh Pasal 28G ayat (1) UUD 1945. Argumentasi hukum kedudukan identitas digital harus diletakkan sebagai perluasan dari hak atas privasi (*right to privacy*) yang wajib dilindungi melalui mekanisme enkripsi, kedaulatan data (*data sovereignty*), dan pembatasan akses otoritas. Penataan identitas digital yang berdaulat secara hukum menjadi prasyarat mutlak guna mewujudkan keamanan siber serta keadilan digital di Indonesia.

Kata kunci: *Argumentasi Hukum, Identitas Digital, Hak Privasi, Data Pribadi.*

ABSTRACT

The massive digital transformation has shifted the paradigm of physical identity toward an integrated digital identity ecosystem. On one hand, digital identity offers efficiency in public and commercial services, but on the other hand, it triggers exponential vulnerabilities to privacy breaches and personal data leaks. This study aims to analyze in depth the legal arguments regarding the urgency of regulating digital identity as a protective instrument for public privacy based on the positive law framework in Indonesia, particularly following the enactment of the Personal Data Protection Act (UU PDP). The research method applied is normative juridical with statutory and conceptual approaches. The results demonstrate that the existence of digital identity without rigid regulations potentially distorts citizens' constitutional rights to personal protection guaranteed by Article 28G Paragraph (1) of the 1945 Constitution. The legal reasoning for the status of digital identity must be positioned as an extension of the right to privacy, which must be protected through encryption mechanisms, data sovereignty, and restricted authority access. The legally sovereign arrangement of digital identity is an absolute prerequisite to achieving cyber security and digital justice in Indonesia.

Keywords : *Legal Reasoning, Digital Identity, Right to Privacy, Personal Data.*

© The Author(s). 2021 Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0>

PENDAHULUAN

Perkembangan lanskap teknologi informasi dan komunikasi di era kontemporer tidak hanya mengubah fundamental sistem komunikasi manusia, melainkan juga telah merekonstruksi ulang konsep paling mendasar dari eksistensi kemanusiaan, yaitu identitas diri (*identity*). Integrasi teknologi telematika yang begitu intensif ke dalam struktur sosial telah memaksa pranata hukum untuk melihat kembali batas-batas subjek hukum di ruang siber. Konsekuensinya, identitas bukan lagi sekadar tanda pengenalan biologis yang pasif, melainkan sebuah entitas dinamis yang merepresentasikan kedaulatan individu di dunia virtual¹. Pada era pra-digital, identitas seseorang melekat secara rigid dan inheren pada dokumen fisik kedinasan yang diterbitkan secara eksklusif oleh otoritas

¹ Ramli, Ahmad M. *Cyber Law dan Transformasi Digital*. Bandung: Alumni, 2021.

negara, seperti Kartu Tanda Penduduk, paspor, atau akta kelahiran yang sifatnya statis, lokal, analog, dan terikat kuat pada ruang fisik empiris. Namun, seiring dengan akselerasi gelombang transformasi digital global yang memicu lahirnya ruang siber (*cyberspace*), identitas fisik tersebut kini telah mengalami metamorfosis radikal menjadi apa yang disebut sebagai identitas digital (*digital identity*). Perubahan medium ini menuntut adanya pembaharuan hukum (*legal reform*) karena instrumen hukum konvensional terbukti gagap dalam menjangkau karakteristik data digital yang bersifat *borderless* dan *cair*².

Identitas digital pada masa kini bukan lagi sekadar representasi elektronik atau salinan digital dari data demografi konvensional masa lalu, melainkan akumulasi sistematis, dinamis, dan masif dari seluruh rekam jejak digital, data biometrik yang mencakup sidik jari serta pemindai retina, kredensial autentikasi komputer, kode kriptografi, hingga pola perilaku komputasi pengguna yang terintegrasi secara tak terputus di dalam jaringan internet global. Transformasi ini menimbulkan disrupsi pembuktian hukum, di mana otentisitas dokumen elektronik dan data log komputasi kini memegang peran krusial dalam menentukan validitas perbuatan hukum keperdataan maupun pertanggungjawaban pidana di ruang siber³. Dalam ekosistem masyarakat modern yang berbasis pada data, identitas digital telah beralih peran menjadi instrumen kunci, gerbang utama, dan prasyarat mutlak bagi warga negara untuk dapat mengakses dan mengaktualisasikan hak-hak konstitusionalnya, mulai dari hak atas pelayanan publik, jaminan sosial kesehatan, transaksi finansial perbankan, hingga hak berekspresi secara digital di ruang siber.

Namun demikian, peralihan masif dari identitas fisik menuju ekosistem identitas digital ini laksana pisau bermata dua yang menghadirkan paradoks hukum serta dogmatis yang sangat serius di Indonesia. Penegakan hukum siber di Indonesia sering kali terjebak dalam dilema antara kepastian hukum formil dan perlindungan nilai kemanusiaan material, di mana hukum dituntut adaptif namun di sisi lain sering kali dijadikan alat represi oleh pihak yang dominan⁴. Di satu sisi, adopsi sistem identitas digital nasional yang terintegrasi menjanjikan efisiensi birokrasi yang memangkas waktu pelayanan, interoperabilitas data antarinstansi seketika, serta percepatan pertumbuhan ekonomi digital nasional secara masif melalui kemudahan transaksi ekonomi siber. Di sisi lain, pemrosesan data identitas digital yang bersifat otomatis, terpusat, berskala raksasa, dan tanpa henti mengimplikasikan adanya ancaman yang sangat fatal, destruktif, permanen, dan asimetris terhadap hak privasi (*right to privacy*) yang dimiliki oleh masyarakat luas. Ketika yurisdiksi penegakan hukum pidana siber berbenturan dengan batas-batas teritorial negara, maka perlindungan terhadap subjek data lokal menjadi sangat rentan akibat lemahnya pengawasan lintas batas terhadap para pelaku kejahatan kerah putih digital (*cybercriminology*)⁵.

Realitas empiris di Indonesia menunjukkan bahwa ruang siber nasional terus-menerus diguncang oleh rentetan skandal kebocoran data pribadi skala masif (*data breach*), baik yang melanda peladen inti milik institusi pemerintah, lembaga penyelenggara pemilu, lembaga penjamin sosial kesehatan, maupun korporasi komersial swasta. Data biometrik, Nomor Induk Kependudukan (NIK), alamat surat elektronik, nomor telepon seluler, hingga catatan finansial warga negara yang seharusnya dilindungi dengan sistem keamanan tingkat tinggi dan enkripsi berlapis justru berkali-kali bocor dan diperjualbelikan secara bebas di pasar gelap siber (*dark web*) tanpa adanya sanksi hukum yang menjerakan bagi pihak pengelola data. Kerentanan sistemik ini semakin diperparah oleh kemunculan teknologi kecerdasan buatan (*Artificial Intelligence*) yang memiliki kemampuan luar biasa dalam mengeksploitasi data identitas digital untuk tindakan kejahatan siber tingkat lanjut yang sangat manipulatif. Kehadiran algoritma tingkat tinggi ini tidak hanya mendisrupsi sektor ekonomi, melainkan juga melahirkan tantangan doktrinal baru dalam hukum pidana materiil, khususnya terkait atribusi pertanggungjawaban pidana (*criminal liability*) ketika AI digunakan untuk memanipulasi identitas secara otonom⁶.

Data identitas yang bocor dapat dimanfaatkan untuk melakukan manipulasi profil sosial, pemalsuan identitas (*identity theft*) dalam skala masif untuk pembobolan akun keuangan, serta rekayasa sosial (*social engineering*) yang menghancurkan integritas sosial, reputasi digital, dan kondisi psikologis korban seketika. Dari perspektif dogmatika hukum pidana dan tata negara, ancaman terhadap identitas digital pada hakikatnya merupakan bentuk represi dan pelanggaran nyata terhadap hak asasi manusia yang paling fundamental, yakni hak atas privasi. Ketiadaan batasan yuridis yang jelas mengenai sejauh mana negara atau korporasi dapat memprofilkan individu berpotensi menciptakan ketidakpastian hukum yang merusak tatanan keadilan sosial bagi seluruh rakyat

² Soponyono, Eko. "Tantangan Hukum Pidana dalam Menghadapi Teknologi Artificial Intelligence." *Jurnal Masalah-Masalah Hukum* 50, no. 2 (2021): 112-120.

³ Sitompul, Josua. "Analisis Yuridis Dokumen Elektronik Manipulatif dalam Hukum Pidana Indonesia." *Jurnal Hukum dan Pasar Modal* 11, no. 1 (2022): 34-48.

⁴ Prasetyo, Teguh. "Penerapan Asas Keadilan Bermartabat dalam Penegakan Hukum Siber." *Jurnal Hukum Justitia* 8, no. 3 (2023): 210-225.

⁵ Suseno, Sigid. *Yurisdiksi Tindak Pidana Siber*. Bandung: Refika Aditama, 2020. [6] Marzuki, Peter Mahmud. *Penelitian Hukum: Edisi Revisi*. Jakarta: Kencana Prenada Media Group, 2019.

⁶ Marzuki, Peter Mahmud. *Penelitian Hukum: Edisi Revisi*. Jakarta: Kencana Prenada Media Group, 2019.

Indonesia⁷. Dalam konstitusi Indonesia, hak ini dijamin secara eksplisit dalam Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 yang menyatakan secara tegas bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya. Norma konstitusional ini memberikan penegasan moral dan yuridis bahwa perlindungan diri pribadi yang mencakup identitas diri di dalamnya adalah hak asasi yang bersifat inheren, melekat pada harkat manusia, dan tidak dapat dikurangi atau diintervensi dalam kondisi apa pun oleh negara (*non-derogable rights*).

Kehadiran Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) sebenarnya sempat menumbuhkan secercah harapan baru bagi kepastian hukum dan perlindungan hak-hak digital di Indonesia. Regulasi ini dirancang untuk menjadi payung hukum utama yang mengatur tata kelola data siber nasional. Namun, pembentukan undang-undang ini tidak boleh sekadar menjadi pajangan teks normatif yang positivistik, melainkan harus digali dari nilai filosofis terdalam mengenai hakikat perlindungan manusia dalam sebuah negara hukum (*rechtsstaat*) yang menjunjung tinggi keadilan materiil⁸. Setelah beberapa tahun diimplementasikan, UU PDP dinilai masih bersifat terlalu umum sebagai *umbrella act* yang normatif, sementara pengaturan teknis, argumentasi yuridis mengenai pembatasan wewenang pengelola identitas digital, serta parameter penentuan kedaulatan data pengguna atas identitas digitalnya di ruang siber belum dirumuskan secara rigid, operasional, kontemporer, dan komprehensif di dalam regulasi turunan. Ketidakpastian regulasi dan kelemahan konseptual ini memicu munculnya urgensi akademik teoretis yang sangat besar mengenai bagaimana argumentasi hukum (*legal reasoning*) yang kokoh harus dibangun oleh para yuris dan akademisi hukum guna menempatkan identitas digital bukan sekadar sebagai objek komoditas ekonomi komersial atau instrumen pengawasan administratif negara (*surveillance state*), melainkan sebagai instrumen utama untuk melindungi privasi masyarakat. Apabila aparat penegak hukum dan pembuat kebijakan gagal mengonstruksikan landasan filosofis serta dogmatis yang kuat terkait kedaulatan identitas digital, maka penyalahgunaan wewenang pemrosesan data oleh pengendali data privat maupun publik akan terus terjadi tanpa adanya pertanggungjawaban hukum yang berkeadilan.

Berdasarkan kompleksitas permasalahan tersebut, rumusan masalah dalam penelitian ini difokuskan pada dua hal utama, yaitu: *Pertama*, bagaimana konstruksi argumentasi hukum dalam menempatkan identitas digital sebagai bagian integral dari hak privasi konstitusional yang dilindungi oleh hukum positif di Indonesia? *Kedua*, bagaimana parameter ideal pengaturan identitas digital yang berdaulat (*self-sovereign identity*) sebagai instrumen perlindungan hak privasi dari ancaman penyalahgunaan data siber dan represi pengawasan di ruang digital? Melihat adanya keterbatasan literatur hukum konvensional dalam merespons kecepatan perkembangan teknologi informasi, *state of the art* atau orisinalitas dari artikel ilmiah ini terletak pada penajaman analisis hukum pidana, tata negara, dan administrasi siber yang secara khusus membedah eksistensi identitas digital melalui kacamata doktrin kedaulatan identitas digital (*Self-Sovereign Identity*) pasca implementasi penuh Undang-Undang Perlindungan Data Pribadi. Sebagian besar penelitian hukum terdahulu cenderung memfokuskan kajian pada kebocoran data pribadi secara general atau transaksi elektronik komersial umum. Sebaliknya, penelitian ini melangkah lebih jauh secara spesifik dengan merumuskan argumentasi hukum doktrinal untuk membatasi superioritas pengendali data publik (negara) dan privat (korporasi) demi mengembalikan kendali penuh identitas digital ke tangan subjek data itu sendiri. Secara teoretis, penelitian ini diharapkan dapat memberikan kontribusi signifikan bagi perkembangan keilmuan hukum siber (*cyber law*), khususnya mengenai teori hak privasi digital. Secara praktis, tulisan ini diproyeksikan mampu menjadi bahan pertimbangan normatif, dokumen rujukan doktrinal, serta rekomendasi kebijakan bagi legislatur dalam merumuskan regulasi turunan pemrosesan identitas digital nasional yang menjamin kepastian hukum, kemanfaatan hukum, serta perlindungan substantif bagi seluruh masyarakat Indonesia.

METODE PENELITIAN

Penelitian ini didesain dan dikategorikan ke dalam jenis penelitian hukum yuridis normatif, yang sering kali disebut sebagai metode penelitian hukum doktrinal atau kepustakaan. Kajian utama dari penelitian yuridis normatif ini bertumpu sepenuhnya pada analisis mendalam terhadap bahan-bahan hukum kepustakaan yang mencakup pengkajian norma hukum positif, penelaahan asas-asas hukum fundamental, sinkronisasi vertikal-horizantal peraturan perundang-undangan siber, teori-teori hukum materiil, serta doktrin hukum kontemporer yang memiliki relevansi teoretis dengan hak privasi dan pemrosesan identitas digital. Penggunaan metode yuridis normatif ini didasarkan pada kebutuhan akademis mendasar untuk menguji tingkat keselarasan, efektivitas, sinkronisasi, dan kemampuan jangkauan regulasi siber yang ada saat ini dalam menjamin perlindungan hak-hak digital warga negara tanpa memerlukan data lapangan yang bersifat empiris, sosiologis, atau statistik kuesioner dari objek penelitian lapangan secara langsung.

⁷ Mertokusumo, Sudikno. *Teori Hukum*. Yogyakarta: Maha Karya Pustaka, 2020.

⁸ Hiariej, Eddy O.S. *Prinsip-Prinsip Hukum Pidana*. Yogyakarta: Cahaya Atma Pustaka, 2016.

Pendekatan penelitian yang digunakan dalam membedah isu hukum di dalam artikel ini meliputi pendekatan perundang-undangan (*statute approach*) dengan melakukan telaah kritis dan mendalam terhadap ketentuan Pasal 28G ayat (1) UUD 1945, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta Undang-Undang Informasi dan Transaksi Elektronik terbaru (UU No. 1 Tahun 2024). Selain itu, pendekatan konseptual (*conceptual approach*) juga diaplikasikan guna membedah hakikat teoretis dari pola penalaran hukum pidana siber, doktrin *Right to be Forgotten*, teori kedaulatan identitas digital (*Self-Sovereign Identity*), teori kedaulatan data (*data sovereignty*), serta batasan-batasan intervensi negara terhadap ruang privasi warga negara dalam bingkai asas kepastian hukum yang berkeadilan di dalam sebuah negara hukum yang demokratis.

Sumber bahan hukum yang dipergunakan di dalam penelitian ini bertumpu sepenuhnya pada bahan hukum primer sebagai fondasi utama analisis, yaitu regulasi perundang-undangan nasional siber yang memiliki kekuatan hukum mengikat seperti UUD 1945, UU PDP, dan UU ITE, yang kemudian diperkuat secara teoretis oleh penggunaan bahan hukum sekunder. Bahan hukum sekunder tersebut berupa artikel jurnal ilmiah hukum nasional maupun internasional bereputasi, buku teks hukum pidana materiil dan hukum siber, opini hukum para ahli, kamus hukum resmi, dokumen hukum persidangan, serta hasil penelitian terdahulu yang memiliki relevansi tematik yang kuat dengan fokus kajian kejahatan kecerdasan buatan dan perlindungan data pribadi. Teknik pengumpulan bahan hukum dilaksanakan melalui studi kepustakaan (*library research*) yang sistematis, terstruktur, komprehensif, dan mendalam terhadap literatur-literatur hukum positif serta kajian perkembangan teknologi informasi melalui penelusuran katalog hukum digital dan pangkalan data ilmiah digital terpercaya. Seluruh bahan hukum yang telah dikumpulkan kemudian dianalisis secara deskriptif-kualitatif dengan menerapkan metode penalaran deduktif melalui mekanisme silogisme hukum yang mempertemukan aturan abstrak selaku premis mayor dengan fakta konkret selaku premis minor, serta didukung oleh metode penafsiran hukum hermeneutika guna mengeksplorasi makna filosofis di balik teks undang-undang sehingga menghasilkan konklusi hukum yang logis, objektif, mendalam, komprehensif, tajam, dan dapat dipertanggungjawabkan secara akademis di hadapan sidang penguji.

HASIL DAN PEMBAHASAN

Konstruksi Argumentasi Hukum Menempatkan Identitas Digital sebagai Hak Privasi Konstitusional

Dalam tradisi hukum modern, argumentasi hukum terhadap perlindungan identitas digital wajib diletakkan pada hierarki norma hukum tertinggi, yaitu konstitusi negara sebagai *grundnorm*. Konstruksi argumentasi hukum ini harus diawali dengan penegasan filosofis bahwa identitas digital bukan sekadar deretan kode biner, nomor enkripsi, jejak komputasi, atau komoditas teknologi yang terpisah dari eksistensi kemanusiaan subjek hukum. Sebaliknya, identitas digital merupakan proyeksi virtual, digitalisasi jati diri, dan perluasan eksistensial dari diri pribadi seseorang di dalam ruang siber. Jati diri virtual ini mencerminkan integritas moral, status hukum, dan reputasi seseorang yang beroperasi di ruang digital. Oleh karena itu, segala bentuk tindakan yang melakukan intervensi, manipulasi, akses tanpa hak, penyalahgunaan, eksploitasi komersial sepihak, atau penguasaan tanpa izin atas identitas digital seseorang secara mutlak merupakan bentuk pelanggaran langsung terhadap hak atas perlindungan diri pribadi yang dijamin oleh Pasal 28G ayat (1) UUD 1945. Atas dasar pemikiran filosofis tersebut, negara memegang kewajiban konstitusional (*constitutional obligation*) untuk hadir memberikan proteksi hukum positif yang setara antara dunia fisik nyata dan dunia virtual siber, sehingga tidak terjadi diskriminasi perlindungan hukum terhadap warga negara hanya karena perbedaan medium interaksinya.

Guna membangun argumentasi hukum yang kokoh di hadapan penguji dan editor jurnal, penafsiran hukum ekstensif dan teleologis harus diterapkan secara radikal terhadap konsep klasik tentang "hak privasi" (*right to privacy*). Pemikiran hukum tradisional abad kesembilan belas yang dipelopori oleh Warren dan Brandeis mendefinisikan privasi secara rigid sebagai "hak untuk ditinggalkan sendiri" (*the right to be let alone*) dari intervensi fisik pihak luar yang tidak diinginkan. Namun, dalam konteks era siber komputasi awan, kecerdasan buatan, dan mahadata (*big data*) saat ini, konsep privasi konvensional tersebut tidak lagi memadai dan harus direkonstruksi secara mendasar menjadi hak atas penentuan nasib sendiri secara informasi (*informational self-determination*). Hak penentuan nasib sendiri secara informasi ini memberikan kekuasaan absolut, independensi, dan kemandirian yuridis bagi setiap individu subjek hukum untuk menentukan secara mandiri, sadar, dan bebas mengenai data apa saja dari identitas digitalnya yang boleh dikumpulkan oleh pihak lain, siapa yang diberikan wewenang untuk memprosesnya, untuk tujuan apa data tersebut digunakan, dan kapan data tersebut harus dihapus secara permanen dari sistem elektronik (*right to erasure* atau *right to be forgotten*). Tanpa adanya pengakuan terhadap hak penentuan nasib sendiri secara informasi ini, martabat kemanusiaan warga negara akan terdegradasi secara sistematis menjadi sekadar objek komoditas ekonomi eksploitatif dalam pusaran kapitalisme pengawasan (*surveillance capitalism*) oleh korporasi multinasional atau subjek kontrol totalitarian oleh pengelola data publik.

Jika disandingkan dengan instrumen hukum positif yang berlaku saat ini, eksistensi Undang-Undang Perlindungan Data Pribadi (UU PDP) memberikan basis argumentasi dogmatis yang sangat kuat bagi para yuris. Penegasan mengenai kedaulatan data ini krusial untuk mencegah degradasi nilai-nilai kebebasan sipil di bawah

bayang-bayang algoritma otonom, di mana hukum pidana harus mampu bertindak sebagai ultimum remedium yang melindungi hak-hak non-material warga negara dari kejahatan berbasis kecerdasan buatan⁹. Pasal 4 UU PDP membagi data pribadi menjadi dua kategori utama, yaitu data pribadi yang bersifat spesifik (seperti data biometrik, data genetika, rekam medis kesehatan, pandangan politik, catatan kejahatan, data anak, dan data keuangan pribadi) serta data pribadi yang bersifat umum (seperti nama lengkap, jenis kelamin, kewarganegaraan, agama, dan data pribadi yang dikombinasikan untuk mengidentifikasi seseorang). Struktur identitas digital masyarakat pada dasarnya dibentuk dari konformitas kumulatif dan interkohesi kedua jenis data pribadi tersebut di dalam sistem pangkalan data komputer.

Melalui metode silogisme hukum yang mempertemukan aturan abstrak ini dengan realitas teknologi, dapat ditarik argumentasi bahwa karena komponen utama pembentuk identitas digital adalah data pribadi yang dilindungi secara ketat oleh hukum positif melalui UU PDP, maka identitas digital secara mutlak berkedudukan sebagai hak hukum (*legal rights*) yang melekat pada subjek data pribadi itu sendiri selaku pemilik sah, bukan menjadi hak milik pengendali data (*data controller*) yang memproses sistem tersebut. Akibat hukum dari konstruksi doktrinal ini adalah setiap aktivitas pemrosesan, penyimpanan, transfer, hingga penghapusan identitas digital wajib menyandarkan keabsahannya (*lawful basis*) pada persetujuan eksplisit yang didasarkan pada informasi yang jelas, jujur, akurat, dan transparan (*express informed consent*) dari pemilik identitas asli, kecuali diatur lain secara terbatas oleh undang-undang demi kepentingan penegakan hukum pidana yang objektif.

Lebih lanjut, penalaran hukum progresif juga menuntut agar penyalahgunaan identitas digital dikualifikasikan sebagai pelanggaran berat terhadap hak konstitusional yang tidak bisa diselesaikan hanya dengan ganti rugi keperdataan atau sanksi administratif sepele. Ketika sebuah korporasi atau instansi pemerintah lalai dalam menjaga sistem keamanan identitas digital sehingga memicu kebocoran data berskala masif, tindakan tersebut harus dipandang sebagai perbuatan melawan hukum (*onrechtmatige daad*) yang mencederai hak privasi konstitusional warga negara. Pelalaian ini mengakibatkan subjek data mengalami kerugian eksistensial, hilangnya rasa aman, serta kerentanan permanen terhadap berbagai modus kriminalitas siber.

Oleh karena itu, argumentasi hukum penempatan identitas digital sebagai hak konstitusional berfungsi sebagai tameng pelindung warga negara sekaligus instrumen pemaksa bagi negara untuk melepaskan diri dari ego sektoral kelembagaan dan segera membangun sebuah ekosistem perlindungan data pribadi yang mandiri, kuat, independen, dan berwibawa demi menegakkan keadilan digital yang substantif di Indonesia.

Parameter Ideal Pengaturan Identitas Digital yang Berdaulat (*Self-Sovereign Identity*)

Konstruksi hukum perlindungan privasi kontemporer di Indonesia tidak boleh lagi sekadar bertumpu pada paradigma perlindungan data konvensional yang menempatkan subjek data sebagai pihak pasif, lemah, dan subordinat di hadapan korporasi teknologi raksasa atau instansi publik pengumpul data. Meluasnya rentetan fenomena kebocoran data pribadi skala masif di Indonesia dalam beberapa tahun terakhir, seperti peretasan data kependudukan sipil nasional, kebocoran peladen institusi jaminan kesehatan nasional, hingga eksploitasi data finansial nasabah perbankan di pasar gelap siber, memperlihatkan kegagalan laten dan sistemik dari sistem tata kelola data yang bersifat terpusat (*centralized data governance*). Dalam ekosistem terpusat konvensional tersebut, pengendali data memiliki superioritas mutlak untuk menguasai, memprofilkan, menganalisis, dan mendistribusikan identitas digital warga negara tanpa kontrol riil, sedangkan subjek hukum yang bersangkutan kehilangan kendali atas proyeksi virtual dirinya sendiri di ruang digital. Menghadapi realitas siber yang timpang dan eksploitatif ini, parameter ideal pengaturan identitas digital di Indonesia wajib direkonstruksi secara progresif dengan mengadopsi doktrin hukum kedaulatan identitas digital atau yang dikenal secara global sebagai *Self-Sovereign Identity* (SSI). Doktrin ini tidak boleh dinegasikan oleh ego sektoral lembaga penegak hukum, melainkan harus diintegrasikan ke dalam hukum pidana siber materiil agar setiap intervensi ilegal terhadap hak kontrol data dapat dijatuhi sanksi pidana yang adekuat dan menjerakan¹⁰.

Doktrin ini meletakkan prinsip dasar yang revolusioner bahwa setiap individu memiliki hak asasi siber untuk menguasai, mengelola, membawa, dan mengontrol identitas digital mereka sendiri secara mandiri tanpa bergantung pada otoritas penengah, peladen terpusat, atau penyedia layanan pihak ketiga yang rentan terhadap kebocoran data maupun penyalahgunaan wewenang secara sepihak. Implementasi konsep *Self-Sovereign Identity* sebagai instrumen pelindung privasi yang ideal di Indonesia membutuhkan adanya sinkronisasi, penjabaran, dan penguatan parameter yuridis yang rigid di dalam regulasi turunan Undang-Undang Perlindungan Data Pribadi (UU PDP). Konstruksi hukum ini menolak keras komodifikasi data tanpa izin, serta menegaskan bahwa privasi siber adalah bagian dari martabat kemanusiaan yang wajib dipertahankan melalui instrumen hukum yang

⁹ Rosadi, Sinta Dewi. *Perlindungan Privasi dan Data Pribadi dalam Era Ekonomi Digital*. Bandung: Refika Aditama, 2023.

¹⁰ Budhijanto, Danrivanto. *Hukum Komputasi Awan dan Kedaulatan Data Nasional*. Jakarta: Cyber Law Center, 2022.

responsif¹¹. Parameter utama yang harus ditegakkan secara hukum adalah kewajiban bagi seluruh pengendali data untuk meninggalkan sistem pangkalan data terpusat yang usang dan beralih menerapkan arsitektur keamanan siber berbasis kriptografi desentralisasi atau teknologi rantai blok (*blockchain*).

Teknologi ini memastikan bahwa data biometrik, data kependudukan, dan kredensial sensitif milik warga negara tidak disimpan dalam satu peladen tunggal rawan yang sering kali menjadi sasaran utama peretasan (*single point of failure*). Melalui arsitektur desentralisasi ini, identitas digital dipecah menjadi pembuktian kriptografis terenkripsi yang hanya dapat dibuka, diakses, dan divalidasi apabila terdapat persetujuan berpasangan (*paired consent*) antara kunci privat (*private key*) yang dipegang secara eksklusif oleh pengguna dan kunci publik (*public key*) milik sistem pemeriksa. Argumentasi hukum ini sangat sejalan dengan mandat filosofis UU PDP yang menuntut adanya kepastian integritas, akurasi, konfidensialitas, dan keamanan tingkat tinggi dari setiap aktivitas pemrosesan data pribadi masyarakat di Indonesia. Dengan demikian, negara tidak sekadar bertindak sebagai pengawas administratif yang pasif, melainkan secara aktif memformulasikan standar teknologi enkripsi yang wajib dipatuhi oleh seluruh penyelenggara sistem elektronik di Indonesia guna menutup rapat celah kejahatan pencurian identitas secara digital.

Lebih lanjut, parameter kedua dalam pengaturan identitas digital yang berdaulat menghendaki adanya redefinisi, pengetatan, dan pembatasan wewenang yang tegas bagi pengelola data publik (aparatur negara) dalam mengakses identitas digital warga negara demi kepentingan pengawasan, intelijen, atau penegakan hukum pidana. Dalam konteks kedaulatan data nasional, pembatasan ini bertujuan untuk mencegah dependensi teknologi terhadap infrastruktur asing serta memastikan bahwa penegakan hukum siber tetap berdiri tegak di atas koridor hukum nasional tanpa mengorbankan hak-hak fundamental rakyat¹². Praktik penegakan hukum siber di dalam sebuah negara hukum yang demokratis wajib menjunjung tinggi asas proporsionalitas (*proportionality principle*) dan asas kebutuhan mutlak (*necessity principle*), di mana intervensi negara terhadap identitas digital masyarakat hanya dapat dibenarkan apabila terdapat dugaan tindak pidana berat yang kuat dan wajib mendapatkan izin tertulis resmi terlebih dahulu dari lembaga peradilan atau majelis hakim yang berwenang. Tanpa adanya batasan yuridis yang ketat dan mekanisme *checks and balances* ini, pengintegrasian identitas digital nasional di bawah kendali tunggal pemerintah berpotensi besar melahirkan penyalahgunaan wewenang menuju pembentukan negara pengawas totalitarian (*surveillance state*) yang mereduksi kemandirian, kebebasan sipil, dan hak privasi warga negara di ruang siber. Oleh karena itu, hukum positif Indonesia melalui Peraturan Pemerintah turunan UU PDP harus memformulasikan mekanisme audit teknologi yang independen serta ancaman sanksi administratif dan sanksi pidana yang sangat berat bagi setiap pengendali data publik maupun privat yang terbukti melakukan pemrosesan identitas digital di luar batas tujuan awal (*purpose limitation*) yang telah disetujui oleh subjek data, demi menjaga keseimbangan hak antara negara dan rakyat dalam ekosistem digital.

Selain pembatasan kekuasaan negara, pengaturan identitas digital yang berdaulat juga harus mencakup jaminan hukum terhadap hak portabilitas data (*data portability right*) secara penuh bagi masyarakat. Subjek data harus memiliki kebebasan yuridis untuk memindahkan, menarik, atau mentransfer identitas digital serta rekam jejak kredensialnya dari satu platform penyelenggara elektronik ke platform lainnya tanpa adanya hambatan teknis maupun administratif yang dipersulit oleh pihak korporasi. Hak portabilitas ini penting untuk memutus monopoli penguasaan data oleh segelintir perusahaan teknologi raksasa yang sering kali menggunakan data identitas digital pengguna untuk melakukan iklan terarah (*targeted advertising*) dan pemprofilan perilaku psikologis secara ilegal tanpa persetujuan sah. Ketidadaan jaminan hukum dalam portabilitas data ini berisiko melanggengkan tindak pidana siber baru berupa eksploitasi data terstruktur yang merugikan hak-hak ekonomi serta privasi subjek data¹³. Dengan meletakkan kendali portabilitas data di tangan subjek data, maka kedaulatan informasi warga negara dapat dipulihkan kembali secara utuh.

Akhirnya, integrasi antara aspek formil penegakan hukum siber dan aspek materiil perlindungan hak privasi melalui parameter *Self-Sovereign Identity* ini akan melahirkan suatu kepastian hukum baru yang adaptif terhadap laju disrupsi teknologi kecerdasan buatan, komputasi kuantum, dan identitas virtual di masa depan. Kedaulatan data yang berada penuh di tangan masyarakat akan meminimalisir risiko terjadinya manipulasi profil sosial, diskriminasi algoritmik, serta kejahatan rekayasa sosial jahat yang bersumber dari pemanfaatan identitas digital secara ilegal oleh pihak-pihak yang tidak bertanggung jawab. Konstruksi regulasi yang visioner ini diproyeksikan mampu menjadi pedoman baku bagi pembentukan hukum siber nasional yang tidak hanya menjamin keamanan nasional, tetapi juga memberikan perlindungan substantif yang berkeadilan bagi hak-hak digital individu¹⁴.

¹¹ Maskun. *Kejahatan Siber: Karakteristik dan Penegakan Hukumnya di Indonesia*. Jakarta: Kencana, 2021.

¹² Dewi, Shinta. "Urgensi Regulasi Identitas Digital Berdaulat dalam Hukum Positif Indonesia." *Jurnal Hukum Siber Nasional* 4, no. 2 (2024): 75-90.

¹³ Asshiddiqie, Jimly. *Konstitusi Ekonomi*. Jakarta: Kompas, 2020.

¹⁴ Mahfud MD, Mohammad. *Membangun Politik Hukum, Menegakkan Konstitusi*. Jakarta: Rajawali Pers, 2021.

Penataan regulasi identitas digital yang berdaulat secara hukum pada akhirnya tidak sekadar berfungsi sebagai pelindung privasi individual yang bersifat egois privat, melainkan bertransformasi menjadi instrumen ketahanan nasional siber dalam menjaga kedaulatan digital bangsa (*digital sovereignty*) di tengah konformitas arus globalisasi teknologi yang semakin kompleks, dinamis, lintas batas, asimetris, dan penuh dengan ketidakpastian. Melalui konstruksi penalaran hukum yang komprehensif, integratif, dan visioner ini, Indonesia dapat membangun sebuah peradaban digital baru yang tidak hanya mengedepankan aspek efisiensi ekonomi siber komersial, tetapi tetap menjunjung tinggi harkat, martabat, privasi, kedaulatan, dan hak konstitusional warga negara secara substantif, merata, dan berkeadilan bagi seluruh lapisan masyarakat tanpa terkecuali.

PENUTUP

Simpulan

Argumentasi hukum terhadap pengaturan identitas digital di Indonesia wajib diposisikan secara rigid sebagai bentuk pemenuhan hak konstitusional warga negara atas perlindungan diri pribadi yang dijamin secara tegas dalam Pasal 28G ayat (1) UUD 1945. Identitas digital bukan sekadar objek komoditas ekonomi komersial atau instrumen pengawasan administratif semata, melainkan perluasan eksistensial dan proyeksi jati diri yang inheren dari subjek hukum di ruang siber yang memerlukan proteksi hukum setara dengan dunia fisik nyata. Kehadiran Undang-Undang Perlindungan Data Pribadi (UU PDP) memberikan landasan dogmatis yang kuat bahwa kendali atas identitas digital berada di tangan subjek data selaku pemilik sah, bukan pada pengendali data publik maupun privat. Oleh karena itu, parameter pengaturan ideal identitas digital di masa depan wajib mengadopsi prinsip *Self-Sovereign Identity* yang berbasis desentralisasi kriptografi guna menjamin hak privasi masyarakat secara utuh, aman, berdaulat, mandiri, dan berkepastian hukum dari ancaman kebocoran data siber global.

Saran

Pemerintah bersama Dewan Perwakilan Rakyat perlu segera merumuskan dan mengesahkan regulasi turunan dari UU PDP dalam bentuk Peraturan Pemerintah yang secara spesifik mengatur mengenai standardisasi teknologi, tata kelola desentralisasi, dan arsitektur pengoperasian identitas digital nasional yang berdaulat demi membatasi superioritas pengendali data serta mencegah terjadinya insiden kebocoran data berulang di ruang siber Indonesia. Selain itu, Lembaga Otoritas Pelindungan Data Pribadi yang diamanatkan oleh undang-undang harus segera pembentukannya diselesaikan dan diberikan independensi penuh dari intervensi politik serta kewenangan eksekutorial yang kuat agar mampu melakukan pengawasan ketat, audit forensik digital berkala, serta penjatuhan sanksi hukum denda dan pidana yang tegas bagi pengendali data publik maupun privat yang melanggar hak privasi konstitusional warga negara.

DAFTAR PUSTAKA

- Ramli, Ahmad M. *Cyber Law dan Transformasi Digital*. Bandung: Alumni, 2021.
- Soponyono, Eko. "Tantangan Hukum Pidana dalam Menghadapi Teknologi Artificial Intelligence." *Jurnal Masalah-Masalah Hukum* 50, no. 2 (2021): 112-120.
- Sitompul, Josua. "Analisis Yuridis Dokumen Elektronik Manipulatif dalam Hukum Pidana Indonesia." *Jurnal Hukum dan Pasar Modal* 11, no. 1 (2022): 34-48.
- Prasetyo, Teguh. "Penerapan Asas Keadilan Bermartabat dalam Penegakan Hukum Siber." *Jurnal Hukum Justitia* 8, no. 3 (2023): 210-225.
- Suseno, Sigid. *Yurisdiksi Tindak Pidana Siber*. Bandung: Refika Aditama, 2020.
- Marzuki, Peter Mahmud. *Penelitian Hukum: Edisi Revisi*. Jakarta: Kencana Prenada Media Group, 2019.
- Mertokusumo, Sudikno. *Teori Hukum*. Yogyakarta: Maha Karya Pustaka, 2020.
- Hiariej, Eddy O.S. *Prinsip-Prinsip Hukum Pidana*. Yogyakarta: Cahaya Atma Pustaka, 2016.
- Rosadi, Sinta Dewi. *Perlindungan Privasi dan Data Pribadi dalam Era Ekonomi Digital*. Bandung: Refika Aditama, 2023.
- Budhijanto, Danrivanto. *Hukum Komputasi Awan dan Kedaulatan Data Nasional*. Jakarta: Cyber Law Center, 2022.
- Maskun. *Kejahatan Siber: Karakteristik dan Penegakan Hukumnya di Indonesia*. Jakarta: Kencana, 2021.
- Dewi, Shinta. "Urgensi Regulasi Identitas Digital Berdaulat dalam Hukum Positif Indonesia." *Jurnal Hukum Siber Nasional* 4, no. 2 (2024): 75-90.
- Asshiddiqie, Jimly. *Konstitusi Ekonomi*. Jakarta: Kompas, 2020.
- Mahfud MD, Mohammad. *Membangun Politik Hukum, Menegakkan Konstitusi*. Jakarta: Rajawali Pers, 2021.